

**1. Комплекс основных характеристик программы**

**1.1. Пояснительная записка**

***Нормативно-правовое обеспечение программы***

- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (ст.2, ст.15, ст.16, ст.17, ст.75, ст.79);

- Проект Концепции развития дополнительного образования детей до 2030 года;

- Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

- Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы»;

- Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

- Распоряжение Правительства Российской Федерации от 28.04.2023 № 1105-р «Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 № 2471-р»;

- Приказ Министерства просвещения РФ от 27.07.2022 № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;

- Постановление Главного государственного санитарного врача РФ 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»;

- Письмо Минобрнауки России от 18.11.2015 № 09-3242 «О направлении информации» (вместе с «Методическими рекомендациями по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы)»);

- Локальные акты ОО (Устав, Положение о проектировании ДООП в образовательной организации, Положение о проведение промежуточной аттестации обучающихся и аттестации по итогам реализации ДООП).

***Уровень программы:*** базовый

***Направленность программы***: техническая.

Безопасность в сети Интернет в свете быстрого развития информационных технологий, их глобализации, использования облачных технологий и повсеместного массового распространения среди детей мобильных персональных цифровых устройств доступа к сети Интернет, появления большого количества сетевых сервисов и интернет-коммуникаций, в том числе закрытых сетевых сообществ неизвестного толка, а также общедоступных и зачастую навязчивых интернет-ресурсов (СМИ, реклама, спам), содержащих негативный и агрессивный контент, расширения угроз новых сетевых средств вмешательства в личное информационное пространство на персональных устройствах, работающих в Интернете, а также в связи с массовым использованием детьми электронных социальных/банковских карт, имеющих персональные настройки доступа к ним, резко повышает потребность в воспитании у обучающихся культуры информационной безопасности в целях предотвращения негативных последствий массового использования Интернета детьми и их защиты от агрессивной и противоправной информации.

В программе «Информационная безопасность» учтены приоритеты научно-технологического развития Российской Федерации (Пр-294, п.2а-16).

***Актуальность программы:*** Программа отражает важные вопросы безопасной работы с новыми формами коммуникаций и услуг цифрового мира: потребность в защите персональной информации, угрозы, распространяемые глобальными средствами коммуникаций Интернета и мобильной связи, использующими рассылки сообщений, электронную почту, информационно-коммуникативные ресурсы взаимодействия в сети Интернет через массово доступные услуги электронной коммерции, социальные сервисы, сетевые объединения и сообщества, ресурсы для досуга (компьютерные игры, видео и цифровое телевидение, цифровые средства массовой информации и новостные сервисы), а также повсеместное встраивание дистанционных ресурсов и технологий в учебную деятельность, использующую поиск познавательной и учебной информации, общение в социальных сетях, получение и передачу файлов, размещение личной информации в коллективных сервисах.

Помимо профилактики информационных угроз и противоправных действий через ресурсы в сети Интернет и мобильные сети, крайне актуально использовать коммуникации для привлечения обучающихся к информационно-учебной и познавательно-творческой активности по использованию позитивных интернет-ресурсов: учебных, культурных, научно-популярных, интеллектуальных, читательских, медийных, правовых, познавательных и специализированных социальных сообществ и сервисов для детских объединений и творческих мероприятий для детей младшего школьного возраста.

*Новизна:* Новизна программы состоит в том, что она учитывает новые технологические уклады, которые требуют новый способ мышления и тесного взаимодействия при постоянном повышении уровня междисциплинарности проектов, а также использует новые формы диагностики и подведения итогов реализации программы, выполняемые в формате защиты проектов.

В основу программы «Информационная безопасность» заложены принципы практической направленности, курс ориентирован на изучение и выполнение конкретных задач по защите действующей информационной инфраструктуры от противоправного воздействия.

***Отличительные особенности программы:*** Программа предназначена для учащихся, проявляющих повышенный интерес к информационным технологиям. Программа имеет практическую направленность с ориентацией на реальные потребности, соответствующие возрасту ученика.

Программа поддерживается электронными ресурсами на основе документальных фильмов, анимационных ресурсов и электронных практикумов в открытом доступе от ИТ-компаний Российской Федерации в рамках их участия в проектах по информационной безопасности для детей. В основе курса лежат технические, этические и правовые нормы соблюдения информационной безопасности, установленные контролирующими и правоохранительными органами, а также практические рекомендации ведущих ИТ-компаний и операторов мобильной связи Российской Федерации.

***Педагогическая целесообразность******программы****:* заключается в создании организационных и психолого-педагогических условий для привлечения детей к занятиям техническим творчеством, обеспечивающих развитие мотивации к познанию, творчеству и труду, конструкторских и изобретательских способностей, формирование инженерно-технических компетенций, как факторов успешного самоопределения и самореализации личности в современном мире.

***Адресат программы: Возраст детей 9-14 лет***

***Объём программы: 72 часа.***

***Формы обучения и виды занятий:*** теоретические, практические, групповые. Конкурсы, соревнования, экскурсии, выставки.

***Срок освоения программы: полгода.***

***Режим занятий:*** Занятия проводятся 2 раза в неделю по 2 часа.

**1.2. Цель и задачи программы**

***Цель программы*** *–* формирование у обучающегося цифровой зрелости по вопросам информационной безопасности, которая влияет на дальнейшую социализацию детей в информационном обществе.

***Задачи:***

**Обучающие:**

- обучить критической оценке сетевого контента, анализу достоверности информации, навыкам эффективной интернет-коммуникации;

- способствовать повышению уровня информированности учащихся об опасностях и угрозах в информационно-телекоммуникационных сетях;

- содействовать профилактике совершения учащимися правонарушений в информационно-коммуникационной сфере;

- сформировать устойчивую направленность у обучающихся на освоение механизмов информационно-психологической самозащиты;

- расширить репертуар стратегий поведения у обучающихся в трудных ситуациях, связанных с коммуникационными технологиями.

**Развивающие:**

- способствовать приобретению навыков поиска информации в сети Интернет, анализ выбранной информации на соответствие запросу, использование информации при решении задач;

- развивать познавательные способности ребенка, память, внимание, пространственное мышление, аккуратность и изобретательность;

- формировать творческий подход к поставленной задаче;

- развивать навыки инженерного мышления, умения работать как по предложенным инструкциям, так и находить свои собственные пути решения поставленных задач;

- развивать способности к самоанализу, самопознанию;

**Воспитывающие:**

- воспитать мотивацию учащихся к изобретательству, созданию собственных инженерных и программных реализаций;

- воспитать уважительное отношение к товарищам, к педагогу;

- формировать потребность в самостоятельном приобретении и применении знаний, потребность к постоянному саморазвитию;

- воспитывать социально-значимые качества личности человека: ответственность, коммуникабельность, добросовестность, взаимопомощь, доброжелательность.

1.3 Планируемые результаты освоения программы

**Личностные результаты:**

- формирование ответственного отношения к учению, готовности и способности, обучающихся к саморазвитию и самообразованию на основе мотивации к обучению и познанию;

- формирование целостного мировоззрения, соответствующего современному уровню развития науки и общественной практики;

- развитие осознанного и ответственного отношения к собственным поступкам при работе с графической информацией;

- формирование коммуникативной компетентности в процессе образовательной, учебно-исследовательской, творческой и других видов деятельности.

**Метапредметные результаты:**

- активное использование средств информационно-коммуникационных технологий (ИКТ) для решения коммуникативных и познавательных задач;

- соблюдение норм информационной избирательности, этики и этикета;

- умение адекватно оценивать собственное поведение и поведение окружающих;

- готовность конструктивно разрешать конфликты посредством учета интересов сторон и сотрудничества;

- умение излагать свое мнение и аргументировать свою точку зрения и оценку событий.

- умение осуществлять итоговый и пошаговый контроль выполнения учебного задания по переходу информационной обучающей среды из начального состояния в конечное;

- умение сличать результат действий с эталоном (целью);

- умение вносить коррективы в действия в случае расхождения результата решения задачи с ранее поставленной целью;

- умение оценивать результат своей работы с помощью тестовых компьютерных программ, а также самостоятельно определять пробелы в усвоении материала курса.

**Предметные результаты:**

- понимать источники информационных угроз, вредоносные программы и нежелательные рассылки, поступающие на мобильный телефон, планшет, компьютер;

- знать виды информационных угроз, правила поведения для защиты от угроз;

- определять проблемные ситуации и опасности в сетевом взаимодействии и правила поведения в проблемных ситуациях, ситуациях профилактики и предотвращения опасности;

- использовать этикет сетевого взаимодействия;

- применять простейшие правила защиты персональных данных;

- умение реализовывать простейшие правила цифровой гигиены для использования средств защиты персональных данных (формировать и использовать пароль, регистрироваться на сайтах без распространения личных данных).

Программа может корректироваться в ходе деятельности самого ученика, который оказывается субъектом, конструктором своего образования, полноправным источником и организатором своих знаний.

**1.4. Содержание программы**

**УЧЕБНЫЙ ПЛАН**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Название раздела, темы | Количество часов | | | Форма контроля |
| Всего | Теория | Практика |
| **Модуль 1. Угрозы и риски цифрового пространства** | | | | | |
| 1. | Охрана труда и техника безопасности | 1 | 1 | 0 | Устный опрос |
| 2. | Угрозы и риски цифрового пространства | 1 | 1 | 0 | Устный опрос |
|  | Итого | 2 | 2 | 0 |  |
| Модуль 2. Безопасность общения | | | | | |
| 3. | Общение в социальных сетях и мессенджерах | 3 | 1 | 2 | Практическая работа. Устный опрос |
| 4. | Пароли для аккаунтов социальных сетей | 3 | 1 | 2 | Практическая работа. Устный опрос |
| 5. | Безопасный вход в аккаунты | 3 | 1 | 2 | Практическая работа. Устный опрос |
| 6. | Настройки конфиденциальности в социальных сетях | 3 | 1 | 2 | Практическая работа. Устный опрос |
| 7. | Публикация информации в социальных сетях | 3 | 1 | 2 | Практическая работа. Устный опрос |
| 8. | Кибербуллинг | 2 | 1 | 1 | Практическая работа. Устный опрос |
| 9. | Публичные аккаунты | 3 | 1 | 2 | Практическая работа. Устный опрос |
| 10. | Фишинг | 3 | 1 | 2 | Практическая работа. Устный опрос |
| 11. | Правила безопасной работы в социальной сети. Этикет общения | 2 | 1 | 1 | Практическая работа. Устный опрос |
|  | Итого | 25 | 9 | 16 |  |
| Модуль 3. Безопасность устройств | | | | | |
| 12. | Распространение вредоносного кода | 6 | 2 | 4 | Практическая работа. Устный опрос |
| 13. | Методы защиты от вредоносных программ | 6 | 2 | 4 | Практическая работа. Устный опрос |
| 14. | Распространение вредоносного кода для мобильных устройств | 6 | 2 | 4 | Практическая работа. Устный опрос |
|  | Итого | 18 | 6 | 12 |  |
| Модуль 4. Безопасность информации | | | | | |
| 15. | Социальная инженерия: распознать и избежать | 3 | 1 | 2 | Практическая работа. Устный опрос |
| 16. | Ложная информация в Интернете | 3 | 1 | 2 | Практическая работа. Устный опрос |
| 17. | Безопасность при использовании платежных карт в Интернете | 3 | 1 | 2 | Практическая работа. Устный опрос |
| 18. | Беспроводная технология связи | 3 | 1 | 2 | Практическая работа. Устный опрос |
| 19. | Резервное копирование данных | 3 | 1 | 2 | Практическая работа. Устный опрос |
| 20. | Правила безопасной работы в сети Интернет с планшетом или на компьютере при получении и передаче информации | 3 | 1 | 2 | Практическая работа. Устный опрос |
|  | **Итого** | 18 | 6 | 12 |  |
| **Модуль 5. Персональные данные** | | | | | |
| 21. | Структура персональных данных | 2 | 1 | 2 | Практическая работа. Устный опрос |
| 22. | Способы защиты персональных данных | 3 | 1 | 2 | Практическая работа. Устный опрос |
| 23. | Использование персональных данных | 3 | 1 | 2 | Практическая работа. Устный опрос |
|  | **Итого** | 9 | 3 | 6 |  |
|  | **Итого** | **72** | **26** | **46** |  |

**СОДЕРЖАНИЕ УЧЕБНОГО ПЛАНА**

**Модуль 1. Угрозы и риски цифрового пространства**

***1. Охрана труда и техника безопасности.***

**Теория**. Инструктаж по технике безопасности и правилам противопожарной безопасности.

**Форма контроля**. Устный опрос.

**Оборудование:** Ноутбуки, мышь компьютерная.

***2. Угрозы и риски цифрового пространства***

**Теория**. Характеристика основных угроз в информационной среде.

**Форма контроля**. Устный опрос.

**Оборудование:** Ноутбуки, мышь компьютерная.

**Модуль 2. Безопасность общения**

***3. Общение в социальных сетях и мессенджерах***

**Теория**. Правила общения в социальных сетях. С кем безопасно общаться в интернете.

**Практика**. Применение изученных правил в личных социальных сетях. Переписка.

**Форма контроля**. Устный опрос.

**Оборудование.** Ноутбуки, мышь компьютерная.

***4. Пароли для аккаунтов социальных сетей***

**Теория**. Безопасный вход в аккаунты. Виды аутентификации. Настройки безопасности аккаунта.

**Практика**. Настройки безопасности своего аккаунта.

**Форма контроля**. Устный опрос.

**Оборудование.** Ноутбуки, мышь компьютерная.

***5. Безопасный вход в аккаунты***

**Теория**. Безопасный вход в аккаунты. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

**Практика**. Настройки безопасности своего аккаунта.

**Форма контроля**. Устный опрос.

**Оборудование.** Ноутбуки, мышь компьютерная.

***6. Настройки конфиденциальности в социальных сетях***

**Теория**. Настройки конфиденциальности в социальных сетях.

**Практика**. Настройки приватности в социальных сетях.

**Форма контроля**. Устный опрос.

**Оборудование.** Ноутбуки, мышь компьютерная.

***7. Публикация информации в социальных сетях***

**Теория**. Публикация личной информации в социальных сетях.

**Практика**. Применение изученных правил публикации в социальных сетях.

**Форма контроля**. Устный опрос.

**Оборудование.** Ноутбуки, мышь компьютерная.

***8. Кибербуллинг***

**Теория**. Что такое кибербуллинг. Правила поведения.

**Практика**. Применение изученных правил.

**Форма контроля**. Устный опрос.

**Оборудование.** Ноутбуки, мышь компьютерная.

***9. Публичные аккаунты***

**Теория**. Публичные аккаунты – задачи и отличия.

**Практика**. Поиск и изучение публичных аккаунтов.

**Форма контроля**. Устный опрос.

**Оборудование.** Ноутбуки, мышь компьютерная.

***10. Фишинг***

**Теория**. Что такое фишинг и как с ним бороться.

**Практика**. Определение фишинговых сайтов.

**Форма контроля**. Устный опрос.

**Оборудование.** Ноутбуки, мышь компьютерная.

***11. Правила безопасной работы в социальной сети. Этикет общения***

**Теория**. Правила безопасной работы в социальной сети.

**Практика**. Применение изученных правил.

**Форма контроля**. Устный опрос.

**Оборудование.** Ноутбуки, мышь компьютерная.

**Модуль 3. Безопасность устройств**

***12. Распространение вредоносного кода***

**Теория**. Распространение вредоносного кода. Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты.

**Практика**. Способы выявления наличия вредоносных кодов на устройствах.

**Форма контроля**. Устный опрос. Практическая работа.

**Оборудование.** Ноутбуки, мышь компьютерная.

***13. Методы защиты от вредоносных программ***

**Теория**. Действия при обнаружении вредоносных кодов на устройствах. Способы защиты устройств от вредоносного кода. Правила защиты от вредоносных кодов.

**Практика**. Изучение антивирусных программ и их характеристик.

**Форма контроля**. Устный опрос. Практическая работа.

**Оборудование.** Ноутбуки, мышь компьютерная.

***14. Распространение вредоносного кода для мобильных устройств***

**Теория**. Распространение вредоносного кода для мобильных устройств. Расширения вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

**Практика**. Применение изученных правил.

**Форма контроля**. Устный опрос. Практическая работа.

**Оборудование.** Ноутбуки, мышь компьютерная.

**Модуль 4. Безопасность информации**

***15. Социальная инженерия: распознать и избежать***

**Теория.** Популярные методы социальной инженерии (Фишинг, Троян, Кви про кво, Претекстинг, Обратная социальная инженерия, Внедрение особого ПО, Реклама.

**Практика**. Применение изученных способов защиты.

**Форма контроля**. Устный опрос. Практическая работа.

**Оборудование.** Ноутбуки, мышь компьютерная.

***16. Ложная информация в Интернете***

**Теория.** Виды ложной информации в Интернете.

**Практика**. Применение изученных способов распознавания ложной информации.

**Форма контроля**. Устный опрос. Практическая работа.

**Оборудование.** Ноутбуки, мышь компьютерная.

***17. Безопасность при использовании платежных карт в Интернете***

**Теория.** Правила использования платежных карт в Интернете.

**Практика**. Применение изученных правил.

**Форма контроля**. Устный опрос. Практическая работа.

**Оборудование.** Ноутбуки, мышь компьютерная.

***18. Беспроводная технология связи***

**Теория.** Виды и характеристики беспроводных технологий связи.

**Практика**. Применение изученных правил работы с беспроводными технологиями связи.

**Форма контроля**. Устный опрос. Практическая работа.

**Оборудование.** Ноутбуки, мышь компьютерная.

***19. Резервное копирование данных***

**Теория.** Для чего нужно резервное копирование данных. Где находится резервная копия на телефоне. Как сохранить все данные с телефона. Когда резервное копирование необходимо. Как посмотреть, что входит в резервную копию. Как сохранить всю информацию с телефона в облако.

**Практика**. Применение изученных правил по резервному копированию данных.

**Форма контроля**. Устный опрос. Практическая работа.

**Оборудование.** Ноутбуки, мышь компьютерная.

***20*. *Правила безопасной работы в сети Интернет с планшетом или на компьютере при получении и передаче информации***

**Теория.** Правила безопасной работы в сети Интернет с планшетом или на компьютере при получении и передаче информации.

**Практика**. Применение изученных правил.

**Форма контроля**. Устный опрос. Практическая работа.

**Оборудование.** Ноутбуки, мышь компьютерная.

**Модуль 5. Персональные данные**

***21*. *Структура персональных данных***

**Теория.** Понятие и виды персональных данных. Перечень нормативных правовых актов, регулирующих работы с персональными данными

**Практика**. Применение изученной информации.

**Форма контроля**. Устный опрос. Практическая работа.

**Оборудование.** Ноутбуки, мышь компьютерная.

***22*. *Способы защиты персональных данных***

**Теория.** Основные способы защиты персональных данных. Контролирующие органы власти.

**Практика**. Применение изученной информации.

**Форма контроля**. Устный опрос. Практическая работа.

**Оборудование.** Ноутбуки, мышь компьютерная.

***23*. *Использование персональных данных***

**Теория.** Формы и правила использования персональных данных. Сайт «Госуслуги»

**Практика**. Применение изученной информации.

**Форма контроля**. Устный опрос. Практическая работа.

**Оборудование.** Ноутбуки, мышь компьютерная.

**2. Комплекс организационно-педагогических условий**

**2.1. Календарный учебный график 1 модуль – 2 часа**

**Место проведения:** ЦЦОД «IT-куб» (Заволжье)

**Время проведения занятий:** 15:00-16:30, 16:40-18:10, 18:15-19:45.\_

**Изменения расписания занятий:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| №п/п | Тема занятия | Кол-во часов | Форма занятия | Форма контроля | Дата проведения занятия | | Причина изменения даты |
| планируемая | фактическая |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|  | | | | | | | |
| 1 | Охрана труда и техника безопасности. | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 2 | Угрозы и риски цифрового пространства | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
|  | **Итого:** | **2 часа** |  |  |  |  |  |

**Календарный учебный график модуль 2 – 25 часов**

**Место проведения:** ЦЦОД «IT-куб» (Заволжье)

**Время проведения занятий:** 15:00-16:30, 16:40-18:10, 18:15-19:45.\_

**Изменения расписания занятий:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| №п/п | Тема занятия | Кол-во часов | Форма занятия | Форма контроля | Дата проведения занятия | | Причина изменения даты |
| планируемая | фактическая |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|  | | | | | | | |
| 3. | Общение в социальных сетях и мессенджерах | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 4. | Пароли для аккаунтов социальных сетей | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 5. | Общение в социальных сетях и мессенджерах | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 6 | Пароли для аккаунтов социальных сетей | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 7 | Безопасный вход в аккаунты | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 8 | Настройки конфиденциальности в социальных сетях | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 9 | Безопасный вход в аккаунты | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 10 | Настройки конфиденциальности в социальных сетях | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 11 | Публикация информации в социальных сетях | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 12 | Кибербуллинг | 1 | Лекция (видеокон-ференция) | устный опрос |  |  |  |
| 13 | Публикация информации в социальных сетях | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 14 | Кибербуллинг | 1 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 15 | Публичные аккаунты | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 16 | Фишинг | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 17 | Публичные аккаунты | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 18 | Фишинг | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 19 | Правила безопасной работы в социальной сети. Этикет общения | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 20 | Правила безопасной работы в социальной сети. Этикет общения | 1 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
|  | **Итого:** | **25 часов** |  |  |  |  |  |

**Календарный учебный график модуль 3 – 18 часов**

**Место проведения:** ЦЦОД «IT-куб» (Заволжье)

**Время проведения занятий:** 15:00-16:30, 16:40-18:10, 18:15-19:45.\_

**Изменения расписания занятий:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| №п/п | Тема занятия | Кол-во часов | Форма занятия | Форма контроля | Дата проведения занятия | | Причина изменения даты |
| планируемая | фактическая |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|  | | | | | | | |
| 21 | Распространение вредоносного кода | 2 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 22 | Распространение вредоносного кода | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 23 | Распространение вредоносного кода | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 24 | Методы защиты от вредоносных программ | 2 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 25 | Методы защиты от вредоносных программ | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 26 | Методы защиты от вредоносных программ | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 27 | Распространение вредоносного кода для мобильных устройств | 2 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 28 | Распространение вредоносного кода для мобильных устройств | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 29 | Распространение вредоносного кода для мобильных устройств | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
|  | **Итого:** | **18 часов** |  |  |  |  |  |

**Календарный учебный график модуль 4 – 18 часов**

**Место проведения:** ЦЦОД «IT-куб» (Заволжье)

**Время проведения занятий:** 15:00-16:30, 16:40-18:10, 18:15-19:45.\_

**Изменения расписания занятий:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| №п/п | Тема занятия | Кол-во часов | Форма занятия | Форма контроля | Дата проведения занятия | | Причина изменения даты |
| планируемая | фактическая |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|  | | | | | | | |
| 30 | Социальная инженерия: распознать и избежать | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 31 | Ложная информация в Интернете | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 32 | Социальная инженерия: распознать и избежать | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 33 | Ложная информация в Интернете | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 34 | Безопасность при использовании платежных карт в Интернете | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 35 | Беспроводная технология связи | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 36 | Безопасность при использовании платежных карт в Интернете | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 37 | Беспроводная технология связи | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 38 | Резервное копирование данных | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 39 | Правила безопасной работы в сети Интернет с планшетом или на компьютере при получении и передаче информации | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 40 | Резервное копирование данных | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 41 | Правила безопасной работы в сети Интернет с планшетом или на компьютере при получении и передаче информации | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
|  | **Итого:** | **18 часов** |  |  |  |  |  |

**Календарный учебный график модуль 5 – 9 часов**

**Место проведения:** ЦЦОД «IT-куб» (Заволжье)

**Время проведения занятий:** 15:00-16:30, 16:40-18:10, 18:15-19:45.\_

**Изменения расписания занятий:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| №п/п | Тема занятия | Кол-во часов | Форма занятия | Форма контроля | Дата проведения занятия | | Причина изменения даты |
| планируемая | фактическая |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|  | | | | | | | |
| 42 | Структура персональных данных | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 43 | Способы защиты персональных данных | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 44 | Структура персональных данных | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 45 | Способы защиты персональных данных | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
| 46 | Использование персональных данных | 1 | лекция (видеокон-ференция) | устный опрос |  |  |  |
| 47 | Использование персональных данных | 2 | комбинированное занятие (онлайн-консульта-ция) | практическая работа |  |  |  |
|  | **Итого:** | **9 часов** |  |  |  |  |  |

**2. Комплекс организационно-педагогических условий**

**2.1. Условия реализации программы**

**Материально-техническое обеспечение**

Для электронного обучения и обучения с применением дистанционных образовательных технологий используются технические средства, а также информационно-телекоммуникационные сети, обеспечивающие передачу по линиям связи указанной информации (образовательные онлайн-платформы, цифровые образовательные ресурсы, размещенные на образовательных сайтах, видеоконференции, вебинары, skype-общение, e-mail, облачные сервисы и т.д.)

Объединение располагается в учебном кабинете. Кабинет обеспечен соответствующей мебелью: рабочими столами, стульями, компьютерами, программным обеспечением, выходом в интернет, мультимедийной доской, столом для руководителя.

Группа учеников состоит из 10-12 человек.

Рабочее место оснащено столом, стульями, персональным компьютером или ноутбуком, компьютерной мышью, программным обеспечением.

К работе в объединении дети приступают после проведения руководителем соответствующего инструктажа по правилам техники безопасной работы, объявлением темы занятия, плана работы. Новую тему руководитель объясняет с применением технологий мультимедиа.

**Технические средства обучения**

1) Кабинет (35 кв. м.)

2) Персональный компьютер с процессором не ниже 1,2 Ггц и 256 Мб оперативной памяти с установленной операционной системой Linux или Windows (13 шт.).

3) Персональный компьютер с процессором не ниже 1,2 Ггц и 256 Мб оперативной памяти без операционной системы (7 шт.).

4) МФУ (1 шт.)

5) Выход в Интернет

6) Интерактивная доска (1 шт.)

**2.2. Формы аттестации**

***Формы проведения аттестации:*** защита проекта, соревнования различного уровня.

**Формы подведения итогов**:

- Практическая работа.

- Соревнования различного уровня.

**Способы определения результативности**

В образовательном процессе для диагностики успешности освоения учебной программы используются:

- метод наблюдения;

- метод анализа продуктов образовательной деятельности обучающегося.

**Виды контроля:**

- предварительный: опрос;

- практическая работа по созданию защищенного аккаунта в социальной  
сети;

- текущий: конкурсы внутри объединения, дискуссии;

- итоговый: Настройка операционной системы для защиты от различных вредоносных программ.

**Формы диагностики:**

1. Промежуточная диагностика, проводится по завершении полугодия или года обучения (при переводе на следующий учебный год).

2. Итоговая диагностика, проводится после завершения всей учебной программы.

Предметом оценки служат умения и знания, направлены на формирование общих и профессиональных компетенций.

Оперативный контроль учебных достижений осуществляется на протяжении всех занятий и имеет своей целью оценку систематичности учебной работы обучающихся по формированию знаний и умений в рамках освоения данного материала. Проводится в процессе устного опроса, проведения практических работ, выполнения индивидуальных заданий и т.п.

***Задачи текущего контроля:***

- повышение мотивации обучающихся к регулярной учебной работе;

- развитие навыков самостоятельной работы;

- обеспечение обратной связи между обучающимися и преподавателем, на основании которой устанавливается, как обучающиеся воспринимают и усваивают учебный материал;

- дифференциация итоговой оценки знаний.

**2.3. Оценочные материалы**

**Формы подведения итогов**:

- Практическая работа.

- Соревнования различного уровня.

**Способы определения результативности.**

В образовательном процессе для диагностики успешности освоения учебной программы используются:

- метод наблюдения;

- метод анализа продуктов образовательной деятельности обучающегося.

**Виды контроля**

- предварительный: опрос;

- практическая работа по созданию защищенного аккаунта в социальной  
сети;

текущий: конкурсы внутри объединения, дискуссии;

- итоговый: Настройка операционной системы для защиты от различных вредоносных программ.

**Формы диагностики:**

1. Промежуточная диагностика, проводится по завершении полугодия или года обучения (при переводе на следующий учебный год).

2. Итоговая диагностика, проводится после завершения всей учебной программы.

Предметом оценки служат умения и знания, направлены на формирование

Общих и профессиональных компетенций.

Оперативный контроль учебных достижений осуществляется на протяжении всех занятий и имеет своей целью оценку систематичности учебной работы обучающихся по формированию знаний и умений в рамках освоения данного материала. Проводится в процессе устного опроса, проведения практических работ, выполнения индивидуальных заданий и т.п.

**Задачи текущего контроля:**

- повышение мотивации обучающихся к регулярной учебной работе;

- развитие навыков самостоятельной работы;

- обеспечение обратной связи между обучающимися и преподавателем, на основании которой устанавливается, как обучающиеся воспринимают и усваивают учебный материал;

- дифференциация итоговой оценки знаний.

**Критерии оценивания практической работы:**

**-** Полнота выполненных заданий учеником.

**-** Понимание для какой цели существует каждое задание.

**-** Степень самостоятельности выполнения итоговой работы.

**2.4. Методические материалы**

Учебно-наглядные пособия:

- стенды со справочным материалом;

- презентации к лекционному материалу;

- учебные и методические пособия (учебники, учебно-методические пособия, пособия для самостоятельной работы, сборники упражнений и др.).

**Приложение**

**Оценочные материалы**

**Тест по технике безопасности**

Каждый правильный ответ оценивается в 1 балл. **Выберите один вариант ответа.**

**Общие правила поведения и ТБ в кабинете**

**1. Перед началом работы в кабинете информатики необходимо:**

1) оставить вещи, не требующиеся во время урока, в специально отведенном месте, пройти на своё рабочее место, включить персональный компьютер и дожидаться указаний учителя

2) пройти на рабочее место, включить компьютер и дожидаться указаний учителя

3) оставить вещи, не требующиеся во время урока, в специально отведенном месте, пройти на своё рабочее место и дожидаться указаний учителя

**2. Можно ли приносить в кабинет продукты питания и напитки?**

1) нет

2) да, только в том случае, если сильно хочется, есть или пить

3) да

**3. Что можно делать обучающемуся в компьютерном классе только с разрешения педагога?**

1) сдвигать с места монитор и/или системный блок

2) устанавливать или удалять программы на компьютер

3) отключать и подключать устройства к компьютеру

**4. При появлении запаха гари или странного звука обучающимся необходимо:**

1) продолжить работу за компьютером

2) сообщить об этом учителю

3) немедленно покинуть класс

**5. В случае пожара необходимо:**

1) прекратить работу, под руководством учителя покинуть кабинет

2) немедленно покинуть компьютерный класс

3) выключить компьютер и покинуть здание

**6. Какие из перечисленных действий не запрещаются в кабинете?**

1) отключать и подключать устройства к компьютеру

2) вставать со своих рабочих мест во время работы, чтобы поприветствовать учителя

3) работать двум обучающимся за одним компьютером

**7. Сколько обучающихся допускаются одновременно к работе за одним компьютером?**

1) двое

2) трое

3) один

4) четыре

**8. Какие действия не запрещены правилами поведения в кабинете?**

1) пройти в кабинет без обуви

2) работать с влажными или грязными руками

3) отключать и подключать кабели, трогать соединительные разъёмы проводов

**II. Правила работы за компьютером**

**9. Можно ли перезагружать ПК во время работы на уроке?**

1) да, если это необходимо

2) можно, но только с разрешения учителя

3) нет

**10. Если персональный компьютер не включается, необходимо:**

1) проверить питание

2) проверить переключатели

3) сообщить учителю

**11. Можно ли выключать ПК по окончании работы на занятии?**

1) да, при необходимости

2) да

3) нет

**12. Какие компьютерные программы можно запускать обучающимся во время урока?**

1) любые

2) только те, которые вам разрешил запустить учитель во время урока

3) только те, которые изучали раньше

**13. Что делать если не работает клавиатура или мышка?**

1) проверить, подключено ли устройство к ПК

2) перезагрузить ПК

3) сообщить учителю

**14. Что нужно сделать по окончании работы за ПК?**

1) привести в порядок рабочее место, закрыть окна всех программ, задвинуть кресло, сдать учителю все материалы, при необходимости выключить ПК

2) покинуть кабинет

3) выключить компьютер

**III. Сохранение здоровья при работе за компьютером**

**15. Можно ли работать за компьютером при плохом самочувствии?**

1) нет

2) да, если разрешил учитель

3) да

**Правильные ответы**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № вопроса | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| ответ | 3 | 1 | 2 | 2 | 1 | 2 | 3 | 3 | 2 | 3 | 1 | 2 | 3 | 1 | 1 |

**Список литературы для педагога**

1. Бабаш, А.В. Информационная безопасность: Лабораторный практикум/ А.В.Бабаш, Е.К.Баранова, Ю.Н.Мельников. - Москва: КноРус, 2019. - 432 c.

2. Воеводин В.А., Хорев А.А. Аудит информационной безопасности автоматизированных систем: учебное пособие/ В.А.Воеводин, А.А.Хорев; под редакцией А.А.Хорева Министерство науки и высшего образования Российской Федерации, Национальный исследовательский университет «МИЭТ». - Москва: МИЭТ, 2021. - 208 с.

**Список литературы для обучающихся**

3. Наместникова, М.С. Информационная безопасность, или на расстоянии одного вируса. 7-9 классы. Учебное пособие. ФГОС/ М.С.Наместникова. – Москва: Просвещение, 2019. – 80 с.

4. Солдатова, Г.У. Тренажер по курсу «Кибербезопасность». 6 класс/ Г.У.Солдатова, И.Д.Пермякова, С.В.Чигарькова. – Москва: Русское слово, 2019. – 56 с.

5. Цветкова, М.С. Информационная безопасность. Кибербезопасность. 7–9 классы: учебное пособие /М.С.Цветкова, И.Ю.Хлобыстова. - 2-е изд., пересмотр. - Москва: БИНОМ. Лаборатория знаний, 2020. - 64 с.:

6. Цветкова, М.С. Информационная безопасность. Правовые основы информационной безопасности.10–11 классы: учебное пособие/ М.С.Цветкова и др.; под ред. М.С.Цветковой. - М.: БИНОМ. Лаборатория знаний, 2020. - 112 с.

7. Цифровой ликбез от Благотворительного фонда Сбербанка «Вклад в будущее». - https://digital-likbez.datalesson.ru/

**Список литературы для родителей**

8. Антипова, А.В. Формирование у младшего школьника навыка безопасного пользования информационными ресурсами и средствами/ А.В.Антипова// Социальные отношения. – 2021. – № 2(37). – С.43-53

9. Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов/ Е.В. Вострецова. - Екатеринбург: Изд-во Урал. ун-та, 2019. - 204 с.

10. Стародубцева, Г.А. Информационная безопасность детей дошкольного возраста как ресурс позитивной социализации: метод. пособие/ авт.- сост. Г.А.Стародубцева – Иркутск: Изд-во ГАУ ДПО ИРО, 2015. – 23 с.