

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ

РЯЗАНСКОЙ ОБЛАСТИ

**Областное государственное автономное учреждение**

**дополнительного образования «Центр цифрового образования»**

|  |  |  |
| --- | --- | --- |
| **РЕКОМЕНДОВАНО**Заседание педагогического совета ОГАУ ДО «ЦЦО «ИТ-куб»Протокол № \_\_\_ от «\_\_\_» \_\_\_\_\_ 202 г.Председатель педагогического совета |  | **УТВЕРЖДАЮ**ДиректорОГАУ ДО «ЦЦО «ИТ-куб»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.И. ДоронинПриказ № от ------ |

**ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ**

**ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА**

**ТЕХНИЧЕСКОЙ НАПРАВЛЕННОСТИ**

**«Кибергигиена и работа с большими данными»**

 **базовый уровень**

|  |  |
| --- | --- |
| **Срок реализации:** | **6 месяцев** |
| **Общее количество часов:** | **72 часа** |
| **Количество часов в неделю:** | **4 часа** |
| **Возраст обучающихся:** | **11-17 лет** |
| **Автор-составитель:** | **Киселев Евгений Витальевич** |

Рязань

2021

Пояснительная записка

В профессиональном сообществе людей, чья деятельность тем или иным образом связана с информационной безопасностью, все чаще стал звучать термин «кибергигиена». Какой смысл вкладывается в это понятие? Говоря о кибергигиене, в первую очередь подразумевают соблюдение элементарных основ цифровой безопасности при работе с интернетом, ставшим неотъемлемой частью нашей жизни. И проводят параллель с известными нам правилами личной гигиены. Тем самым подчеркивается, с одной стороны, элементарность правил кибергигиены, с другой — необходимость восприятия этих правил на уровне повседневной привычки.

В ситуации стремительного перехода информации в цифровую форму каждому из нас крайне важно соблюдать набор правил кибербезопасности — это основа нашей безопасности в мире информационных технологий

Все слышали о свирепствовавших в прошлом эпидемиях чумы, холеры и других заразных заболеваний. Основной причиной их распространения было несоблюдение гигиены. Повсеместная грязь, контакты с больными, крысы-разносчики — всё это приводило к чудовищным последствиям. В XXI веке мы должны говорить уже не о простой гигиене, а о кибергигиене. В это понятие входит и использование сложных для подбора паролей, и умение распознать фишинговое письмо, и аккуратность в отношении незнакомых ссылок. Вопреки заблуждениям, кибергигиена не элементарна и порой требует целого курса обучения.

Это общий термин для обозначения инструментов и методов, направленных на защиту устройств от вредоносных и шпионских программ, а также вирусов в сети Интернет.

Кроме того, кибергигиена включает в себя все действия, необходимые для предотвращения попадания ваших личных данных в сеть.
Кибергигиена тесно связана с кибербезопасностью. Это не основная область, в отличие от кибербезопасности, где используется [ВПН](https://le-vpn.com/ru/vpn-service-information/). Но несмотря на это, его ценность нельзя отрицать. Использование подобных инструментов сделает процесс чистки намного проще.

Основная идея кибергигиены заключается в том, чтобы не допускать чрезмерного обмена информацией. В эпоху, когда и общество, и компании испытывают искушение «выйти в люди», очень важно обеспечить сохранность личных данных. Вся информация, которую вы предоставляете, должна быть либо неполной, либо вымышленной.

 «Крибрум» — это система мониторинга и анализа социальных медиа для управления репутацией в интернете.

Дополнительная общеобразовательная программа разработана на основе рабочей программы по направлению «Кибергигиена» (разработчики программы: Говор Светлана Александровна, Теделури Мария Михайловна, Шулаева Оксана Вячеславовна)

***Актуальность и практическая значимость образовательной программы***

Программа «Кибергигиена и работа с большими данными» поможет освоить азы интернет-безопасности и этикета в сети, ребята научатся быстро и эффективно искать информацию в глобальной сети, анализировать группы в социальных сетях, освоят основы защиты персональных данных. Программа носит междисциплинарный характер и позволяет решить задачи развития у учащихся научно-исследовательских, технико-технологических и гуманитарных компетенций.

Ключевые навыки, приобретаемые в ходе освоения образовательной программы, компетенции Hard Skills и Soft Skills, подразумевает получение ряда базовых компетенций.

***Отличительные особенности и новизна образовательной программы***

Новизна программы заключается в использовании инструментов и методов, созданных за последние два года для изучения быстро меняющегося интернет-пространства. Система мониторинга и анализа социальных медиа («Крибрум») впервые используется для обучения детей школьного возраста.

Данная программа может стать толчком к раскрытию личности и творческого потенциала ребенка, т.к. не загоняет его в конкретные рамки, а навыки групповой и проектной работы будут способствовать самореализации обучающегося, и помогут ему лучше адаптироваться в современном мире.

**Адресат программы**

Образовательная программа рассчитана на обучающихся в возрасте от 11-17 лет (5 - 11 класс). Предусмотрено разделение обучающихся на группы. Группа с нулевым уровнем и группа с начальным уровнем.Определяющим фактором при разделении является уровень входных компетенций. Набор в группы – свободный (без предъявления дополнительных требований к уровню входных компетенций). Рекомендуемое количество обучающихся в группе от 8 до 12 человек.

**Формы обучения**

В ходе реализации образовательной программы рекомендуется использовать следующие формы занятий:

* на этапе изучения нового материала – лекция, объяснение, рассказ, демонстрация;
* на этапе закрепления изученного материала - беседа, дискуссия, практическая работа, дидактическая;
* на этапе повторения изученного материала –творческое задание;
* на этапе проверки полученных знаний – выполнение индивидуальных или групповых кейсов, публичное выступление с демонстрацией результатов работы над образовательным модулем.

Реализация образовательной программы предусматривает проведения занятий следующих форм: беседа, круглый стол, демонстрации, объяснение, практическая работа на компьютере, самостоятельная работа, ролевые и деловые игры, проектная деятельность, консультация, групповые работы, проектная деятельность.

Образовательная программа предполагает возможность организации и проведения с обучающимися культурно-массовых мероприятия в том числе:

* конкурсы;
* мастер-классы;
* открытые занятия;
* выставки.

При реализации образовательной программы применяются активные методы обучения такие, как:

* метод проектов (методика проектной деятельности);
* кейс метод (методика проблемного обучения).

**Режим занятий**

Занятия проводятся по два в неделю. Каждое занятие по два часа.

**Объем и срок реализации**

Программа рассчитана на первое полугодие 2021 года из расчета 72 часа (два раза в неделю по 2 часа).

Цель образовательной программы

Цель программы **-** обучить приемам и методам самостоятельного анализа и оценки информации в интернет-пространстве в контексте личной психологической безопасности.

**Задачи образовательной программы.**

**Личностные:**

* сформировать устойчивый интерес к правилам здоровье сберегающего и безопасного поведения;
* сформировать умение проявлять в самостоятельной деятельности вале логическую культуру и компетентность;
* развить аналитическое, практическое и логическое мышление;
* развить самостоятельность и самоорганизацию;
* развить умение работать в команде, развить коммуникативные навыки;
* сформировать умение вести себя сдержанно и спокойно.

**Развивающие:**

* развить творческую активность;
* развить умение представлять результаты своей работы окружающим, аргументировать свою позицию;
* развить познавательную активность.

**Социальные:**

* сформировать умение пользоваться приемами коллективного творчества;
* сформировать умение эстетического восприятия мира и доброе отношение к окружающим.

**Регулятивные:**

* сформировать умение соотносить свои действия с планируемыми результатами, осуществлять контроль своей деятельности в процессе достижения результата;
* сформировать умение определять способы действий в рамках предложенных условий и требований, корректировать свои действия в соответствии с изменяющейся ситуацией.

**Предметные:**

* владеть основными приемами работы в прикладных программах для обработки информации;
* сформировать представление о структуре и типах информации в интернет-пространстве, больших данных и больших пользовательских данных;
* познакомить с методами и средствами поиска информации в интернет-пространстве;
* сформировать навыки планирования, проведения и обработки результатов исследования информации в интернет-пространстве при помощи поисковых систем, общедоступных средств поиска информации и системы мониторинга и анализа социальных медиа «Крибрум»;
* сформировать у учащихся способность выявлять и критически оценивать источники и каналы распространения информации в интернет-пространстве и определять ее качество;
* сформировать способность определять социальные характеристики и индивидуальные особенности людей и обнаруживать признаки опасного поведения на основании их аккаунтов в социальных сетях;
* сформировать способность к успешной самопрезентации и формированию позитивного имиджа в социальных сетях;
* сформировать у учащихся способность распознавать опасный и вредный контент и идентифицировать явления манипулирования сознанием в интернет-пространстве, внушения деструктивных идей и вовлечения в социально опасные группы в социальных сетях;
* обучить приемам противодействия негативным воздействиям в интернет пространстве;
* сформировать культуру позитивного использования интернет-пространства.

**Учебный план**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование модуля** | **Количество часов** | *Виды и формы контроля* |
| ***Всего*** | ***Теория*** | ***Практическая подготовка*** |
| 1. | **Распознавание опасного и вредного контента в интернет-пространстве. Безопасное поведение в сети.** | 20 | 14 | 6 | текущий |
| 2 | **Угрозы в интернет-пространстве, методы противодействия.**  | 8 | 6 | 2 | текущий |
| 3 | **Безопасность мобильных устройств** | 10 | 7 | 3 | текущий |
| 4 | **Угрозы безопасности в сетях WiFi. Онлайн сервисы безопасности.**  | 14 | 10 | 4 | текущий |
| 5 | **Обработка и анализ больших данных. Основные принципы построения нейросетей.** | 12 | 9 | 3 | текущий |
| 6 | **Проектная деятельность** | 8 | - | 8 | Защита проекта |
|  | Итого | 72 | 46 | 26 |  |

Содержание учебного плана

Структура программы основа на модульном принципе.

**Модуль 1. Распознавание опасного и вредного контента в интернет-пространстве. Безопасное поведение в сети.**

Теория: ааспознавание опасного контента (деструктивные группы в социальных медиа, вовлечение в опасные виды деятельности), интернет зависимость и ее признаки, сетевые игры. Изучение противодействия угрозам интернет-пространства.

Практическая подготовка: составление правил взаимодействия со злоумышленниками. Анализ собственной интернет зависимости и составление правил минимизации рисков манипулирования через сеть.

**Модуль 2. Угрозы в интернет-пространстве, методы противодействия.**

Теория: Кибертерроризм и кибершпионаж, кибероружие. Борьба с использованием интернета в террористических, сепаратистских и экстремистских целях.

Практическая подготовка: проверка сетевых ресурсов (группы в ВК, сайты, форумы и т.п.), посещаемых учениками, на наличие террористических, сепаратистских и экстремистских материалов. Составление памятки по выявлению подобных угроз.

**Модуль 3. Безопасность мобильных устройств.**

Теория: Источники заражения мобильных устройств, угрозы для Android-устройств и IOS-устройств, вредоносное ПО для смартфонов и методы борьбы с ним.

Практическая подготовка: проверка на безопасность различных приложений, установка, удаление. Работа с антивирусом на мобильном телефоне.

**Модуль 4. Угрозы безопасности в сетях WiFi. Онлайн сервисы безопасности.**

Теория: устройство Wi-Fi сетей, угрозы безопасности и методы защиты Wi-Fi сетей, сервисы для проверки безопасности пользователя.

Практическая подготовка: использование сервисов для проверки безопасности пользователя, проверка сети Wi-Fi ИТ-куба на наличие уязвимостей.

**Модуль 5. Обработка и анализ больших данных. Основные принципы построения нейросетей.**

Теория: определение больших данных, сферы применения и перспективы. Анализ и визуализация данных. Машинное обучение и принципы построения нейросетей, нейрокомпьютеры. Методы шифрования данных.

Практическая подготовка: шифрование и дешифровка, с использованием различных методов (Атбаш, диск Энея, шифр Цезаря и др.)

**Проектная деятельность**

Практическая подготовка: Самостоятельный выбор учащимися тем проектов, разработка плана работы для его реализации.

Подготовка плана работы для реализации программы, поиск информации, патентный поиск, побор литературы, подготовка работ для участия в различных конкурсах и мероприятиях.

**Итоговое занятие**

Презентация проектных работ.

# **Календарный учебный график**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Тема** | **Кол-во часов** | **Характеристика деятельности учащихся** |
| Модуль 1. Распознавание опасного и вредного контента в интернет-пространстве. Безопасное поведение в сети. | 20 | Изучение,обсуждение |
| 1 | Деструктивное воздействие в социальных медиа | 2 |  |
| 2 | Деструктивные группы | 2 |  |
| 3 | Персональная информация пользователя, как она может быть использована злоумышленниками | 2 |  |
| 4 | Правила безопасного обращения с персональными данными в социальных медиа | 2 |  |
| 5 | Правила взаимодействия со злоумышленниками. Что делать, если ваши персональные данные похищены | 2 |  |
| 6 | Урон репутации и правонарушения в сети | 2 |  |
| 7 | Сетевые игры: польза и вред. (Сетевые игры как массовые развлечения. Бесплатные и платные игры. Для чего может быть полезен ПК и Интернет и как польза превращается во вред.) | 2 |  |
| 8 | Понятие интернет-зависимости, компьютерной зависимости и причин их возникновения.Интернет-сообщество. Зависимость от интернет-общения. Виртуальная личность. | 2 |  |
| 9 | Развлечения в Интернет. Признаки зависимости. Сайты знакомств. Управление личностью через сеть. Киберкультура и личность.Типы интернет-зависимости. | 2 |  |
| 10 | Представление результатов проделанной работы. | 2 |  |
| Модуль 2. Угрозы в интернет-пространстве, методы противодействия. | 8 | Изучение,практика,обсуждение |
| 11 | Киберугрозы Интернета. Кибертерроризм и кибервойны. | 2 |  |
| 12 | Кибершпионаж. Кибероружие. | 2 |  |
| 13 | Борьба с использованием Интернета в террористических, сепаратистских и экстремистских целях. Интернет как оружие массового поражения. | 2 |  |
| 14 | Представление результатов проделанной работы. | 2 |  |
| Модуль 3. Безопасность мобильных устройств | 10 | Изучение,практика,обсуждение |
| 15 | Безопасность мобильных устройств в информационных системах. | 2 |  |
| 16 | Источники заражения мобильных устройств. | 2 |  |
| 17 | Угрозы для IOS-устройств. Угрозы для Android-устройств. | 2 |  |
| 18 | Рост числа угроз для мобильных устройств. Вирусы для мобильных устройств. | 2 |  |
| 19 | Представление результатов проделанной работы. | 2 |  |
| Модуль 4. Угрозы безопасности в сетях WiFi. Онлайн сервисы безопасности. | 14 | Изучение,практика,обсуждение |
| 20 | Общие понятия об устройстве WiFi-сетей | 2 |  |
| 21 | Угрозы безопасности WiFi-сетей | 2 |  |
| 22 | Сниффинг | 2 |  |
| 23 | Методы защиты сетей WiFi. Меры безопасности для пользователя WiFi. | 2 |  |
| 24 | Настройка безопасности сетей WiFi | 2 |  |
| 25 | Онлайн сервисы для безопасности пользователя в интернете. | 2 |  |
| 26 | Представление результатов проделанной работы. | 2 |  |
| Модуль 5. Обработка и анализ больших данных. Основные принципы построения нейросетей | 12 | Изучение,практика,обсуждение |
| 27 | Определение больших данных, характеристики, сферы применения. | 2 |  |
| 28 | Процесс анализа. Общая схема анализа. Извлечение и визуализация данных. | 2 |  |
| 29 | Реальное применение и перспективы использования технологии BIG DATA. | 2 |  |
| 30 | Принципы машинного обучения. Основы построения нейросетей. | 2 |  |
| 31 | Место нейрокомпьютеров в современных информационных технологиях. | 2 |  |
| 32 | Основы криптографии | 2 |  |
| 33-35 | Проектная деятельность | 6 | Демонстрацияпроектов |
| 36 | Итоговое занятие | 2 | Подведение итогов |
|  |  | 72 |  |

Планируемые результаты обучения

Hard Skills:

• научиться понимать структуру интернет-пространства;

• научиться работать с поисковыми системами, общедоступными средствами поиска информации в интернет-пространстве;

• научиться выявлять признаки рискованного и опасного поведения и различных угроз в интернет-пространстве (фишинг, мошенничество, вовлечение в опасные виды деятельности), уметь идентифицировать их в социальных сетях;

• сформировать понимание и принятие правил безопасного поведения в интернет-пространстве, рационального использования персональных данных, защиты от вредоносных воздействий;

• знать типы источников информации и разновидности контента;

• уметь использовать антивирусное ПО для защиты от вредоносных программ;

• уметь составить план, разбивая задачу на подзадачи. Самостоятельно планировать и реализовать проект.

• тестируют проект и дорабатывают с учётом обратной связи.

Soft Skills:

• научить свободно ориентироваться в интернет-пространстве, использовать различные типы источников для решения научно-исследовательских задач;

• знать правила безопасной работы на компьютере;

• научить ставить цели, планировать свою работу и следовать намеченному плану, критически оценивать достигнутые результаты;

• научить представлять результаты своей работы окружающим, аргументировать свою позицию;

• научить особенностям работы в группе;

• научатся проектировать и создавать собственные проекты;

• способы планирования деятельности, разбиения задач на подзадачи, распределения ролей в рабочей группе.

**Формы аттестации**

Аттестация учащихся – неотъемлемая часть образовательного процесса, позволяющая всем его участникам оценить реальную результативность совместной научно-технической и творческой деятельности.

Аттестация учащихся проводится в соответствии с критериями оценки по результатам предварительной и промежуточной аттестации оформляется протокол.

**Средства контроля** – устный опрос, соответствие созданной модели определенной тематике, тестирование, проверка творческих проектов.

**Формы подведения итогов реализации программы** – итоговая творческая работа (проект) с последующей защитой.

Требования к проекту - необходимо выполнить работу по следующей номинации: инструкция по использованию безопасного Интернета. Работа должна быть выполнена с использованием свободного программного обеспечения для создания готового продукта: брошюра; учебное пособие; наглядный материал и т.д.

Условия реализации программы

Материально-техническое обеспечение дополнительной общеобразовательной программы по направлению «Кибергигиена и работа с большими данными».

Занятия в помещении, оснащенном ПК для обучающихся и педагога. В процессе занятий используется оборудование, необходимое для занятий.

Особое внимание уделяется соблюдению техники безопасности при работе. Не завершенные работы обучающихся сохраняют на ПК.

**Аппаратное обеспечение и оборудование**

| **№****п/п** | **Наименование** | **Требуемое количество** |
| --- | --- | --- |
| 1. | Персональные компьютеры с выходом в интернет | 12+1 для преподавателя |
| 2. | Интерактивная доска или экран  | 1 |
| 3. | Маркерная доска, магнитная доска(магниты) | 1 |
| 4. | МФУ | 1 |

**Программное обеспечение**

| **№****п/п** | **Наименование** | **Требуемое количество** |
| --- | --- | --- |
| 1. | Офисное программное обеспечение | По количеству ПК |
|  |  |  |

**Расходные материалы**

| **№****п/п** | **Наименование** | **Требуемое количество** |
| --- | --- | --- |
| 1. | Бумага для рисования и распечатки | 1 упаковка |
| 2. | Маркеры для доски | 4 цвета (по 2 шт) |
|  |  |  |

**Учебно-методическое и информационное обеспечение**

**1. Методические материалы:**

1. Говор С.А., Теделури М.М., Шулаева О.В. Рабочая программа по направлению «Кибергигиена». – Москва, 2019 г.

2. Методическое пособие по направлению «Dataквантум». – Москва, 2018 г.

**2. Основная литература:**

1. Богачева Т.Ю., Соболева А.Н., Соколова А.А. Риски интернет пространства для здоровья подростков и пути их минимизации // Наука для образования: Коллективная монография. М.: АНО «ЦНПРО», 2015.

2. Ефимова Л.Л., Кочерга С.А. Информационная безопасность детей: российский и зарубежный опыт: Монография. М.: ЮНИТИ-ДАНА, 2013.

3. Солдатова Г., Зотова Е., Лебешева М., Вляпников В. Интернет: возможности, компетенции, безопасность. Методическое пособие для работников системы общего образования. Ч. 1. Лекции. М.: Google, 2013.

4. Революция в аналитике. Как в эпоху Big Data улучшить ваш бизнес с помощью операционной аналитики | Фрэнкс Билл, 2020.

**3. Дополнительная литература:**

1. Горошко Е.И. Современная Интернет-коммуникация: структура и основные параметры // Интернет-коммуникация как новая речевая формация: коллективная монография / науч. ред. Т. Н. Колокольцева, О.В. Лутовинова. М.: Флинта: Наука, 2012.

2. Крупник А.Б. Поиск в Интернете: самоучитель. СПБ.: Питер, 2004.

3. Солдатова Г.У., Рассказова Е.И., Зотова Е.Ю. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования. М.: Фонд Развития Интернет, 2013.

**4. Интернет-ресурсы:**

1. Официальный сайт Kaspersky https://www.kaspersky.ru