ШКОЛА 800

Автономная некоммерческая общеобразовательная организация «Школа 800»

РАБОЧАЯ ПРОГРАММА

учебного курса

«Основы информационной безопасности»

Нижний Новгород, 2025

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Исследование проблемы безопасности детей и подростков в сети Интернет последние годы является особенно актуальным, в связи с бурным развитием IT- технологий и со свободным использованием детьми и подростками современных информационно - коммуникационных технологий.

Программа разработана в связи с возросшей потребностью обеспечения информационной безопасности детей и подростков при организации урочной и внеурочной деятельности.

Программа разработана с учетом требований законов Российской Федерации: «Об образовании в Российской Федерации», «О защите детей от информации, причиняющей вред их здоровью и развитию» и «Санитарно-эпидемиологических требований к условиям и организации обучения в общеобразовательных учреждениях» и "Санитарно - эпидемиологических требований к устройству, содержанию и организации режима работы образовательных организаций дополнительного образования детей".

В требованиях ФГОС к предметным результатам освоения курса информатики отсутствует предметная область «Основы безопасности в Интернете», но в рамках метапредметных результатов и предметных умений дисциплины «Информатика» вопросы информационной безопасности обозначены.

ЦЕЛИ ИЗУЧЕНИЯ КУРСА

Цель программы: формирование у обучающегося правовой грамотности по вопросам информационной безопасности, которые влияют на социализацию в информационном обществе, формирование личностных и метапредметных результатов обучения и воспитания детей.

Задачи обучения:

Формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как человеческая жизнь, свобода, равноправие и достоинство людей, здоровье, опыт гуманных, уважительных отношений с окружающими;

Создавать педагогические условия для формирования правовой и информационной культуры обучающихся, развития у них критического отношения к информации, ответственности за поведение в сети Интернет и

последствий деструктивных действий, формирования мотивации к познавательной, а не игровой деятельности, воспитания отказа от пустого времяпрепровождения в социальных сетях, осознания ценности живого чело веческого общения;

Формировать отрицательное отношение ко всем проявлениям жестокости, насилия, нарушения прав личности, экстремизма во всех его формах в сети Интернет;

Мотивировать обучающихся к осознанному поведению на основе понимания и принятия ими морально правовых регуляторов жизни общества и государства в условиях цифрового мира;

Научить молодых людей осознавать важность проектирования своей жизни и будущего своей страны — России в условиях развития цифрового мира, осознавать ценность ИКТ для достижения высоких требований к обучению профессиям будущего в мире, принимать средства в Интернете как среду созидания, а не разрушения человека и общества.

Данная программа составлена на основе курса «Информационная безопасность. Кибербезопасность» для общеобразовательных организаций авторов Цветкова М.С, Хлобыстова И.Ю, переработана и модифицирована.

Содержание программного материала этих тем, как в теории, так и на практических занятиях составлено с учётом возрастных особенностей обучающихся, весь материал построен по принципу от простого к сложному.

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.

МЕСТО КУРСА В УЧЕБНОМ ПЛАНЕ

Курс «Кибербезопасность» разработан для учащихся 5–9 классов и предлагается к изучению как учебный предмет входящий в часть учебного плана, формируемой участниками образовательных отношений. Курс рассчитан на 34 часа и может реализоваться по 11 часов в качестве внеурочного модуля в 5, 6, 7, 8 и 9 классах, или как одногодичный курс в 5 или в 6 классах.

СОДЕРЖАНИЕ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Курс для школьников 5–9 классов отражает особенности современного цифрового мира как киберпространства, насыщенного сетевыми сервисами и интернеткоммуникациями, доступными детям, в том числе негативной направленности: закрытые сетевые сообщества неизвестного толка, опасные группы, негативные контакты, навязчивые интернет ресурсы (спам, реклама, азартные игровые сервисы), сайты, содержащие негативный и агрессивный контент, в том числе противоправные материалы, влекущие ответственность по законам Российской Федерации,сетевые средства вмешательства в личное информационное пространство на персональных устройствах, работающих в Интернете, использование детьми электронных социальных/банковских карт, имеющих персональные настройки доступа к ним.

Все это резко повышает потребность в воспитании у учащихся культуры информационной безопасности с одной стороны и профориентации в мире профессий будущего — с другой, а также популяризации полезных интернет ресурсов.

«Информационные войны» в глобальном цифровом пространстве породили новые угрозы для общества — кража персональных данных, призывы к агрессии и террору, склонение к насилию, суициду. С учетом последних тенденций, названных «фейковые новости», в киберпространстве появились: навязчивый ложный контент деструктивного, очерняющего людей и события содержания, пропаганда наркотических средств под видом ложной информации о продукции, в том числе распространяемый автоматически, ложные новости и постановочные репортажи. Навыки обдуманного поведения при поиске информации в сети Интернет, критического анализа полученной информации, умения работать с информацией избирательно и ответственно, знакомство с профессиями в сфере информационной безопасности — это важная часть современной цифровой грамотности школьников 7–9 классов, которая востребована в жизни и учебе при работе в сети Интернет, социальных сетях и мессенджерах.

Проникновение мобильных устройств с доступом к Интернету в быт и досуг детей обострило проблему интернет зависимости, игромании, зависимости от социальных сетей, необоснованного доверия посторонним людям в сети, и как следствие, незащищенности детей от атак мошенников, преступников, агрессивно настроенных людей, включая вовлечение детей в теневые, закрытые субкультуры, несу щие угрозу здоровью и даже жизни ребенка. При этом в сети Интернет есть много позитивного контента, СМИ, позволяющих получать информацию о профессиях будущего, использованию

цифровых технологий в быту на основе «умных» технологий, направлениях развития современного киберискусства, использования Интернета для электронного обучения и др.

Все это потребовало расширить тему информационной безопасности в сети Интернет для школьников 7–9 классов такими понятиями, как:

- киберагент,
- кибермир,
- киберискусство,
- киберобщество,
- киберугорозы,
- кибератака,
- киберпреступность

Важную часть практического содержания курса составляет выполнение заданий по информационной безопасности с использованием сети Интернет, ознакомление с позитивным контентом познавательного, учебного и развивающего назначения, выполнение практической работы, предложенной в открытых практикумах ИТ-компаний и операторов мобильной телефонии для разных возрастных групп учащихся (практикумы встроены к содержание модулей курса).

Содержание программы

№ п/п	Модуль	Часы
1	Киберпространство	11
2	Киберкультура	11
3	Киберугрозы	12

ПЛАНИРУЕМЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

Личностные результаты:

- осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям,

взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;

- готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений с учётом устойчивых познавательных интересов;
- освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
- сформированность ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Метапредметные результаты:

- Освоение социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах, включая взрослые и социальные сообщества; участие в школьном самоуправлении и общественной жизни в пределах возрастных компетенций с учетом региональных, этнокультурных, социальных и экономических особенностей;
- Формирование коммуникативной компетентности в общении и сотрудничестве со сверстниками, детьми старшего и младшего возраста, взрослыми в процессе образовательной, общественно полезной, учебноисследовательской, творческой и других видов деятельности;
- Умение использовать средства информационных и коммуникационных технологий (далее — ИКТ) в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности.

Предметные результаты:

- формирование основ правосознания для соотнесения собственного поведения и поступков других людей с нравственными ценностями и нормами поведения, установленными законодательством Российской Федерации;
- освоение приемов работы с социально значимой информацией, ее осмысление; развитие способностей обучающихся делать необходимые выводы и давать обоснованные оценки социальным событиям и процессам;

- формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

Модуль	Разделы в учебном пособии	Вс часов	Теоретические занятия	Практическая работа с ресурсами и программами на компьютере
Модуль 1	дел 1. Киберпространство			
Киберпространство	Киберпространство. Кибермиры. Киберобщество. Киберденьги. Киберфизическая система. Кибермошенничество			
Практикум	Практическая работа на основе онлайн курса Академии Яндекс «Безопасность в Интернете» по теме «Безопасные онлайнплатежи».			
Модуль 2	Раздел 2. Киберкультура			

Киберкультура	Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство. Социальная инженерия. Классификация угроз социальной инженерии			
Практикум	Практическая работа от компаний мобильной связи Билайн, МТС и Мегафон (по выбору обучающегося)			
Модуль 3	Раздел 3. Киберугрозы			
Киберугрозы	Кибервойны. Киберпреступность. Примеры киберпреступлений.Уязвимости кибербезопасности.Угрозы информационной безопасности. Запрещенные и нежелательные сайты. Новые профессии в кибероббществ			

Практикум	Практическая работа на основе онлайн курса Академии Яндекса «Безопасность в Интернете» (продолжение), по темам: защита от вредоносных программ; безопасность аккаунтов			
Итого				

НАУЧНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОСВОЕНИЯ КУРСА

Список литературы

1. Цветкова М.С., Хлобыстова И.Ю. Информационная безопасность. Кибербезопасность. 7-9 класс, Бином. Лаборатория знаний, 2021, 279 с.
2. Бирюков А.А. Информационная безопасность защита и нападение 2 е издание: Издательство: ДМК-Пресс., 2017, 434 с.
3. Бирюков А.А. Информационная безопасность защита и нападение.: Издательство: ДМК-Пресс., 2018, 474 с.
4. Колесниченко Денис. Анонимность и безопасность в интернете. От чайника к пользователю. Самоучитель Издательство: БХВ-Петербург, 2018, 240с.
5. Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей: издательство: ЭКСМО, 2019, 256 с.
6. Мэйволд Э. Безопасность сетей (2-е изд.) Книги» Сетевые Технологии. Название: Безопасность сетей: Издательство: М.: НОУ "Интуит", 2020,571 с.
7. 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.
8. Проскурин В.Г Защита в операционных системах: Издательство: Горячая линия-Телеком, 2019, 192 с.

9. Савченко Е. Кто, как и зачем следит за вами через интернет: Москва - Третий Рим, 2019, 100 с.

10. Яковлев В.А.Шпионские и антишпионские штучки: Техническая литература Издательство: Наука и Техника, 2018, 320 с.

Материально-техническое обеспечение

- Персональный компьютер с предустановленным ПО
- Средство демонстрации изображения
- Доступ к широкополосной сети Интернет