ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 8
городского округа Чапаевск Самарской области

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
Ответственный УВР	Ответственный ВД	Директором школы
Горшенина Т. А.	Емельянова Е. Г.	Трясуновой А.А.
Приказ № 1	Приказ №1	Приказ №1
от «29» 08.2025г.	от «29» 08.2025г.	от «29» 08.2025г

.

ЭП

C=RU, S=Самарская область, STREET="ул. Советская, д.56", L=г.о. Чапаевск, T=И.О.ДИРЕКТОРА, O=ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 8 ГОРОДСКОГО ОКРУГА ЧАПАЕВСК САМАРСКОЙ ОБЛАСТИ, ОГРН=1116330005065, СНИЛС=00955869388, ИНН ЮЛ=6330050480, ИНН=633515748581, E=shkola08@yandex.ru, G=Алла Александровна, SN=Трясунова, CN=ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 8 ГОРОДСКОГО ОКРУГА ЧАПАЕВСК САМАРСКОЙ ОБЛАСТИ
2025-09-09 22:13:43

РАБОЧАЯ ПРОГРАММА
ВД «Информационная безопасность»
для обучающихся 7 классов

г.о. Чапаевск, 2025

Пояснительная записка

Актуальность данной программы определена тем, что она является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к
обеспечению своей личной безопасности, безопасности своей семьи и своих друзей. Кроме того, реализация программы создаст условия для сокращения цифрового разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт.

Программа реализует обще интеллектуальное направление во внеурочной деятельности.

Данная рабочая программа «Информационная безопасность» разработана на основе:

- примерной рабочей Программы учебного курса «Цифровая гигиена», рекомендованной координационным советом учебно- методических объединений в системе общего образования Самарской области (протокол № 27 от 21.08.2019)
- учебного пособия для общеобразовательных организаций «Информационная безопасность, или на расстоянии одного вируса» 7 – 9 классы. Внеурочная деятельность /М.С. Наместникова. –М.: Просвещение, 2019.

Цель программы:

обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз, формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Задачи программы:

- сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);
- создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно- телекоммуникационной среде;
- сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;
- сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников,

связанного с компьютерными технологиями и Интернетом.

Срок реализации программы – 1год.

Участники программы: обучающиеся 7-х классов.

Объем курса – 34 часа в год, что соответствует одному академическому часу в неделю при годовом учебном графике.

Место проведения: программа составлена с учетом санитарно-гигиенических требований, возрастных особенностей учащихся и рассчитана на работу в учебном компьютерном классе, в котором 20 учебных мест и одно рабочее место – для преподавателя.

Формы организации внеурочной деятельности: традиционный урок (коллективная и групповая формы работы), тренинги (в классической форме или по кейс- методу), дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микро- обучение), смешанный формат.

Необходимое оборудование:

1. Компьютерное учебное место: - 20 штук, для учителя - 1. Все компьютеры имеют выход в Интернет.
2. Мультимедиа проектор и экран.
4. Интерактивная доска SMART Board.
5. Принтер.
6. Сканер.
7. Доска.

Взаимосвязь с программой воспитания

Программа курса внеурочной деятельности «Информационная безопасность» разработана с учётом рекомендаций Примерной программы воспитания. Это позволяет на практике соединить обучающую и воспитательную деятельность педагога, ориентировать её не только на интеллектуальное, но и на нравственное, социальное развитие учащегося

Особенности работы педагога по программе

Задача педагога состоит в том, чтобы сопровождать процесс профессиональной ориентации школьника, раскрывая потенциал каждого через вовлечение в многообразную деятельность, организованную в разных формах При этом результатом работы педагога в первую очередь является личностное развитие учащегося Личностных результатов педагог может достичь, увлекая учащегося совместной и интересной им обоим деятельностью, устанавливая во время занятий доброжелательную, поддерживающую атмосферу, насыщая занятия ценностным содержанием

Планируемые результаты освоения учебного модуля «Информационная безопасность»

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 учетом устойчивых познавательных интересов;
- освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
- сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Предметные:

Ученик научится:

- анализировать доменные имена компьютеров и адреса документов в интернете;
- безопасно использовать средства коммуникации,
- безопасно вести и применять способы самозащиты при попытке мошенничества,
- безопасно использовать ресурсы интернета.

Ученик овладеет:

- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Ученик получит возможность овладеть:

- основами соблюдения норм информационной этики и права;
- основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;
- использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включаяИнтернет- ресурсы и другие базы данных.

Метапредметные результаты:

Регулятивные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- идентифицировать собственные проблемы и определять главную проблему;
- выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;
- ставить цель деятельности на основе определенной проблемы и существующих возможностей;
- выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
- составлять план решения проблемы (выполнения проекта, проведения исследования);
- описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения

практических задач определенного класса;

- оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;
- находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;
- работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
- принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- выделять явление из общего ряда других явлений;
- определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений;
- строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;
- излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
- самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;
- критически оценивать содержание и форму текста;

определять необходимые ключевые поисковые слова и запросы

Коммуникативные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- строить позитивные отношения в процессе учебной и познавательной деятельности;
- критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
- договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
- делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его.
- целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
- выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;
- использовать компьютерные технологии (включая выбор адекватных задаче инструментальных

программно-аппаратных средств и сервисов) для

- решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;
- использовать информацию с учетом этических и правовых норм;
- создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Содержание программы

Содержание программы учебного курса «**Информационная безопасность»** соответствует темам примерной основной образовательной программы основного общего образования (ПООП ООО) по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», а также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

Основное содержание программы представлено разделами ниже. Каждый раздел данного учебного курса завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста.

Система контролирующих материалов для оценки планируемых результатов. В течение всего курса обучения проводятся:

- ✓ конкурсы работ учащихся по созданию тематических презентаций, видеороликов;
- ✓ выставки лучших работ, выполненных в виде брошюр, листовок, буклетов, плакатов;
- ✓ защита промежуточных проектов

Основой для оценивания практической деятельности учеников выступают результаты анализа созданных ими проектов. Итоговый контроль осуществляется в конце всего курса. Он имеет форму зачета творческих работ.

Оценка выражается различными способами: устные суждения учителя, ведение протокола защиты проектов. Протокол может заполняться как учителем, так и учениками, кроме тех, кто выступает на данный момент. Затем подсчитывается сумма баллов и объявляется общий итог.

Оценка результативности учащихся осуществляется по следующим критериям:

- высокий уровень – успешное освоение учащимся более 70% содержания программы, подлежащего аттестации;
- средний уровень - успешное освоение учащимся от 50% до 70% содержания программы, подлежащего аттестации;
- низкий уровень – успешное освоение учащимся менее 50% содержания программы, подлежащего аттестации. Итоги аттестации фиксируются педагогом в журнале внеурочной деятельности.

Уровень развития у учащихся личностных качеств определяется на основе сравнения результатов их

диагностики в начале и конце курса.

Содержание учебного курса

Раздел 1. «Основы киберпространства»

Тема 1. Киберпространство. 1 час.

Киберпространство. Цифровая среда. Интернет. Сеть. Сервер. Виртуальный мир.

Тема 2. Виртуальная реальность. 1 час.

Виртуальная реальность. Дополнительная реальность. Иммерсивность. Цифровые двойники.

Тема 3. Кибермиры. 1 час.

Кибермиры, метавселенная, онлайн-сообщества, виртуальная экономика, аватар.

Тема 4. Управление дронами. 1 час.

Дрон, БПЛА, киберфизическая система, беспроводное управление, телеметрия.

Тема 5. Киберфизическая система. Искусственный интеллект. 1 час.

Искусственный интеллект (ИИ), машинное обучение, киберфизическая система, автоматизация, Big Data.

Раздел 2. «Цифровое общество и экономика»

Тема 6. Киберобщество. Соцсети. 1 час.

Киберобщество, социальные сети, цифровая идентичность, сетевой этикет, онлайн-сообщества.

Тема 7. Киберденьги. 1 час.

Киберденьги, электронные платежи, онлайн-банкинг, цифровой кошелек.

Тема 8. Криптовалюты. 1 час.

Криптовалюта, блокчейн, Биткоин, майнинг, децентрализация.

Тема 9. Кибермошенничество. 1 час.

Кибермошенничество, фишинг, вишинг, фарминг, мошеннические сайты.

Тема 10. Кибермошенничество. Документ Уголовный Кодекс РФ. 1 час.

Уголовный кодекс РФ, киберпреступность, статья 159 (мошенничество), статья 273 (создание вредоносных программ), правовая ответственность.

Тема 11. Киберкультура. 1 час

Киберкультура, интернет-мемы, цифровой фольклор, сленг, сетевая этика.

Раздел 3 «Информация и манипуляции»

Тема 12. От книги к гипертексту. 1 час.

Гипертекст, линейный текст, веб-страница, ссылка, навигация.

Тема 13. Киберкнига. 1 час.

Киберкнига, электронная книга, DRM, авторское право, цифровая библиотека.

Тема 14. Киберискусство. 1 час.

Цифровое искусство, NFT, генеративное искусство, цифровая живопись, медиаарт.

Тема 15-16. Социальная инженерия. 2 часа.

Социальная инженерия, манипуляция, психологические уловки, доверие, защита от манипуляций.

Тема 17. Угрозы социальной инженерии. Федеральный закон о персональных данных. 1 час.

Угрозы, персональные данные, 152-ФЗ, конфиденциальность, согласие на обработку ПДн.

Тема 18. Угрозы социальной инженерии. 1 час.

Телефонное мошенничество, фишинг, техподдержка, скимминг, претекстинг.

Тема 19. Новые профессии в кибероществе. 1 час.

Digital-профессии, SMM, таргетинг, контент-менеджер, SEO, копирайтер.

Тема 20. Цифровизация профессий. 1 час.

Цифровизация, IT в профессиях, дистанционные технологии, цифровые компетенции.

Раздел 4 «Киберугрозы и защита»

Тема 21. Киберугрозы. 1 час.

Киберугрозы, классификация угроз, вредоносное ПО, хакерская атака, ботнет.

Тема 22. Кибервойны. 1 час.

Кибервойна, кибероружие, критическая инфраструктура, государственная безопасность, хактивизм.

Тема 23. Киберпреступность. Примеры киберпреступлений. 1 час.

Киберпреступность, ransomware, DDoS-атака, кража данных, кибергруппировка.

Тема 24. Уязвимости кибербезопасности. Запрещенные и нежелательные сайты. 1 час.

Уязвимость, эксплойт, патч, фишинг-сайт, мошеннический сайт, запрещенный контент.

Тема 25-29. Защита от вредоносных программ и информационных атак. 5 часов.

Антивирус, фаервол, двухфакторная аутентификация, менеджер паролей, шифрование, бэкап.

Тема 30. Профессии, связанные с безопасностью в IT-сфере. 1 час.

Пентестер, этичный хакер, SOC-аналитик, криминалистика, специалист по ИБ.

Тема 31. Архитектор информационных систем. Кибертехникумных сред. 1 час.

Архитектор ИС, проектирование, сетевая безопасность, политики безопасности.

Тема 32. Консультант по информационной безопасности Личного профиля. 1 час.

Консультант, аудит безопасности, настройки приватности, личный профиль.

Тема 33. Куратор информационной безопасности. 1 час.

Куратор, правила безопасности, просвещение, инфографика, памятка.

Тема 34. Обобщение изученного материала. Итоговый урок. 1 час.

Обобщение, итоговый контроль, защита проекта, систематизация знаний.

Тематическое планирование

№	Название темы	Всего	Форма деятельности	Электронные образовательные ресурсы
1	Безопасность общения	13	Беседы, диалоги, дискуссии.	https://www.kaspersky.ru/ http://www.threatpost.ru/
2	Безопасность устройств	8	Круглый стол, беседы, диалоги, дискуссии	https://www.kaspersky.ru/ http://www.threatpost.ru/
3	Безопасность информации	10	Диалоги, беседы, дискуссии	https://www.kaspersky.ru/ http://www.threatpost.ru/
4	Повторение	4	Круглый стол, беседы, диалоги, дискуссии	https://www.kaspersky.ru/ http://www.threatpost.ru/
	Итого:	35		

Календарно-тематическое планирование

№	Тема занятия	Количество часов
1	Киберпространство	1
2	Виртуальная реальность.	1
3	Кибермиры	1
4	Управление дронами	1
5	Кибер физическая система. Искусственный интеллект.	1
6	Киберобщество.Соцсети	1
7	Киберденьги.	1
8	Криптовалюты	1
9	Кибермошенничество	1
10	Кибермошенничество. Документ Уголовный КодексРФ	1
11	Киберкультура	1
12	От книги к гипертексту	1
13	Киберкнига	1
14	Киберискусство	1
15	Социальная инженерия	1
16	Социальная инженерия	1
17	Угрозы социальной инженерии. Федеральный закон о персональных данных.	1
18	Угрозы социальной инженерии	1
19	Новые профессии в киберобществе	1
20	Цифровизация профессий	1
21	Киберугрозы	1
22	Кибервойны	1
23	Киберпреступность. Примеры киберпреступлений	1
24	Уязвимости кибербезопасности. Запрещенные и нежелательные сайты	1
25	Защита от вредоносных программ и информационных атак.	1
26	Защита от вредоносных программ и информационных атак.	1
27	Защита от вредоносных программ и информационных атак.	1
28	Защита от вредоносных программ и информационных атак.	1
29	Защита от вредоносных программ и информационных атак.	1
30	Профессии, связанные с безопасностью в IT сфере	1
31	Архитектор информационных систем. Кибертехникумных сред	1
32	Консультант по информационной безопасности Личного профиля	1
33	Куратор информационной безопасности	1

34	Обобщение изученного материала. Итоговый урок.	**1**
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ ПО ПРОГРАММЕ		**34**