государственное бюджетное общеобразовательное учреждение Самарской области
средняя общеобразовательная школа с. Красноармейское
муниципального района Красноармейский Самарской области

ПРОВЕРЕНО
Советник директора по воспитанию
_____О.Н. Мишустина
от «30» августа 2023 г.

УТВЕРЖДЕНО
директор ГБОУ СОШ с. Красноармейское
О.Н. Абашкина
Приказ № 69/2 от «30» августа 2023 г.

ГБОУ СОШ с. Красноармейское
CN=Абашкина О.Н.
E=o.n.abashkina@mail.ru
место подписания

Рабочая программа курса внеурочной деятельности

«Информационная безопасность, или на расстоянии одного вируса»

Возраст 13-15 лет

Количество часов по учебному плану 34 часа в год, 1 час в неделю.

РАССМОТРЕНА на заседании творческой группы учителей
«Здоровьесберегающие технологии»
Протокол № 1 №1 от «29» августа 2023 г.
Председатель творческой группы_/Т.В. Христич/

2023 г.

Личностные, метапредметные и предметные результаты освоения учебного курса

Предметные:

Выпускник 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. Выпускник овладеет:

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

Выпускник 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, включая Интернет-ресурсы и другие базы данных. **Метапредметные**

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.

Личностные

• 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; соблюдение правил индивидуального и коллективного безопасного поведения в информационно- телекоммуникационной среде.

Содержание программы

Содержание программы курса внеурочной деятельности соответствует темам ООП ООО ГБОУ СОШ с. Красноармейское по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», 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 «Безопасность общения», «Безопасность устройств», «Безопасность информации».

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. 1 час Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете. 1 час Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Тема 3. Пароли для аккаунтов социальных сетей. 1 час Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей. Тема 4. Безопасный вход в аккаунты. 1 час Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях. 1 час Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях. 1 час Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. 1 час Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты. 1 час Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Тема 9. Фишинг. 2 часа Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как

защититься от фишеров в социальных сетях и мессенджерах. Выполнение и защита индивидуальных и групповых проектов3. 3 часа

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. 1 час Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода. 1 час Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при об- наружении вредоносных кодов на устройствах.

Тема 3. Методы защиты от вредоносных программ. 2 час Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защитыот вредоносных кодов.

Тема 4. Распространение вредоносного кода для мобильных устройств. 1 час Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства. Выполнение и защита индивидуальных и групповых проектов. 3 часа Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. 1 час Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. 1 час Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальныхролей. Фейковые новости. Поддельные страницы.

Тема 3. Безопасность при использовании платежных карт в Интернете. 1 час Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Тема 4. Беспроводная технология связи. 1 час Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Тема 5. Резервное копирование данных. 1 час Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 2 час. Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования

культуры информационной безопасности. Выполнение и защита индивидуальных и групповых проектов. 3 часа Повторение. Волонтерская практика. 3 часа

Календарно – тематическое планирование

№п/п	Тема	Кол-во часов	Основное содержание	Характеристика основных видов учебной деятельности обучающихся
	Тема 1. «Безопасность общения»			
1	Общение в социальных сетях и мессенджерах	1	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальныхсетей и мессенджеров. Пользовательский контент.	Выполняет базовые операции при использовании мессенджеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.
2	С кем безопасно общаться в интернете	1	Персональные данные как основной капитал личного пространства в цифровом мире.	Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.
3	Пароли для аккаунтов социальных сетей	1	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	Изучает основные понятия регистрационной информации и шифрования. Умеет их применить.
4	Безопасный вход в аккаунты	1	Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасноговхода.
5	Настройки конфиденциальности в социальных сетях	1	Настройки приват- ности и конфиден- циальности в разныхсоциальных сетях. Приватность и конфиденциальность в мессенджерах.	Раскрывает причины установки закрытого
6	Публикация информации в социальных сетях	1	Персональные дан-ные. Публикация личной информации.	Осуществляет поиск и использует инфор- мацию, необходимую для выполнения поставленных задач.

7	Кибербуллинг	1	Определение кибер-буллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой ки-бербуллинга. Как помочь жертве кибербуллинга.	Реагирует на опасные ситуации, распознает провокациии попытки манипляции со стороны виртуальных собеседников.
8	Публичные аккаунты	1	Настройки приватности публичных страниц	Решает экспериментальные задачи. Самостоятельно создаетисточники информа-ции разного типа и для разных аудиторий, соблюдая правила информационной безопасности.
9-10	Фишинг	2	Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	Анализ проблемных ситуаций. Разборка кейсов с примерами
11	Тест по модулю «Безопасность общения»	1		
Тема 2. «Безопасность устройств»				
12	Что такое вредоносный код	1	Виды вредоносных кодов. Возможностии деструктивные функции вредоносных кодов.	Соблюдает технику безопасности при эксплуатации ком-пьютерных систем. Использует инструментальные про-граммные средства исервисы адекватно задаче.
13	Распространение вредоносного кода	1	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рас-сылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов наустройствах.	Выявляет и анализирует (при помощи чек-листа) возможные угрозы инфор- мационной безопасности объектов.

14	Методы защиты от вредоносных программ	2	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.	Изучает виды анти-вирусных программ и правила их установки.
15	Распространение вредоносного кода для мобильных устройств	1	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младше-го возраста.
16	Выполнение и защита индивидуальных и групповых проектов	2		
17	Тест по модулю «Безопасность устройств»	1		
Тема 3 «Безопасность информации»				
1	Социальная инженерия: распознать и избежать	1	Приемы социальной инженерии. Правила безопасности при виртуальных кон-тактах.	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.
2	Ложная информация в Интернете	1	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	Определяет возможные источники необходимых сведений, осуществляет поискинформации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации.
3	Безопасность при использовани и платежных карт в Интернете	2	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	Приводит примерырисков, онлайн покупок (умеет определить источник риска). Разрабатывает возможные ва рианты решения ситуаций, связан ных с рисками использования платежных карт в Интернете.

4	Беспроводная технология связи	1	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичныхсетях.	Используя различ- ную информацию, определяет понятия.Изучает особенности и стиль веденияличных и публичных аккаунтов.
5	Резервное копированиеданных	2	Безопасность личной информации. Со- здание резервныхкопий на различных устройствах.	Создает резервные копии
6	Основы государ-ственной политики в области формированиякуль туры информационной безопасности	1	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области	Умеет привести выдержки из законодательства РФ: обеспечивающего конституционное право на поиск, получение и распространение информации; отражающего правовые аспекты защиты киберпространства.
			формирования культуры информационной безопасности.	
7	Выполнение и защита индивидуальных и групповых проектов	4		
8	Повторение, волон-терская практика, резерв	3		
	Итого	34		

Ключи ответов к тесту по модулю «Безопасность общения»

номер задания	правильный ответ
1	1-Е, 2-Д, 3-Г, 4-В, 5-А, 6-Б
2	онлайн сервис в Интернете для общения и связи
3	
4	учётная запись пользователя в каком-либо сервисе
5	любимые места в городе; твоё хобби; любимые книги
6	приватность фотографий приватность списка друзей приватность персональных данных приватность местоположения
7	Ytrewq drowssap uiop Mypassword Ivan1968
8	Логин и пароль от учетной записи и пароль из смс Логин и пароль от учётной записи и USB- токен Логин и пароль от учётной записии смарткарта
9	Травля, оскорбления и угрозы в условиях интернет- коммуника-ции
10	Паспортные данные Телефон Проверочный код от карты Пароль от учётной записи в социальной сетиПароль от онлайн-банкинга Номер банковской карты Логин и пароль от почты

Ключи ответов к тесту по модулю «Безопасность устройств»

Номер задания	правильный ответ
1	ворующие регистрационные данные; дающие несанкционированный доступ к ключевым файлам различных программных продуктов; использующие ресурсы компьютеров в интересах своего автора; программы, проникающие в системные области данных и меняющие их; программы, шифрующие персональные файлы пользователя.
2	Возможные ответы: трояны-клавиатурные шпионы; трояны-шифровальщики; программы, организующие зомби-сети, и атаку с них; специализированные программы- боты; сетевые черви. Ответами могут быть конкретные названия троянов, червей, приложений и ботнетов.
3	Трояны распространяют люди, а вирусы распространяются самостоятельно. Черви распространяются также, как и вирусы.
4	с помощью вложенных в письма файлов при скачивании приложений при посещении популярных сайтов с помощью файлообменных сетей и торрентовс помощью методов социальной инженерии при использовании зараженной интернет-страницы компаниями, которые создают и продают защиту от вредоносных программ
5	обновлять операционную систему для устранения в новых версиях ошибок и уязвимости; обновлять браузер, потому что в новых версиях исправляют уязвимости и недостатки предыдущих версий; обновлять антивирусное программное обеспечение, для детектирования и блокирования вновь появившихся вредоносных программ;
6	Не буду заходить на сайт, даже проверенный сайт может быть заражён.
7	Любой человек
8	компьютерная программы, использующие уязвимости в программном обеспечении
9	разнообразие функций уровень детектирования доставка обновлений наличие лицензии продление лицензии

10	Возможные ответы: Использовать антивирусное ПО. Своевременное обновлять ПО, операционную систему, браузер иприложения Проверять приходящие файлы и ссылки перед скачиванием и открытием. Проявлять Интерес к информации от антивирусных компаний и экспертов по компьютерной безопасности. Не проводить процедуру получения прав суперпользователя на устройствах. Не скачивать файлы с подозрительных источников. Обращать внимание на расширение загружаемого файла. Воздержаться от загрузки пиратской версии программ, а скачивать файлы сфициального сайта производителя. Не скачивать приложение в комплекте с дополнительным ПО. Читать отзывы и советоваться с родителями и друзьями.
11	Вирусы Черви Трояны Бэкдоры Руткиты
12	регулярное обновление браузера регулярное обновление операционной системы регулярное обновление антивирусной базы проверка адресов сайтов отказ от перехода по ссылкам из всплывающих окон использование диспетчера задач для закрытия браузера в случае заражения загрузка ПО только с официальных сайтов-разработчиков выбор зарекомендовавших себя антивирусных программ установка только лицензионных версий ПО установке про- активного и поведенческого анализа в антивирусной базе
	проверка почтовых сообщений и их вложений полное ска- нирование компьютера и подключаемых устройств не реже1 раза в неделю

Ключи ответов к тесту по модулю «Безопасность информации»

номер задания	**правильный ответ**
1	Возможные ответы: А) фальшивые новости, ложно смонтированные видео; Б) приложение, которые имеет дизайн и функционал, напоминающий переделываемую программу; В) виртуальный номер телефона; Г) любой аккаунт с недостоверной информацией — имя, контакты, фотографии; Д) фиктивная страница в интернет-ресурсах; Е) банковская карта, оформленная на человека, который в реальности не существует; Ж) профиль, содержащий ложную информацию о владельце либо не содержащую вовсе; 3) сайт фаль- сифицированный, копия главной страницы которого напоминает известный.
2	Политика Реклама и продвижение товаров Торговля Маркетинг Артистическая сфера

<table>
<tr><td>3</td><td>3,4,5
Возможный ответ: Википедия в сочетании в другими источниками, но не менее 3х разных источников.</td></tr>
<tr><td>4</td><td>технология внедрения вредоносных программ, использующая управление действиями пользователя</td></tr>
<tr><td>5</td><td>школа;
общественный транспорт; поликлиника; ВУЗ.</td></tr>
<tr><td>6</td><td>WEP</td></tr>
<tr><td>7</td><td>замочек рядом со значком WI-FI Авторизация в сети WI-FIс паролем доступа</td></tr>
<tr><td>8</td><td>операционная система обновлена версия браузера обновлена двухфакторная онлайн транзакция свой компьютер обновленный антивирус, установленный на устройстве, с
которого производится транзакция правильный
адрес в адресной строке
банковское приложение, скачанное с официального сайта
банка</td></tr>
<tr><td>9</td><td>Правильное распределение:
<table>
<tr><td>От сбоев оборудования</td><td>От случайной потери илиискажения храня-щейся информации</td><td>От несанкционированного доступа к информации</td></tr>
<tr><td>защита от фи-зической порчи жесткого диска
защита от фи-зической порчи флеш - карты</td><td>возможность исполь-зования и сохранения последней версии ре-ферата, доклада или других рабочих доку-ментов
хранение ценных файлов и данных на любом устройстве</td><td>защита информации от вредоносного ПО
хранение первоначальной версии операционной системы, незаражённой вредоносными программами</td></tr>
<tr><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>10</td><td>Возможные ответы: некоторые программы перестают работать, на экран выводятся посторонние сообщения или сим- волы, работа существенно замедляется, некоторые файлы не открываются или оказываются испорченными, операция сохранения файлов или какая-нибудь другая операция происходит без
команды пользователя.</td></tr>
</table>

Требования к содержанию итоговых проектно-исследовательских работ

Критерии содержания текста проектно-исследовательской работы

Во введении сформулирована актуальность (личностную и социальную значимость) выбранной проблемы. Тема может быть переформулирована, но при этом четко определена, в необходимости исследования есть аргументы.

Правильно составлен научный аппарат работы: точность формулировки проблемы, четкость и конкретность в постановке цели и задач, определении объекта и предмета исследования, выдвижении гипотезы. Гипотеза сформулирована корректно и соот- ветствуют теме работы

Есть планирование проектно-исследовательской деятельности, корректировка ее в зависимости от результатов, получаемых на разных этапах развития проекта. Дана характеристика каждого этапа реализации проекта, сформулированы задачи, которые решаются на каждом этапе, в случае коллективного проекта - распределены и выполнены задачи каждым участником, анализ ресурсного обеспечения проекта проведен корректно Используется и осмысляется междисциплинарный подход к исследованию и проек-

тированию и на базовом уровне школьной программы, и на уровне освоения дополнительных библиографических источников

Определён объём собственных данных и сопоставлено собственное проектное решениес аналоговыми по проблеме. Дан анализ источников и аналогов с точки зрения значимости для собственной проектно-исследовательской работы, выявлена его новизна, библиография и интернет ресурсы грамотно оформлены

Соблюдены нормы научного стиля изложения и оформления работы. Текст работы должен демонстрировать уровень владения научным стилем изложения.

Есть оценка результативности проекта, соотнесение с поставленными задачами.

Проведена оценка социокультурных и образовательных последствий проекта на ин- дивидуальном и общественном уровнях.

Критерии презентации проектно-исследовательской работы (устного выступления)

Демонстрация коммуникативных навыков при защите работы. Владение риторическими умениями, раскрытие автором содержание работы, достаточная осведомлен-ность в

терминологической системе проблемы, отсутствие стилистических и речевых ошибок, соблюдение регламента.

Умение чётко отвечать на вопросы после презентации работы.

Умение создать качественную презентацию. Демонстрация умения использовать IT- технологии и создавать слайд презентацию на соответствующем его возрасту уровне.

Умение оформлять качественный презентационный буклет на соответствующем его возрасту уровне.

Творческий подход к созданию продукта, оригинальность, наглядность, иллюстративность. Предоставлен качественный творческий продукт (макет, программный

продукт, стенд, статья, наглядное пособие, литературное произведение, видеоролик, мультфильм и т.д.).

Умение установить отношения коллаборации с участниками проекта, наметить пути создания сетевого продукта. Способность намечать пути сотрудничества на уровне взаимодействия с членами кружка или секции, проявление в ходе презентации ком- муникабельности, благодарности и уважения по отношению к руководителю, кон- сультантам, умение четко обозначить пути создания сетевого продукта.

Ярко выраженный интерес к научному поиску, самостоятельность в выборе проблемы, пути ее исследования и проектного решения.