Рабочая программа рассмотрена на заседании кафедры учителей информатики, технологии, ОБЖ, физической культуры и предметов эстетического цикла
Заведующая кафедрой
«26» августа 2021 г.
Крыпаева В.Б./_____/

Проверена
« 28 » августа 2021 г.
Заместитель директора по ВР
Шапошникова Е.Ю./_____/

Утверждаю к использованию
в образовательном процессе школы
директор школы
Плотников Ю.А. /_____/
« 1 » сентября 2021г.

Рабочая программа
по внеурочной деятельности
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
ДЛЯ 8 КЛАССОВ
ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБЩЕОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ САМАРСКОЙ ОБЛАСТИ
СРЕДНЕЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ШКОЛЫ №2
С УГЛУБЛЕННЫМ ИЗУЧЕНИЕМ ОТДЕЛЬНЫХ ПРЕДМЕТОВ
п.г.т. Усть-Кинельский г.о. Кинель Самарской области
НА 2021 – 2022 УЧЕБНЫЙ ГОД

Автор-составитель: учитель Плотникова С.В.

ЭП
C=RU, O=ГБОУ СОШ №2 пгт. Усть-Кинельский,
CN=Плотников Ю.А., E=plot.02@mail.ru
место подписания
2021.10.13 10:16:36+04'00'

п.г.т. Усть-Кинельский
2021 г.

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа по внеурочной деятельности «Информационная безопасность» составлена в соответствии с требованиями ФГОС среднего общего образования к структуре и результатам освоения основных образовательных программ среднего общего образования. 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.

Программа разработана на основе следующих документов:

1) Приказа Министерства образования и науки Российской Федерации №413 от 17.05.2012 (ред. от 29.06.2017) «Об утверждении Федерального государственного образовательного стандарта среднего общего образования»;
2) примерной основной образовательной программой среднего общего образования (протокол от 28.06.2016 г. №2/16-з);
3) основной образовательной программы среднего общего образования ГБОУ СОШ №2 с углубленным изучением отдельных предметов п.г.т. Усть–Кинельский г. о. Кинель Самарской области (протокол № 1 от 29.08.2019 г., приказ № 210-3 от 30.08.2019 г.);
4) положения о рабочей программе учебных курсов, предметов, дисциплин в образования ГБОУ СОШ № 2 с углубленным изучением отдельных предметов п.г.т. Усть–Кинельский г. о. Кинель Самарской области (приказ № 71-1 ОД от 22 марта 2019 г.);

Для реализации образовательной программы выбран:

1. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы : учеб. Пособие для общеобразоват. Организаций / М.С. Наместникова. – М. : Просвещение, 2019. – 79 с. : ил. – (Внеурочная деятельность).

Место предмета в учебном плане

Согласно учебному плану ГБОУ СОШ №2 п.г.т. Усть–Кинельский на изучение курса «Информационная безопасность» отводится в общем объеме 34 часа (1 урок в неделю).

Цели и задачи реализации курса «Информационная безопасность»

Цель изучения курса:

- 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).

Достижение поставленных целей при разработке и реализации программы внеурочной деятельности «Информационная безопасность» предусматривает решение следующих **основных задач**:

- 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, изобрази- тельных, 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.

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Планируемые личностные результаты программы внеурочной деятельности

Личностным результатом изучения курса является формирование:

- 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.

Планируемые метапредметные результаты освоения программы внеурочной деятельности

1. 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.

2. 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.

3. 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.

3.СОДЕРЖАНИЕ ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

№ п/п	Наименование раздела	Содержание	Кол-во часов
1.	«Безопасность общения»	Общение в социальных сетях и мессенджерах. С кем безопасно общаться в интернете. Пароли для аккаунтов социальных сетей. Безопасный вход в аккаунты. Настройки конфиденциальности в социальных сетях. Публикация информации в социальных сетях. Кибербуллинг. Публичные аккаунты. Фишинг. Выполнение и защита индивидуальных и групповых проектов.	13
2.	«Безопасность устройств»	Что такое вредоносный код. Распространение вредоносного кода. Методы защиты от вредоносных программ. Распространение вредоносногокода для мобильных устройств. Выполнение и защита индивидуальных и групповых проектов.	8
3.	«Безопасность информации»	Социальная инженерия: распознать и избежать.	10

		Ложная информация в Интернете. Безопасность при использовании платежных карт в Интернете. Беспроводная технология связи. Резервное копирование данных. Основы государственной политики в области формирования культуры информационной безопасности. Выполнение и защита индивидуальных и групповых проектов.	
4.	Повторение	Повторение. Волонтерская практика.	3
	Общее количество часов:		**34**

УТП 8 класс

№ п/п	Тема	Количество 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 социальных сетей 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.	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.

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. Учится их применять.
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 безопасного входа.

5	Настройки конфиденциальности в социальных сетях	1	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле.
6	Публикация информации в социальных сетях	1	Персональные данные. Публикация личной информации.	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.
7	Кибербуллинг	1	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
8	Публичные аккаунты	1	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.
9	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. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространение чек-листа (памятки) по противодействию фишингу.
10	Выполнение и защита индивидуальных и групповых проектов	3		Самостоятельная работа.

Тема 2. «Безопасность устройств»				
1	Что такое вредоносный код	1	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче.
2	Распространение вредоносного кода	1	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.
3	Методы защиты от вредоносных программ	2	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.	Изучает виды антивирусных программ и правила их установки.
4	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 младшего возраста.
5.	Выполнение и защита индивидуальных и групповых проектов	3		Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории.

Тема 3 «Безопасность информации»				
1	Социальная инженерия: распознать и избежать	1	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	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 поиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации.
3	Безопасность при использовании платежных карт в Интернете	1	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете.
4	Беспроводная технология связи	1	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.
5	Резервное копирование данных	1	Безопасность личной информации. Создание резервных копий на различных устройствах.	Создает резервные копии.

6	Основы государственной политики в области формирования культуры информационной безопасности	2	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.	Умеет привести выдержки из законодательства РФ: -обеспечивающего конституционное право на поиск, получение и распространение информации; - отражающего правовые аспекты защиты киберпространства.
7	Выполнение и защита индивидуальных и групповых проектов	3		
8	Повторение, волонтерская практика, резерв	3		
	Итого	34		

Литература

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с
2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014. – 182 с.
3. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017. – 384 с.
4. Дети в информационном обществе // http://detionline.com/journal/about
5. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИДАНА, 2016. – 239 с.
6. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018. – 558 с.
7. Защита детей by Kaspersky // https://kids.kaspersky.ru/
8. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества/А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017. – 64 с.
9. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019. – 80 с.
10. Основы кибербезопасности. // https://www.xn--d1abkefqip0a2f.xn-- p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa
11. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005. – 304 с.
12. Сусоров И.А. Перспективные технологии обеспечения кибербезопасности// Студенческий: электрон. научн. журн. 2019. № 22(66)
13. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013. – 144 с.