ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 7 С УГЛУБЛЕННЫМ ИЗУЧЕНИЕМ ОТДЕЛЬНЫХ ПРЕДМЕТОВ «ОБРАЗОВАТЕЛЬНЫЙ ЦЕНТР» ИМЕНИ Г.И.ГОРЕЧЕНКОВАГОРОДА НОВОКУЙБЫШЕВСКА ГОРОДСКОГО ОКРУГА НОВОКУЙБЫШЕВСК САМАРСКОЙ ОБЛАСТИ

446218, Самарская область, г.Новокуйбышевск, ул. Свердлова, д. 12, тел. 4-74-17

Р А С С М О Т Р Е Н О	П Р О В Е Р Е Н О	У Т В Е Р Ж Д Е Н О
на заседании ШМО Протокол № 1 от 29 августа 2022 г. С.И. Буранова	Зам. директора по УВР С.Н. Гайдукова 29 августа 2022 г.	приказом директора ГБОУ СОШ № 7 «ОЦ» г.Новокуйбышевска № 232 от 29 августа 2022 г.

ЭП

О="ГБОУ СОШ № 7 ""ОЦ"" г.Новокуйбышевска", CN=Иванова Е.В., E=sch7_nkb@samara.edu.ru
00e90ef5dd17927159
2022.09.01 21:33:57+04'00'

РАБОЧАЯ ПРОГРАММА

внеурочной деятельности «Информационная безопасность» для обучающихся 8 - 9 классов

направление: общеинтеллектуальное

Составитель: Сивцова И.Н.

г.Новокуйбышевск,
2022 г.

1. Планируемые результаты

<table>
<tr><td colspan="2">Личностные результаты освоения программы
В результате освоения программы курса «Информационная безопасность» у обучающихся будут сформированы:
– 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.</td></tr>
<tr><td colspan="2">Предметные результаты освоения программы:</td></tr>
<tr><td>Выпускник научится:</td><td>– 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.</td></tr>
<tr><td>Выпускник овладеет:</td><td>– приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.
– использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.</td></tr>
<tr><td>Выпускник получит возможность овладеть:</td><td>– основами соблюдения норм информационной этики и права;
– основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при форми-ровании современной культуры безопасности жизнедеятельности;</td></tr>
</table>

Метапредметные результаты освоения программы курса	
Познавательные УУД	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, способ-ные быть причиной данного явления, выявлять причины и следствия явле-ний; – строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям; – излагать полученную информацию, интерпретируя ее в контексте решае-мой 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.
Регулятивные УУД	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;
Коммуникативные УУД	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, со-здание 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.

1. Содержание курса

№	Название темы	Форма организации	Кол-во часов	Виды деятельности	Содержание
7 класс					
Безопасность общения			***13***		
1	Общение в социальных сетях и мессенджерах	Презентация, беседа	1	– познавательная – проблемно-ценностное общение	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.
2	С кем безопасно общаться в интернете.	Видеоурок, деловая игра	1	– познавательная – игровая	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.	Видеоурок, беседа	1	– познавательная – проблемно-ценностное общение	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.
4	Безопасный вход в аккаунты.	Презентация, дискуссия	1	– познавательная – проблемно-ценностное общение	Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.
5	Настройки конфиденциальности в социальных сетях	Беседа, практическая работа	1	– познавательная – проблемно-ценностное общение	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.
6	Публикация информации в социальных сетях.	Дискуссия, «круглый стол»	1	– познавательная – проблемно-ценностное общение	Персональные данные. Публикация личной информации.
7	Кибербуллинг.	Презентация, дискуссия	1	– познавательная – проблемно-ценностное общение	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

№	Название темы	Форма организации	Кол-во часов	Виды деятельности	Содержание
8	Публичные аккаунты.	Беседа, практическая работа	1	– познавательная – проблемно-ценностное общение	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.
9-10	Фишинг.	Презентация, дискуссия	2	– познавательная – проблемно-ценностное общение	Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.
11-13	Выполнение и защита индивидуальных и групповых проектов.	Практическая работа	3	– проблемно-ценностное общение	
Безопасность устройств			***8***		
14	Что такое вредоносный код.	Презентация, дискуссия	1	– познавательная – проблемно-ценностное общение	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.
15	Распространение вредоносного кода.	Видеоурок, интерактивная игра	1	– познавательная – игровая	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.
16-17	Методы защиты от вредоносных программ	Дискуссия, деловая игра	2	– игровая – проблемно-ценностное общение	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.
18	Распространение вредоносного кода для мобильных устройств.	Презентация, дискуссия	1	– познавательная – проблемно-ценностное общение	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.
19-21	Выполнение и защита индивидуальных и групповых проектов.	Практическая работа	3	– проблемно-ценностное общение	
Безопасность информации			***13***		

№	Название темы	Форма организации	Кол-во часов	Виды деятельности	Содержание
22	Социальная инженерия: распознать и избежать.	Презентация, беседа	1	– познавательная – проблемно-ценностное общение	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.
23	Ложная информация в Интернете.	«Круглый стол»	1	– проблемно-ценностное общение	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.
24	Безопасность при использовании платежных карт в Интернете.	Презентация, беседа	1	– познавательная	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.
25	Беспроводная технология связи.	Видеоурок, беседа	1	– познавательная – проблемно-ценностное общение	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.
26	Резервное копирование данных.	Беседа, практическая работа	1	– проблемно-ценностное общение	Безопасность личной информации. Создание резервных копий на раз-личных устройствах.
27-28	Основы государственной политики в области формирования культуры информационной безопасности.	Презентация, беседа	2	– познавательная – проблемно-ценностное общение	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.
29-31	Выполнение и защита индивидуальных и групповых проектов.	Практическая работа	3	– проблемно-ценностное общение	
32-34	Повторение. Волонтерская практика.		3	– проблемно-ценностное общение	
Количество часов всего			***34***		

№	Название темы	Форма организации	Кол-во часов	Виды деятельности	Содержание
9 класс					
Безопасность общения			***13***		
1	Общение в социальных сетях и мессенджерах	Презентация, беседа	1	– познавательная – проблемно-ценностное общение	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.
2	С кем безопасно общаться в интернете.	Видеоурок, деловая игра	1	– познавательная – игровая	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.	Видеоурок, беседа	1	– познавательная – проблемно-ценностное общение	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.
4	Безопасный вход в аккаунты.	Презентация, дискуссия	1	– познавательная – проблемно-ценностное общение	Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.
5	Настройки конфиденциальности в социальных сетях	Беседа, практическая работа	1	– познавательная – проблемно-ценностное общение	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.
6	Публикация информации в социальных сетях.	Дискуссия, «круглый стол»	1	– познавательная – проблемно-ценностное общение	Персональные данные. Публикация личной информации.
7	Кибербуллинг.	Презентация, дискуссия	1	– познавательная – проблемно-ценностное общение	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.
8	Публичные аккаунты.	Беседа, практическая работа	1	– познавательная	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

№	Название темы	Форма организации	Кол-во часов	Виды деятельности	Содержание
				– проблемно-ценностное общение	
9-10	Фишинг.	Презентация, дискуссия	2	– познавательная – проблемно-ценностное общение	Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.
11-13	Выполнение и защита индивидуальных и групповых проектов.	Практическая работа	3	– проблемно-ценностное общение	
Безопасность устройств			***8***		
14	Что такое вредоносный код.	Презентация, дискуссия	1	– познавательная – проблемно-ценностное общение	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.
15	Распространение вредоносного кода.	Видеоурок, интерактивная игра	1	– познавательная – игровая	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.
16-17	Методы защиты от вредоносных программ	Дискуссия, деловая игра	2	– игровая – проблемно-ценностное общение	Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.
18	Распространение вредоносного кода для мобильных устройств.	Презентация, дискуссия	1	– познавательная – проблемно-ценностное общение	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.
19-21	Выполнение и защита индивидуальных и групповых проектов.	Практическая работа	3	– проблемно-ценностное общение	
Безопасность информации			***13***		

№	Название темы	Форма организации	Кол-во часов	Виды деятельности	Содержание
22	Социальная инженерия: распознать и избежать.	Презентация, беседа	1	– познавательная – проблемно-ценностное общение	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.
23	Ложная информация в Интернете.	«Круглый стол»	1	– проблемно-ценностное общение	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.
24	Безопасность при использовании платежных карт в Интернете.	Презентация, беседа	1	– познавательная	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.
25	Беспроводная технология связи.	Видеоурок, беседа	1	– познавательная – проблемно-ценностное общение	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.
26	Резервное копирование данных.	Беседа, практическая работа	1	– проблемно-ценностное общение	Безопасность личной информации. Создание резервных копий на раз-личных устройствах.
27-28	Основы государственной политики в области формирования культуры информационной безопасности.	Презентация, беседа	2	– познавательная – проблемно-ценностное общение	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.
29-31	Выполнение и защита индивидуальных и групповых проектов.	Практическая работа	3	– проблемно-ценностное общение	
32-34	Повторение. Волонтерская практика.		3	– проблемно-ценностное общение	
Количество часов всего			***34***		

2. **Тематическое планирование «Информационная безопасность»**

№	Название разделов и тем	Количество часов			Примерная дата	Форма контроля
		всего	теор.	Практ.		
Первый год обучения						
Безопасность общения		***13***	***7***	***6***		
1	Общение в социальных сетях и мессенджерах	1	1	0		
2	С кем безопасно общаться в интернете.	1	1	0		
3	Пароли для аккаунтов социальных сетей.	1	1	0		Практическая работа
4	Безопасный вход в аккаунты.	1	1	0		
5	Настройки конфиденциальности в социальных	1	0	1		Практическая работа
6	Публикация информации в социальных сетях.	1	0	1		
7	Кибербуллинг.	1	1	0		Тестирование
8	Публичные аккаунты.	1	1	0		
9	Фишинг.	2	1	1		
10	Выполнение и защита индивидуальных и групповых проектов.	3	0	3		Защита индивидуальных проектов
Безопасность устройств		*8*	*4*	*4*		
11	Что такое вредоносный код.	1	1	0		
12	Распространение вредоносного кода.	1	1	0		Практическая работа
13	Методы защиты от вредоносных программ	2	1	1		
14	Распространение вредоносного кода для мобильных устройств.	1	1	0		Тест
15	Выполнение и защита индивидуальных и групповых проектов.	3	0	3		Защита индивидуальных проектов
Безопасность информации		***13***	***5***	***8***		
16	Социальная инженерия: распознать и избежать.	1	1	0		

17	Ложная информация в Интернете.	1	1	0		Практическая работа
18	Безопасность при использовании платежных карт в Интернете.	1	1	0		
19	Беспроводная технология связи.	1	1	0		Тест
20	Резервное копирование данных.	1	0	1		Практическая работа
21	Основы государственной политики в области формирования культуры информационной безопасности.	2	1	1		
22	Выполнение и защита индивидуальных и групповых проектов.	3	0	3		Защита индивидуальных проектов
23	Повторение. Волонтерская практика.	3	0	3		
	Итого	**34**				

Формы контроля:

1. Практическая работа
2. Тестирование
3. Защита индивидуального проекта

Форма промежуточной аттестации:

Защита 1 проекта

Оценивание: зачет/незачет.

Учебный (тематический) план курса в 9 классе

№	Название разделов и тем	Количество часов			Примерная дата	Форма контроля
		всего	теор.	Практ.		
	Первый год обучения					

Безопасность общения		***13***	***7***	***6***		
1	Общение в социальных сетях и мессенджерах	1	1	0		
2	С кем безопасно общаться в интернете.	1	1	0		
3	Пароли для аккаунтов социальных сетей.	1	1	0	Практическая работа	Практическая работа
4	Безопасный вход в аккаунты.	1	1	0		
5	Настройки конфиденциальности в социальных	1	0	1	Практическая работа	Практическая работа
6	Публикация информации в социальных сетях.	1	0	1		
7	Кибербуллинг.	1	1	0	Тестирование	Тест
8	Публичные аккаунты.	1	1	0		
9	Фишинг.	2	1	1		
10	Выполнение и защита индивидуальных и групповых проектов.	3	0	3	Защита индивидуальных проектов	Защита индивидуальных проектов
Безопасность устройств		*8*	*4*	*4*		
11	Что такое вредоносный код.	1	1	0		
12	Распространение вредоносного кода.	1	1	0	Практическая работа	Практическая работа
13	Методы защиты от вредоносных программ	2	1	1		
14	Распространение вредоносного кода для мобильных устройств.	1	1	0	Тест	Тест
15	Выполнение и защита индивидуальных и групповых проектов.	3	0	3	Защита индивидуальных проектов	Защита индивидуальных проектов
Безопасность информации		***13***	***5***	***8***		
16	Социальная инженерия: распознать и избежать.	1	1	0		
17	Ложная информация в Интернете.	1	1	0	Практическая работа	Практическая работа
18	Безопасность при использовании платежных карт в Интернете.	1	1	0		
19	Беспроводная технология связи.	1	1	0	Тест	Тест

20	Резервное копирование данных.	1	0	1	Практическая работа	Практическая работа
21	Основы государственной политики в области формирования культуры информационной безопасности.	2	1	1		
22	Выполнение и защита индивидуальных и групповых проектов.	3	0	3	Защита индивидуальных проектов	Защита индивидуальных проектов
23	Повторение. Волонтерская практика.	3	0	3		
	Итого	**34**				

Формы контроля:

1. Практическая работа
2. Тестирование
3. Защита индивидуального проекта

Форма промежуточной аттестации:

Защита 1 проекта

Оценивание: зачет/незачет.