МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Министерство образования и науки Самарской области

государственное бюджетное общеобразовательное учреждение

Самарской области средняя общеобразовательная школа № 2 с.

Приволжье муниципального района Приволжский Самарской области

РАССМОТРЕНО	ПРОВЕРЕНО	УТВЕРЖДЕНО
Руководитель ШМС	заместитель директора по УВР	директор ГБОУ СОШ №2 с. Приволжье
_____	_____	_____
Елакова МИ	Левина М.А.	Сергачева Л.Ю.
Протокол№1 от«31» августа 2026г	Протокол№1 от«31» августа2026г.	Приказ№/103-од от«31» августа2026г.

C=RU, O=ГБОУ СОШ №2 с.Приволжье, CN=Сергачева Лилия Юрьевна, E=school2_prv@samara.edu.ru 00f4a897f9467376cf 2026.08.31 17:17:05+04'00'

ЭП

Программа курса внеурочной деятельности

«Информационная безопасность или на расстояние одного вируса»

(реализуется в 7 классе)

Приволжье, 2026г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели изучения курса:

- **Обеспечение условий** для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков, манипуляций и угроз;
- **Формирование навыков** своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера) и предотвращения интернет-зависимости;
- **Развитие критического мышления** при работе с большими массивами данных и верификации контента.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ КУРСА

В соответствии с требованиями обновленного ФГОС ООО, курс направлен на достижение личностных, метапредметных и предметных результатов.

1. Личностные результаты

В процессе освоения программы у обучающегося будут сформированы следующие личностные качества и установки в рамках инвариантных модулей программы воспитания школы:

Гражданское и патриотическое воспитание: Осознание себя гражданином РФ, понимание основ государственной политики в области кибербезопасности, уважение к законодательству РФ в сфере информационного права и защиты персональных данных;

Духовно-нравственное и этическое воспитание: Уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире; интериоризация правил этичного, конструктивного и безопасного сетевого взаимодействия;

Ценность безопасного образа жизни и здоровья: Сформированность понимания ценности здорового и безопасного образа жизни в условиях цифровизации; умение распознавать риски интернет-зависимости и распределять время между активностью в сети и реальной жизнью;

Организация учебного пространства и саморазвитие: Готовность к осознанному выбору дальнейшей образовательной траектории, проявление устойчивого познавательного интереса к профессиям в сфере информационных технологий и кибербезопасности.

2. Метапредметные результаты

Метапредметные результаты группируются по трем направлениям универсальных учебных действий (УУД):

А) Познавательные УУД (базовые логические и исследовательские действия):

Анализ информации: Умение самостоятельно указывать на информацию в сети, нуждающуюся в проверке, и применять методы ее верификации (фактчекинг);

Критическое мышление: Умение критически оценивать форму и содержание интернет-текстов, выявлять скрытые манипуляции, кликбейт и фейковые новости;

Работа с данными: Умение осуществлять целенаправленный поиск информации в верифицированных базах данных с использованием сложных поисковых запросов и ключевых слов.

Б) Регулятивные УУД (самоорганизация и самоконтроль):

Целеполагание и планирование: Способность самостоятельно формулировать цели деятельности при разработке индивидуальных или групповых проектов по информационной безопасности;

Принятие решений: Умение оценивать риски в изменяющейся цифровой среде, принимать осознанные решения в сложных ситуациях (при фишинге, кибербуллинге) и нести за них ответственность;

Оценка результатов: Умение соотносить полученный результат проектной деятельности с изначально поставленными задачами и аргументировать причины успеха или неудач.

В) Коммуникативные УУД (совместная деятельность и общение):

Сетевая коммуникация: Строить позитивные и безопасные отношения в мессенджерах и социальных сетях; конструктивно защищать свою позицию, признавая ошибочность своего мнения в случае аргументированной критики;

Сотрудничество (коллаборация): Эффективно взаимодействовать в малых группах при создании коллективных цифровых продуктов, памяток, чек-листов и презентаций;

Информационное моделирование: Создавать текстовые, графические и мультимедийные ресурсы для различных аудиторий с соблюдением правил информационной гигиены.

3. Предметные результаты

Несмотря на внеурочный статус курса, обучающиеся овладевают практическими ИКТ-компетенциями и навыками ОБЗР:

В области сетевой грамотности: Обучающийся научится анализировать структуру доменных имен, URL-адреса сайтов и верифицировать SSL-сертификаты для распознавания фишинговых платформ;

В области защиты устройств: Обучающийся овладеет знаниями об основных типах вредоносного ПО, методах их распространения на ПК и мобильных платформах, а также научится настраивать алгоритмы работы антивирусного софта;

В области защиты данных: Обучающийся научится безопасно организовывать личное информационное пространство (cloud-сервисы, съемные диски) и создавать стратегии резервного копирования информации;

В области финансовой безопасности: Обучающийся сможет применять правила безопасного совершения транзакций в интернете и использовать способы самозащиты при попытках виртуального мошенничества.

СИСТЕМА ОЦЕНИВАНИЯ И ФОРМЫ АТТЕСТАЦИИ

В соответствии с локальным актом школы, в рамках курса внеурочной деятельности применяется **безотметочная система оценки** результатов.

Основными формами контроля и аттестации являются:

1. **Текущий контроль:** Оценка активности в групповых дискуссиях, разбор практических кейсов, составление памяток и чек-листов противодействия угрозам (например, чек-лист по борьбе с фишингом).

2. **Промежуточная (итоговая) аттестация:** Защита индивидуальных и групповых проектно-исследовательских работ по темам разделов курса.

Критерии оценки итогового проекта включают в себя оценку актуальности темы, глубину анализа цифровой угрозы, качество оформления слайд-презентации и творческий подход к продукту проекта (макет, видеоролик, статья или наглядное пособие).

РАЗДЕЛ 1. БЕЗОПАСНОСТЬ ОБЩЕНИЯ И ЛИЧНЫХ ДАННЫХ В СЕТИ (14 ЧАСОВ)

- **Цифровая идентичность:** Социальные сети и мессенджеры, их история и назначение. Создание безопасного цифрового профиля.
- **Персональные данные:** Понятие личного пространства и защита конфиденциальности. Правила добавления «друзей».
- **Управление доступом:** Сложные пароли, генераторы и менеджеры паролей. Многофакторная аутентификация. Работа на публичных устройствах. Настройки приватности.
- **Угрозы коммуникации:** Овершеринг (избыточная публикация информации). Кибербуллинг: распознавание, способы защиты, помощь жертве агрессии. Фишинг и социальная инженерия в мессенджерах.
- **Проектный блок:** Подготовка и защита индивидуальных/групповых проектов по безопасности общения.

РАЗДЕЛ 2. БЕЗОПАСНОСТЬ ЦИФРОВЫХ УСТРОЙСТВ (8 ЧАСОВ)

- **Вредоносное ПО:** Виды вредоносных кодов (вирусы, трояны, черви, шифровальщики) и их деструктивные функции.
- **Каналы заражения:** Способы распространения вредоносного кода (почта, ссылки, скрипты). Признаки заражения устройства.
- **Методы защиты:** Выбор и настройка антивирусного ПО. Особенности защиты мобильных устройств (смартфоны, планшеты), правила безопасной установки приложений.
- **Проектный блок:** Защита проектов по теме обеспечения безопасности персональных гаджетов.

РАЗДЕЛ 3. БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И ЦИФРОВАЯ ГИГИЕНА (12 ЧАСОВ)

- **Критическое мышление:** Распознавание манипуляций и приемов социальной инженерии. Проверка достоверности информации, фейковые новости и поддельные страницы.
- **Финансовая грамотность в сети:** Безопасность при использовании платежных карт, онлайн-покупки, защита от банковского мошенничества.
- **Сетевая инфраструктура:** Уязвимости Wi-Fi-соединений, правила работы в публичных беспроводных сетях.
- **Резервное копирование:** Стратегии бэкапа данных, использование облачных хранилищ и внешних носителей.
- **Государство и безопасность:** Основы государственной политики в области ИБ, Доктрина информационной безопасности РФ.
- **Итоговый блок:** Защита комплексных проектов, повторение и волонтерская практика (проведение пятиминуток безопасности для младших классов).

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

(1 ЧАС В НЕДЕЛЮ. ВСЕГО: 34 ЧАСА)

№ урока	Тема урока	Кол-во часов	Верифицированные ЭОР / ЦОР
Глава 1 **Безопасность общения и личных данных в сети (14 часов)**			
1	Общение в социальных сетях и мессенджерах: назначение и история развития	1	ФГИС «Моя школа» / Библиотека ЦОК
2	Пользовательский контент и правила создания цифрового образа	1	Российская электронная школа (РЭШ)
3	Персональные данные как капитал личного пространства	1	ФГИС «Моя школа»
4	Настройка профиля пользователя и правила добавления в друзья	1	Библиотека ЦОК
5	Создание и правила хранения сложных паролей. Онлайн-генераторы	1	ФГИС «Моя школа»
6	Способы аутентификации и защита аккаунтов от взлома	1	РЭШ
7	Цифровая гигиена при работе на чужих (публичных) компьютерах	1	Библиотека ЦОК
8	Настройки конфиденциальности в соцсетях и мессенджерах	1	ФГИС «Моя школа»
9	Овершеринг: риски избыточной публикации личной информации	1	РЭШ
10	Кибербуллинг: как распознать манипуляции и защитить себя	1	Библиотека ЦОК
11	Способы помощи жертвам агрессии в интернете	1	ФГИС «Моя школа»
12	Публичные страницы: правила ведения и настройки приватности	1	РЭШ
13	Фишинг: маркеры мошеннических сайтов и защита от них	1	Библиотека ЦОК

14	Защита индивидуальных и групповых проектов по Главе 1	1	Портал проектов edsoo.ru
Глава 2 Безопасность устройств (8 часов)			
15	Что такое вредоносный код? Классификация цифровых угроз	1	ФГИС «Моя школа»
16	Возможности и деструктивные функции современных вирусов	1	Библиотека ЦОК
17	Основные способы доставки и распространения вредоносного кода	1	РЭШ
18	Алгоритм действий при обнаружении заражения устройства	1	ФГИС «Моя школа»
19	Антивирусные программы, их характеристики и правила выбора	1	Библиотека ЦОК
20	Особенности мобильных угроз и защита смартфонов	1	РЭШ
21	Безопасность при установке приложений из сторонних источников	1	ФГИС «Моя школа»
22	Защита практических кейсов по безопасности устройств	1	Портал проектов edsoo.ru
Глава 3 Безопасность информации и цифровая гигиена (12 часов)			
23	Приемы социальной инженерии: как распознать психологическое давление	1	Библиотека ЦОК
24	Способы противодействия манипуляциям при виртуальных контактах	1	ФГИС «Моя школа»
25	Ложная информация и фейковые новости в Интернете	1	РЭШ
26	Методы проверки достоверности информации из разных источников	1	Библиотека ЦОК
27	Безопасность при использовании банковских карт и онлайн-покупках	1	ФГИС «Моя школа»
28	Транзакции в сети: оценка рисков мошенничества	1	РЭШ
29	Уязвимости беспроводных сетей. Работа в публичном Wi-Fi	1	Библиотека ЦОК
30	Резервное копирование данных: правила создания бэкапов	1	ФГИС «Моя школа»

31	Государственная политика РФ в области информационной безопасности	1	Библиотека ЦОК
32	Конституционные права граждан в цифровом пространстве	1	РЭШ
33	Итоговая защита проектно-исследовательских работ	1	Портал проектов edsoo.ru
34	Волонтерская практика: проведение уроков цифровой гигиены	1	Материалы ФГИС «Моя школа»

СПИСОК ИСТОЧНИКОВ И МЕТОДИЧЕСКИХ МАТЕРИАЛОВ

Официальные нормативно-правовые источники и государственные платформы

Портал «Единое содержание общего образования» — официальный конструктор рабочих программ и реестр ФРП. URL: https://edsoo.ru (дата обращения: 15.09.2026).

ФГИС «Моя школа» — федеральная государственная информационная система. Доступ к Универсальной библиотеке цифрового образовательного контента (Библиотека ЦОК). URL: https://myschool.edu.ru.

Российская электронная школа (РЭШ) — интерактивные уроки и методические материалы по цифровой гигиене. URL: https://resh.edu.ru.

Информационно-образовательный портал «Единыйурок.рф» — верифицированная Минпросвещения России площадка по сопровождению ФГОС и обучению ИБ. URL: https://единыйурок.рф.

Научно-методическая литература и материалы экспертных организаций

Информационно-аналитический журнал «Дети в информационном обществе» / Под ред. Г. У. Солдатовой. — М.: Фонд Развития Интернет (издается при поддержке Минпросвещения РФ и Роскомнадзора, действующее свидетельство ПИ ФС77-45884). URL: http://detionline.com/journal/about.

Солдатова Г. У., Нестик Т. А., Рассказова Е. И. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования. — М.: Фонд Развития Интернет.

Методические материалы экспертного портала «Защита детей со вкусом» Лаборатории Касперского. — URL: https://kids.kaspersky.ru/.

Учебно-методические проекты Института коррекционной педагогики (ИКП РАО) по адаптации курсов безопасности. — URL: https://ikp-rao.ru.

ТРЕБОВАНИЯ К СОДЕРЖАНИЮ И ОЦЕНИВАНИЮ ИТОГОВЫХ ПРОЕКТНО-ИССЛЕДОВАТЕЛЬСКИХ РАБОТ

В соответствии с Блоком 3 (Оценочные материалы) и целями ФРП ООО, каждый из трех разделов 34-часового курса завершается выполнением и защитой индивидуального или группового проекта.

А) Критерии оценивания текста и структуры проектной работы

Актуальность и научный аппарат: Во введении четко сформулирована личностная и социальная значимость выбранной проблемы информационной безопасности. Ограничен и определен научный аппарат: цель, задачи, объект, предмет исследования и корректная рабочая гипотеза.

Планирование и междисциплинарность: Наличие поэтапного плана реализации проекта и фиксация корректировок в зависимости от промежуточных результатов. Продемонстрирован междисциплинарный подход (связь информационной безопасности с Информатикой, Математикой, Обществознанием и ОБЗР).

Анализ данных и уникальность: Проведен самостоятельный сбор и анализ данных (опросы класса, чек-листы), выполнено сопоставление своего проектного решения с существующими аналогами, библиография и ЭОР оформлены по ГОСТу.

Стиль и выводы: Соблюдены строгие нормы научного стиля изложения. Присутствует обоснованная оценка результативности проекта с точки зрения его социокультурных последствий (например, польза разработанной памятки для школы).

Б) Критерии презентации и публичной защиты проекта

Коммуникативные навыки и регламент: Свободное владение риторическими умениями, точное использование терминологической системы кибербезопасности, отсутствие стилистических ошибок и строгое соблюдение временного регламента (до 7 минут).

Ответы на вопросы: Проявление аргументированности, стрессоустойчивости и глубины знаний при ответах на уточняющие вопросы аудитории и педагога после презентации.

Качество ИТ-продукта: Создание качественной интерактивной презентации или буклета с использованием современных ИТ-технологий на уровне, соответствующем возрасту 13–14 лет.

Оригинальность и практическая ценность: Творческий подход к созданию конечного продукта проекта (разработка действующего программного скрипта, макета, видеоролика, чек-листа или наглядного пособия для волонтерской практики).

Коллаборация и командная работа: Для групповых проектов — четкое распределение ролей, умение выстраивать сотрудничество внутри команды, проявление взаимного уважения и создание единого сетевого или коллективного продукта.