

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Министерство образования Самарской области

Автономная некоммерческая образовательная организация средняя

общеобразовательная школа «Сота»

АНОО СОШ "СОТА"

РАССМОТРЕНА

на заседании кафедры
ЕМН _____

Очеповский А.В.

Протокол №1
от «21» августа 2026 г.

ПРИНЯТО

на заседании
педагогического
совета

Протокол №1
от «21» августа 2026 г.

УТВЕРЖДЕНА

Директор АНОО СОШ
«Сота» _____ Гендель И.А.

Приказ № 42-ОД
от «21» августа 2026 г.



СОТА
Школа нового
поколения

O="АНОО СОШ ""
СОТА""", CN="Гендель
Ирина Абрамовна,
директор", E=
sota_school@mail.ru
0x 00 FE BB 13 5A 73 87
C4 F5
2026.08.26
15:34:45
+04'00'

**РАБОЧАЯ ПРОГРАММА КУРСА ВНЕУРОЧНОЙ
ДЕЯТЕЛЬНОСТИ**

«Цифровая гигиена»

для обучающихся 7 классов

г.о.Тольятти, 2026

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа курса внеурочной деятельности «Цифровая гигиена» для 7 класса разработана в соответствии с актуальной нормативно-правовой базой Российской Федерации и локальными актами образовательной организации:

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».
2. Федеральный государственный образовательный стандарт основного общего образования, утвержденный Приказом Минпросвещения России от 31.05.2021 № 287 (в ред. Приказа Минпросвещения России от 18.07.2022 № 568).
3. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
5. Концепция информационной безопасности детей в Российской Федерации (Распоряжение Правительства РФ от 28.04.2023 № 1105-р).
6. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (Указ Президента РФ от 09.05.2017 № 203).
7. Основная образовательная программа основного общего образования (ООП ООО) и локальные нормативные акты АНОО СОШ «Сота».

Общая характеристика и актуальность курса

В подростковом возрасте (7 класс) цифровая среда становится ключевым пространством социализации, поиска информации,

коммуникации и формирования личности. При этом учащиеся сталкиваются с рисками: утечкой персональных данных, социальной инженерией, фишингом, кибербуллингом, алгоритмическими «информационными пузырями», клиповым мышлением, интернет-зависимостью, а также манипуляциями с применением генеративного ИИ (дипфейки, генерация дезинформации).

Курс «Цифровая гигиена» логически продолжает линию медиаграмотности 5–6 классов (где закладывались основы информационной культуры и веб-верстки) и предваряет аналитический курс 8 класса (работа с ИИ-ассистентами и программирование на Python). Программа 7 класса ориентирована на формирование устойчивых поведенческих паттернов: осознанное управление личным цифровым следом, аудит безопасности аккаунтов, распознавание манипуляций, фактчекинг и соблюдение баланса между виртуальной и реальной жизнью.

Цели и задачи курса

Цель курса: формирование у обучающихся 7 класса системной цифровой грамотности, осознанной культуры безопасности, критического мышления и практических навыков защиты личных данных и психологического благополучия в интернет-среде.

Задачи курса:

- сформировать понимание механизмов формирования цифрового следа и обучить методам минимизации репутационных и киберрисков;
- освоить практические приемы защиты аккаунтов, двухфакторной аутентификации, безопасного использования публичных сетей и шифрования данных;
- изучить методы социальной инженерии, схемы онлайн-мошенничества и алгоритмы противодействия им;

- обучить инструментам фактчекинга, анализу достоверности источников информации и распознаванию синтетического медиаконтента (дипфейков);
- сформировать навыки бесконфликтного общения, распознавания кибербуллинга и троллинга, алгоритмы правовой и психологической самозащиты;
- привить нормы цифрового детокса, тайм-менеджмента и профилактики экранной зависимости.

Место курса в учебном плане

Курс реализуется в рамках плана внеурочной деятельности АНОО СОШ «Сота».

- Объем учебной нагрузки: **34 академических часа в год** (1 час в неделю, 34 учебные недели).
- Формат занятий: практико-ориентированный (интерактивный разбор кейса/теории - 10 минут, практикум/лабораторный аудит за ПК - 25 минут, рефлексия и чек-листы - 5 минут).

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ КУРСА

Личностные результаты

- **Гражданское и патриотическое воспитание:** уважение к законам РФ в сфере защиты информации и персональных данных, неприятие противоправных действий в сети, понимание значимости отечественных платформ и доверенных сервисов.
- **Духовно-нравственное воспитание:** ориентация на морально-этические стандарты сетевого общения, эмпатия, категорическое неприятие травли (кибербуллинга), сетевой агрессии и распространения чужих приватных данных (доксинга).

- **Ценности научного познания:** развитие критического мышления, устойчивости к дезинформации, когнитивным искажениям и алгоритмическим манипуляциям.
- **Культура здоровья и эмоциональное благополучие:** умение выстраивать баланс онлайн/офлайн, осознанное ограничение экранного времени, противодействие зависимости от уведомлений и соцсетей.
- **Трудовое воспитание и профориентация:** знакомство с направлениями в сфере кибербезопасности (специалист по информационной безопасности, OSINT-аналитик, эксперт по защите данных).

Метапредметные результаты (УУД)

Познавательные УУД:

- *Базовые логические действия:* сопоставлять факты и мнения, выявлять причинно-следственные связи между действиями пользователя в сети и их последствиями.
- *Базовые исследовательские действия:* проводить OSINT-самоаудит (поиск общедоступных сведений о себе), верифицировать подлинность цифровых артефактов (фото, видео, веб-страниц).
- *Работа с информацией:* оценивать надежность веб-ресурсов, сопоставлять несколько независимых источников, структурировать информацию в чек-листы и ментальные карты.

Коммуникативные УУД:

- *Общение:* корректно формулировать позицию в виртуальной коммуникации, противостоять провокациям и манипулятивным приемам собеседников.
- *Совместная деятельность:* участвовать в командном разборе инцидентов безопасности (Capture The Flag / киберквесты),

вырабатывать совместные правила кибербезопасности для классного сообщества.

Регулятивные УУД:

- *Самоорганизация:* формировать личные правила информационной гигиены, планировать график использования гаджетов.
- *Самоконтроль:* регулярно осуществлять проверку настроек конфиденциальности, критически анализировать собственные цифровые привычки.

Предметные результаты

К концу 7 класса обучающийся научится:

- классифицировать виды угроз в цифровом пространстве (вредоносное ПО, фишинг, социальная инженерия, доксинг, киберсталкинг);
- проводить аудит собственного цифрового следа и настраивать параметры приватности в социальных сетях, мессенджерах и операционных системах;
- создавать и администрировать сложные пароли с применением менеджеров паролей и обязательной двухфакторной аутентификации (2FA);
- выявлять признаки фишинговых сайтов, вредоносных ссылок и поддельных писем/сообщений в мессенджерах;
- безопасно использовать общественные сети Wi-Fi, мобильные приложения (анализ разрешений) и облачные хранилища;
- применять инструменты базового фактчекинга (обратный поиск по картинкам, проверка доменных имен, верификация метаданных);
- распознавать манипулятивные техники (кликбейт, фейковые новости, синтетические медиа / дипфейки);

- применять корректные правовые и психологические алгоритмы действий при столкновении с кибербуллингом, шантажом или мошенничеством;
- рассчитывать личный экранный баланс и применять инструменты цифрового детокса.

3. СОДЕРЖАНИЕ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ (34 часа)

Раздел 1. Личная цифровая безопасность и приватность (9 часов)

Цифровой след: пассивный и активный. Чем опасен цифровой отпечаток личности. Понятие персональных данных и правовые основы их защиты (ФЗ-152). Архитектура современных паролей: методы подбора (брутфорс, утечки баз), менеджеры паролей. Двухфакторная аутентификация (2FA) через SMS, приложения-аутентификаторы и аппаратные ключи. Безопасность мобильных устройств: ревизия разрешений приложений (доступ к камере, микрофону, геолокации). Угрозы публичных сетей Wi-Fi и защита интернет-соединения (VPN, протокол HTTPS). Цифровая гигиена браузера: куки (cookies), трекеры, режим инкогнито и блокировщики слежки. Практикум: комплексный аудит приватности личных аккаунтов.

Раздел 2. Социальная инженерия, мошенничество и киберугрозы (8 часов)

Психологические триггеры социальной инженерии (страх, спешка, жадность, жалость). Фишинг: разновидности (почтовый, в мессенджерах, смишинг, вишинг). Анатомия поддельных сайтов и клонов сервисов. Вредоносное программное обеспечение: вирусы, трояны, шифровальщики (ransomware), шпионское ПО (spyware). Мошенничество в онлайн-играх: кража игровых аккаунтов, скинов, мошеннические платформы доната.

Дропперство и финансовая безопасность подростков в сети. Алгоритмы действий при взломе и компрометации данных. Лаборатория: расследование учебных кейсов сетевых атак.

Раздел 3. Фактчекинг, медиаграмотность и защита от манипуляций (9 часов)

Информационный шум, кликбейт и феномен FOMO (страх упустить выгоду). Алгоритмы рекомендательных систем и эффект «информационного пузыря». Дезинформация и мисинформация: цели распространения фейков. Инструменты фактчекинга: обратный поиск по изображениям, проверка даты первоисточника, проверка доменной зоны через Whois. Технологии искусственного интеллекта в медиа: дипфейки (Deepfake), клонирование голоса, генерация фальшивых скриншотов и документов. Правовая ответственность за распространение заведомо ложной информации. Практикум: верификация сомнительного инфоповода и составление аналитического отчета.

Раздел 4. Цифровая культура, этика и цифровой баланс (8 часов)

Сетевой этикет (нетикет) в школьных и публичных чатах. Токсичность, троллинг, флейминг. Кибербуллинг: роли (агрессор, жертва, свидетель), последствия, юридические и психологические инструменты защиты. Доксинг, киберсталкинг и овершеринг: почему нельзя публиковать билеты, геометки дома и документы. Влияние цифровой среды на нервную систему: клиповое мышление, прокрастинация, дофаминовые петли. Практики цифрового детокса и настройка экранного времени. Разработка и публичная защита итогового проекта: «Кодекс цифровой гигиены подростка».

4. ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ (7 класс, 34 часа)

№ п/п	Наименование разделов и тем	Кол-во часов	Форма проведения	Основные виды деятельности обучающихся	Электронные (цифровые) образовательные ресурсы
Раздел 1	Личная цифровая безопасность и приватность	9			
1.1	Цифровой след: что интернет помнит о нас?	1	Беседа, интерактивный опрос	Анализ понятия цифрового следа, классификация активных и пассивных следов пользователя.	Образовательный проект «КиберЗОЖ: Цифровой след» (https://киберзож.рф), портал ФГИС «Моя школа».
1.2	Персональные данные и закон: границы приватности	1	Практикум	Определение состава персональных данных, разбор пользовательских соглашений и рисков их передачи.	Портал Роскомнадзора «Персональные данные. дети» (https://персональныеданные.дети), база законов «КонсультантПлюс».
1.3	Архитектура надежного пароля и менеджеры паролей	1	Практикум	Создание устойчивых мнемонических паролей, тестирование стойкости к взлому, знакомство с менеджерами паролей.	Сервис проверки паролей Kaspersky Password Check (https://password.kaspersky.com/ru/), тренажер «Цифровой ликбез».
1.4	Двухфакторная аутентификация (2FA): двойной замок	1	Лабораторная работа	Настройка 2FA в учебных сервисах, использование приложений-генераторов кодов (Яндекс Ключ).	Инструкции безопасности портала Госуслуги (https://gosuslugi.ru), интерактивный курс платформы Stepik .
1.5	Безопасность	1	Практикум	Анализ разрешений	Обучающие материалы «Урок

	мобильных устройств: ревизия разрешений			мобильных приложений (доступ к GPS, микрофону, контактам), отключение избыточных прав.	цифры: Безопасность мобильных устройств» (https://урокцифры.рф).
1.6	Общественный Wi-Fi и шифрование трафика (HTTPS, VPN)	1	Беседа, практикум	Разбор рисков атак Man-in-the-Middle в открытых сетях, проверка SSL/TLS-сертификатов сайтов.	Тренажер «РЭШ: Сетевая безопасность» (https://resh.edu.ru), симулятор сетевых протоколов.
1.7	Слежка в браузере: cookies, трекеры и режим инкогнито	1	Практикум	Исследование механизмов контекстной рекламы, настройка блокировки сторонних cookies и трекеров.	Тест приватности браузера Cover Your Tracks (https://coveryourtracks.eff.org), настройки Яндекс Браузера .
1.8	Облачные хранилища: безопасный обмен файлами	1	Практикум	Настройка уровней доступа к файлам и папкам по ссылке, разграничение прав просмотра и редактирования.	Сервис Яндекс Диск (https://disk.yandex.ru), образовательная платформа «Сетевичок.рф».
1.9	Практикум: Комплексный аудит личной кибербезопасности	1	Лабораторная работа	Проведение самодиагностики и личных устройств и профилей по чек-листу безопасности, устранение уязвимостей.	Интерактивный чекер « Лаборатория Касперского: Проверь себя », онлайн-доска SBoard .
Раздел 2	Социальная инженерия	8			

	мошенничество и киберугрозы				
2.1	Психология обмана: основы социальной инженерии	1	Беседа, разбор кейсов	Выявление манипулятивных приемов (давление на страх, срочность, авторитет), построение модели защиты.	Проект Минфина и Банка России « Финансовая культура » (Fincult.info), видеоматериалы проекта «Цифровой ликбез».
2.2	Фишинг: как распознать поддельное письмо и сайт-клон	1	Лабораторная работа	Анализ доменных имен, выявление опечаток (тайпсквоттинг), проверка подлинности URL-ссылок.	Интерактивный фишинг-квиз Google / Jigsaw Phishing Quiz (https://phishingquiz.withgoogle.com), платформа Stepik .
2.3	Вредоносное ПО: классификация и методы заражения	1	Беседа, практикум	Знакомство с принципами работы троянов, вымогателей и шпионских программ; правила работы антивирусного ПО.	Материалы портала « Лига безопасного интернета », тренажер « Урок цифры: Кибербезопасность ».
2.4	Игровое онлайн-мошенничество: скины, донаты, аккаунты	1	Практикум	Анализ мошеннических схем в популярных онлайн-играх, правила безопасной торговли виртуальными предметами.	Портал детской кибербезопасности « Веб-ландия », памятки сервиса VK Защита .
2.5	Телефонные и мессенджер-мошенники: правила реагирования	1	Ролевой тренинг	Отработка сценариев прерывания подозрительных звонков и сообщений от имени	Просветительский ресурс МВД России « Киберполиция » (https://мвд.рф), портал « КиберЗОЖ ».

				банков/ведомств.	
2.6	Опасность «легкого заработка»: дропперство и вовлечение	1	Профилактическая беседа	Разбор правовых последствий передачи банковских карт третьим лицам и участия в сомнительных схемах.	Образовательные материалы Банка России, платформа «Единый урок безопасности».
2.7	Алгоритм действий при взломе аккаунта или краже данных	1	Практикум	Составление пошаговой инструкции восстановления доступа, отзыва сессий и уведомления контактов.	Справочный центр Госуслуги / VK Support, интерактивная доска Miro / SBoard.
2.8	Киберквест : Расследование инцидента безопасности	1	Деловая игра / Квест	Поиск уязвимостей и распутывание смоделированной фишинговой атаки в командной среде.	Обучающая платформа Кибербитва / Capture The Flag (детский трек).
Раздел 3	Фактчекинг, медиаграмотность и защита от манипуляций	9			
3.1	Информационный шум, кликбейт и клиповое мышление	1	Беседа, практикум	Анализ механизмов привлечения внимания, выявление кликбейтных заголовков и манипулятивной верстки.	Проект «Грамота.ру: Медиатекст» (https://gramota.ru), электронная библиотека ФГИС «Моя школа».
3.2	Рекомендательные алгоритмы и «информационные пузыри»	1	Исследование	Анализ работы лент рекомендаций, поиск способов выхода из	Просветительский курс «Яндекс Учебник: Как работают алгоритмы».

	ионный пузырь»			алгоритмического пузыря предпочтений.	
3.3	Фейковые новости: типология, цели и механика вирусности	1	Практикум	Классификация фейков (намеренная ложь, сатира, ошибка), выявление эмоциональных триггеров вирусного контента.	Портал проверки информации « Лапша Медиа » (https://lapsha.media), ресурс « Урок цифры ».
3.4	Базовый фактчекинг : проверка первоисточников и дат	1	Лабораторная работа	Поиск первичного источника новости, проверка архивных копий веб-страниц и доменов через Whois.	Сервис архивных веб-страниц Web Archive (https://archive.org), база сервисов проверки доменов Whois .
3.5	Анализ изображений: обратный поиск и поиск ретуши	1	Лабораторная работа	Выявление фотомонтажа, поиск первоисточника фото через поисковые системы и анализ EXIF-метаданных.	Сервисы визуального поиска Яндекс Картинки , Google Images , инструмент анализа метаданных FotoForensics .
3.6	Дипфейки (Deepfake) и синтез голоса: маркеры подделки	1	Лабораторная работа	Исследование артефактов нейросетевых видео и синтезированной речи, составление чек-листа проверки.	Образовательный проект « Цифровой ликбез: Искусственный интеллект и дипфейки ».
3.7	Модели генеративного ИИ: фактчекинг «галлюцинаций»	1	Практикум	Анализ ответов языковых моделей, выявление фактологических ошибок и	Отечественные диалоговые системы GigaChat (https://gigachat.sber.ru), YandexGPT .

				вымышленных цитат.	
3.8	Правовые основы: ответственность за клевету и фейки	1	Беседа, практикум	Знакомство со статьями УК РФ и КоАП РФ, регулирующим и распространение недостоверных сведений.	Информационно-правовая система «Гарант / КонсультантПлюс», портал детской правовой помощи.
3.9	Практикум: Верификация сомнительного медиакейса	1	Практическая работа	Комплексная проверка резонансной новости по алгоритму фактчекера с оформлением аналитического отчета.	Текстовый редактор МойОфис / Яндекс Документы , шаблон аналитической справки.
Раздел 4	Цифровая культура, этика и цифровой баланс	8			
4.1	Сетевой этикет: культура переписки в школьных чатах	1	Беседа, практикум	Формулирование правил вежливой и эффективной коммуникации, избегание голосового и текстового спама.	Платформа коммуникаций «Сферум» в VK Мессенджере (https://sferum.ru), проект «Цифровой ликбез».
4.2	Троллинг, хейтинг и флейминг: стратегии реагирования	1	Практикум-тренинг	Отработка тактик «не корми тролля», алгоритмы блокировки агрессоров и сохранения доказательств.	Методические материалы Центра защиты прав и интересов детей (https://fcprc.ru), ресурс «КиберЗОЖ».
4.3	Кибербуллинг: алгоритмы правовой и личной защиты	1	Семинар, разбор ситуаций	Разбор алгоритма действий для жертвы и свидетеля травли:	Горячая линия помощи «Дети онлайн» (http://detionline.com), портал

				фиксация улик, обращение к взрослым и юристам.	Травли.нет (https://travli.net).
4.4	Овершеринг, доксинг и сталкерство: защита границ	1	Практикум	Анализ опасностей публикации геолокации, билетов, личных фото; правила сокрытия конфиденциальных данных.	Памятки проекта «Безопасный интернет для детей» , портал «Сетевичок» .
4.5	Дофаминовые петли: почему приложения крадут внимание	1	Беседа, самоисследование	Разбор механик бесконечной ленты, push-уведомлений и геймификации в интерфейсах сервисов.	Научно-популярные видеоматериалы проекта «Урок цифры» , лекторий общества «Знание» .
4.6	Экранный баланс и техники цифрового детоксинга	1	Практикум	Анализ статистики экранного времени на личных смартфонах, настройка лимитов и режима «Не беспокоить».	Встроенные утилиты ОС (Цифровое благополучие / Экранное время), трекеры полезных привычек.
4.7	Разработка проекта «Кодекс цифровой гигиены 7 класса»	1	Проектная мастерская	Создание интерактивных памяток, инфографики и плакатов с правилами кибербезопасности для школы.	Графический редактор Холст / Flyvi , онлайн-доска SBoard .
4.8	Публичная защита проектов и подведение итогов года	1	Защита проектов / Конференция	Презентация разработанных памяток и гайдов, итоговое тестирование цифровой грамотности.	Мультимедийное оборудование, электронный банк проектов школы.

ИТОГО		34			
--------------	--	-----------	--	--	--