

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

О="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
15:35:11
+04'00'

РАБОЧАЯ ПРОГРАММА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

«Цифровая гигиена»

для обучающихся 9 классов

г.о.Тольятти, 2026

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа курса внеурочной деятельности «Цифровая гигиена» для 9 класса составлена в соответствии с требованиями следующих нормативно-правовых и методических документов:

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. Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 № 646).
6. Стратегия комплексной безопасности детей в Российской Федерации на период до 2030 года (Указ Президента РФ от 17.05.2023 № 358).
7. Основная образовательная программа основного общего образования (ООП ООО) и локальные нормативные акты АНОО СОШ «Сота».

Общая характеристика и специфика курса

Курс «Цифровая гигиена» в 9 классе является завершающим звеном предпрофильной подготовки школьников в области информационной безопасности и культуры цифрового взаимодействия. В отличие от базовой пропедевтики 5–6 классов и прикладной личной безопасности 7 класса, программа 9 класса ориентирована на углубленный аналитический, правовой и профориентационный уровень.

Курс комплексно рассматривает глобальные вызовы информационного общества: противодействие сложным сценариям социальной инженерии, целевым кибератакам (Advanced Persistent Threats), деструктивным сетевым движениям, манипуляциям общественным мнением, глубоким нейросетевым подделкам (дипфейкам нового поколения) и правовым рискам при создании и распространении цифрового контента.

Цели и задачи курса

Цели курса:

- сформировать системные аналитические компетенции и правовую грамотность в сфере защиты личной, корпоративной и государственной информации;
- развить навыки критического противодействия информационным манипуляциям, таргетированному воздействию и деструктивному сетевому контенту;
- подготовить выпускников основной школы к осознанному выбору профиля обучения и профессиональной траектории в IT и сфере кибербезопасности.

Задачи курса:

- изучить архитектуру современных киберугроз, принципы работы криптографических протоколов и систем защиты информации;
- освоить методы анализа цифрового следа методами открытой разведки (OSINT-исследования) и алгоритмы защиты от доксинга;
- сформировать понимание правовой и уголовной ответственности за правонарушения в сфере компьютерной информации и телекоммуникаций (глава 28 УК РФ);

- изучить механизмы алгоритмического профилирования, манипуляции поведением через Big Data и рекомендательные системы;
- обучить профессиональным приемам медиаэкспертизы, цифровой криминалистики (форензики) и верификации контента, созданного генеративным ИИ;
- разработать и защитить индивидуальный или групповой исследовательский проект в сфере информационной безопасности.

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: проблемные дискуссии, аналитические практикумы за ПК, решение практических кейсов (кейс-стади), лабораторные работы по форензике и OSINT, защита проектных исследований.

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ КУРСА

Личностные результаты

- **Гражданское и патриотическое воспитание:** глубокое понимание национальных интересов РФ в информационной сфере, осознание личной гражданской ответственности за соблюдение цифрового суверенитета и законодательства страны.
- **Духовно-нравственное воспитание:** устойчивое неприятие любых форм деструктивного поведения (экстремизм, хейтспич, колумбайн-сообщества, доксинг), следование этике ответственного использования цифровых технологий.

- **Ценности научного познания:** владение исследовательскими методами анализа данных, сформированность системного критического мышления при взаимодействии с медиапространством.
- **Трудовое воспитание и профориентация:** осознанная ориентация на специальности в области кибербезопасности, белого хакинга (пентестинга), цифровой криминалистики, продуктовой безопасности и права в IT.
- **Культура здоровья и безопасность:** навыки предотвращения синдрома хронической информационной усталости, сохранение психологической устойчивости в условиях информационных войн и атак.

Метапредметные результаты (УУД)

Познавательные УУД:

- *Базовые логические действия:* проводить многофакторный системный анализ инцидентов информационной безопасности; сопоставлять гипотезы с техническими доказательствами; выявлять манипулятивные нарративы.
- *Базовые исследовательские действия:* осуществлять OSINT-поиск и анализ первичных данных; применять методы цифровой криминалистики для верификации медиафайлов.
- *Работа с информацией:* оценивать достоверность, полноту и юридическую легитимность информации; выстраивать матрицы угроз и структурировать аналитические справки.

Коммуникативные УУД:

- *Общение:* аргументированно вести дискуссии по правовым и этическим вопросам цифровой эпохи; составлять официальные мотивированные обращения в службы поддержки и надзорные органы.

- *Совместная деятельность:* координировать командные роли при расследовании смоделированных киберинцидентов, распределять зоны ответственности.

Регулятивные УУД:

- *Самоорганизация:* самостоятельно выстраивать стратегию эшелонированной защиты личных цифровых активов; планировать этапы проектного исследования.
- *Самоконтроль:* регулярно анализировать и купировать риски компрометации личных данных; объективно оценивать уровень надежности используемых IT-систем.

Предметные результаты

К концу 9 класса обучающийся научится:

- классифицировать векторы атак и модели угроз в современных IT-системах (DDoS, MITM, целевой фишинг, уязвимости нулевого дня);
- применять методы симметричного и асимметричного шифрования, открытые PGP-ключи, цифровые сертификаты и электронную подпись;
- проводить комплексный OSINT-аудит цифрового присутствия человека или организации в открытых источниках;
- квалифицировать противоправные действия в сети в соответствии с нормами УК РФ (ст. 137, 138, 272–274.1) и КоАП РФ;
- распознавать технологии скрытого влияния, деструктивные сообщества, вербовочные методики и применять протоколы противодействия;
- использовать специализированные программные инструменты форензики и фактчекинга для детекции сгенерированного ИИ контента (дипфейков, синтезированного голоса, клонов документов);

- применять принципы «нулевого доверия» (Zero Trust) при взаимодействии с корпоративными и персональными информационными системами;
- разрабатывать комплексную документацию, чек-листы и проекты по аудиту информационной безопасности организаций и пользователей.

3. СОДЕРЖАНИЕ КУРСА (34 часа)

Раздел 1. Кибербезопасность систем и криптографическая защита (9 часов)

Архитектура компьютерных сетей и модели угроз. Принципы криптографии: симметричное и асимметричное шифрование. Хэш-функции, контрольные суммы (MD5, SHA-256) и проверка целостности файлов. Электронная цифровая подпись (ЭЦП) и сквозное шифрование (End-to-End Encryption) в мессенджерах. Уязвимости беспроводных и проводных сетей, концепция Zero Trust (нулевого доверия). Виртуальные частные сети (VPN), DNS-over-HTTPS и анонимизация трафика. Резервное копирование по схеме «3-2-1» и защита от программ-вымогателей (Ransomware). Практикум: криптографическая защита конфиденциальных документов.

Раздел 2. OSINT, цифровой след и защита от доксинга (8 часов)

Разведка по открытым источникам (OSINT): теория, правовые границы и инструментарий. Геолокация по фото, анализ метаданных EXIF. Поиск утечек баз данных, анализ уязвимостей цифрового следа. Доксинг (деанонимизация) и киберсталкинг: мотивы, механизмы реализации и защита. Социальная инженерия уровня Enterprise: целевой фишинг (Spear Phishing), бизнес-компрометация (BEC), подделка личности руководителя. Практикум: проведение учебного OSINT-расследования и деанонимизация следов в сети.

Раздел 3. Информационные войны, деструктивный контент и фактчекинг 2.0 (9 часов)

Информационные операции, сетевые ботнеты и астротурфинг (имитация общественного мнения). Алгоритмы вовлечения в деструктивные сообщества, вербовка и кибербуллинг в подростковой среде. Синтетические медиа: дипфейки видео и аудиоряда нового поколения, выявление артефактов нейросетей. Форензика изображений: ELA-анализ (Error Level Analysis), верификация источников. Правовое регулирование: ответственность за экстремизм, дискредитацию, распространение фейков и неправомерный доступ к информации (ст. 272 УК РФ). Лаборатория: экспертиза спорного медиамассива.

Раздел 4. Проектная деятельность и культура киберустойчивости (8 часов)

Основы проектирования комплексных систем информационной безопасности. Разработка нормативно-методических рекомендаций по цифровой гигиене для школы и семьи. Подготовка, оформление и защита прикладного исследовательского проекта в сфере кибербезопасности и медиагигиены (темы: «Аудит уязвимостей школьного сообщества», «Детектор нейросетевых фейков», «Памятка по противодействию социальной инженерии»). Итоговая конференция по кибербезопасности.

4. ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

(9 класс, 34 часа)

№ п/п	Наименование разделов и тем	Кол-во часов	Форма проведения	Основные виды деятельности обучающихся	Электронные (цифровые) образовательные ресурсы
Раздел 1	Кибербезопасность систем и криптографическая защита	9			
1.1	Модели киберугроз и концепция Zero Trust (нулевого доверия)	1	Беседа, аналитический практикум	Построение матрицы угроз персональной рабочей станции, разбор концепции эшелонированной защиты.	Образовательный ресурс «КиберЗОЖ: Угрозы» (https://киберзож.рф), портал ФГИС «Моя школа».
1.2	Основы криптографии: симметричное и асимметричное шифрование	1	Практикум	Моделирование работы открытых и закрытых ключей шифрования (RSA, AES), шифрование тестового текста.	Интерактивный эмулятор CrypTool Online (https://www.cryptool.org), платформа Stepik.
1.3	Хэш-функции и проверка целостности файлов (MD5, SHA-256)	1	Лабораторная работа	Расчет хэш-сумм скачанных файлов, проверка неизменности данных, выявление внедренного кода.	Утилиты командной строки (certutil/sha256sum), онлайн-калькулятор хэшей HashCalc Online.
1.4	Электронная подпись (ЭЦП) и сквозное	1	Практикум	Исследование работы цифровых сертификатов, принципов	Просветительский портал «Урок цифры: Безопасность в сети»

	шифрование (E2EE)			работы защищенных протоколов Signal и TLS.	(https://урокцифры.рф).
1.5	Безопасность сетевых соединений: DNS-over-HTTPS и VPN	1	Практикум	Анализ DNS-утечек, настройка защищенных DNS-серверов, сравнение защищенности и протоколов.	Инструмент проверки утечек DNSLeakTest (https://www.dnsleaktest.com), платформа РЭШ .
1.6	Программы-вымогатели (Ransomware) и стратегия бэкапа «3-2-1»	1	Практикум	Настройка автоматического резервного копирования данных на независимые носители и в облако.	Облачная среда Яндекс Диск (https://disk.yandex.ru), проект « Единый урок безопасности ».
1.7	Уязвимости веб-сервисов: SQL-инъекции, XSS и токены сессий	1	Лабораторная работа	Знакомство с принципами работы веб-уязвимостей на учебных безопасных тренажерах OWASP.	Обучающая платформа PortSwigger Web Security Academy (демо-модули) , задачник Stepik .
1.8	Криптографическая защита персональных файлов: утилиты VeraCrypt	1	Практикум	Создание зашифрованного виртуального диска/контейнера для хранения конфиденциальных документов.	Свободное ПО с открытым кодом VeraCrypt (https://veracrypt.fr), видеоинструкции VK Защита .
1.9	Практикум: Настройка комплексной защиты рабочего окружения	1	Лабораторная работа	Аудит настроек безопасности ОС (брандмауэр, политики учетных записей, шифрование BitLocker).	Встроенные утилиты безопасности Windows/Linux, чекер « Лаборатория Касперского ».

Раздел 2	OSINT, цифровой след и защита от доксинга	8			
2.1	Разведка по открытым источникам (OSINT): цели и методы	1	Беседа, разбор кейсов	Изучение методологии поиска открытых данных, анализ легальности и этических рамок OSINT.	Образовательные материалы Музея криптографии (https://cryptography-museum.ru).
2.2	Геолокация и хронолокация по фото- и видеоматериалам	1	Лабораторная работа	Определение места и времени съемки по теньям, архитектуре, метаданным и спутниковым снимкам.	Картографические сервисы Яндекс Карты (панорамы) , Google Earth , инструмент SunCalc .
2.3	Анализ цифрового следа и проверка утечек персональных баз	1	Практикум	Проверка компрометации и личных почтовых адресов и логинов в публичных базах утечек.	Сервис проверки утечек Have I Been Pwned (https://haveibeenpwned.com), портал Госуслуги .
2.4	Доксинг и киберсталкинг : как защитить личные границы	1	Семинар, практикум	Разбор приемов деанонимизации, удаление цифрового следа из агрегаторов данных и спам-баз.	Портал Роскомнадзора « Персональные данные. Дети », проект « КиберЗОЖ ».
2.5	Целевой фишинг (Spear Phishing) и бизнес-атаки (BEC)	1	Разбор кейсов	Выявление таргетированных атак, маскирующихся под официальные запросы государственных органов.	Интерактивный симулятор Jigsaw Phishing Quiz , тренажер « Цифровой ликбез ».

2.6	Социальная инженерия: телефонный спуфинг и дипфейк-звонки	1	Ролевой тренинг	Анализ подделки номеров и голосов близких, составление стоп-слов и протокола семейной проверки.	Проект МВД России «Киберполиция», материалы портала «Финансовая культура».
2.7	Практикум: Учебное OSINT-расследование по открытому профилю	1	Лабораторная работа	Поиск информации о вымышленном персонаже по фрагментарным открытым данным сети.	Поисковые операторы Яндекс / Google , онлайн-доска SBoard для построения графа связей.
2.8	Анализ результатов расследования и защита данных	1	Семинар-дискуссия	Разбор найденных уязвимостей цифрового следа, формирование персонального плана деанонимизации.	Интерактивная доска SBoard , презентационная среда.
Раздел 3	Информационные войны, деструктивный контент и фактчекинг 2.0	9			
3.1	Информационное противоборство, ботнеты и астротурфинг	1	Беседа, исследование	Выявление скоординированных атак ботов, анализ комментариев и накрутки активности в соцсетях.	Аналитический сервис TGStat / Brand Analytics (демо) , портал ФГИС «Моя школа» .
3.2	Деструктивные сетевые движения: вербовка и манипуляции	1	Профилактическая беседа	Анализ психологических крючков радикальных сообществ, алгоритм	Материалы Национального центра информационного противодействия терроризму и

				безопасного выхода и обращения за помощью.	экстремизму (НЦПТИ) (https://ncpti.su).
3.3	Алгоритмическое профилирование и манипуляция вниманием	1	Исследование	Анализ формирования персональных лент на основе Big Data, выход из информационных туннелей.	Видеоматериалы «Урок цифры: Большие данные» (https://урокцифры.рф).
3.4	Продвинутый фактчекинг: проверка первоисточников и метаданных	1	Лабораторная работа	Проверка цепочки цитирования, анализ исходного кода страниц, сопоставление временных меток.	Фактчекинг-портал «Лапша Медиа» (https://lapsha.media), база Web Archive.
3.5	Форензика изображений: EIA-анализ и выявление следов монтажа	1	Лабораторная работа	Исследование уровня сжатия ошибок (Error Level Analysis), поиск клонированных областей на фото.	Онлайн-сервис криминалистического анализа FotoForensics (https://fotoforensics.com), InVID Verification Plugin.
3.6	Дипфейки нового поколения: детекция генеративного контента	1	Лабораторная работа	Выявление микроартефактов, рассинхронизации мимики и неестественного освещения на сгенерированных видео.	Образовательный проект «Цифровой ликбез: Дипфейки», сервис Deepware Scanner.
3.7	Экспертиза текстов, сгенерированных языковыми моделями (LLM)	1	Практикум	Анализ лексических паттернов, проверка фактологии нейросетевых эссе, поиск	Отечественные системы GigaChat, YandexGPT, детекторы сгенерированного текста.

				галлюцинации ИИ.	
3.8	Правовая ответственность за киберпреступления (ст. 272–274 УК РФ)	1	Семинар с разбором судебной практики	Анализ статей УК РФ и КоАП РФ (взлом, распространение вредоносного ПО, клевета, экстремизм).	Информационно-правовая система «КонсультантПлюс / Гарант» .
3.9	Практикум: Экспертиза резонансного медиамассива	1	Лабораторная работа	Комплексная криминалистическая проверка комплекта материалов (текст, фото, видео) с выдачей заключения.	Текстовый процессор МойОфис / Яндекс Документы , шаблон экспертного заключения.
Раздел 4	Проектная деятельность и культура киберустойчивости	8			
4.1	Выбор темы, постановка целей и планирование проекта	1	Проектный семинар	Формулирование ТЗ, выбор темы (аудит безопасности, создание детектора фейков, правовой гайд).	Онлайн-доска Miro / SBoard , облачное хранилище школы.
4.2	Сбор исходных данных и аналитическое исследование	1	Исследовательская работа	Проведение анкетирования, сбор метрик, сопоставление технических решений по выбранной проблеме.	Сервис опросов Яндекс Формы , таблицы МойОфис / Яндекс Таблицы .
4.3–4.4	Разработка проектного продукта	2	Проектная мастерская	Создание итогового программного	Среда верстки VS Code / Tilda , диалоговая

	(стенд, гайд, чекер)			аналитическог о или методическог о продукта проекта.	платформа GigaChat (для ревью текстов).
4.5	Апробация, тестирование и аудит разработанных решений	1	Практикум	Экспертная оценка решений одноклассник ов (Peer-to-Peer ревью), устранение замечаний.	Репозиторий проектов, чек-лист взаимного оценивания.
4.6	Оформление паспорта проекта и презентационн ых материалов	1	Практикум	Оформление пояснительно й записки, структуры презентации и демонстрацио нного стенда.	Редактор Яндекс Презентации , офисный пакет.
4.7–4. 8	Итоговая школьная конференция по кибербезопасн ости	2	Научно-прак тическая конференция / Защита	Публичная защита проектных исследований, демонстрация продуктов, подведение итогов курса ООО.	Мультимедийное демонстрационное оборудование, школьный банк проектов.
ИТО ГО		34			