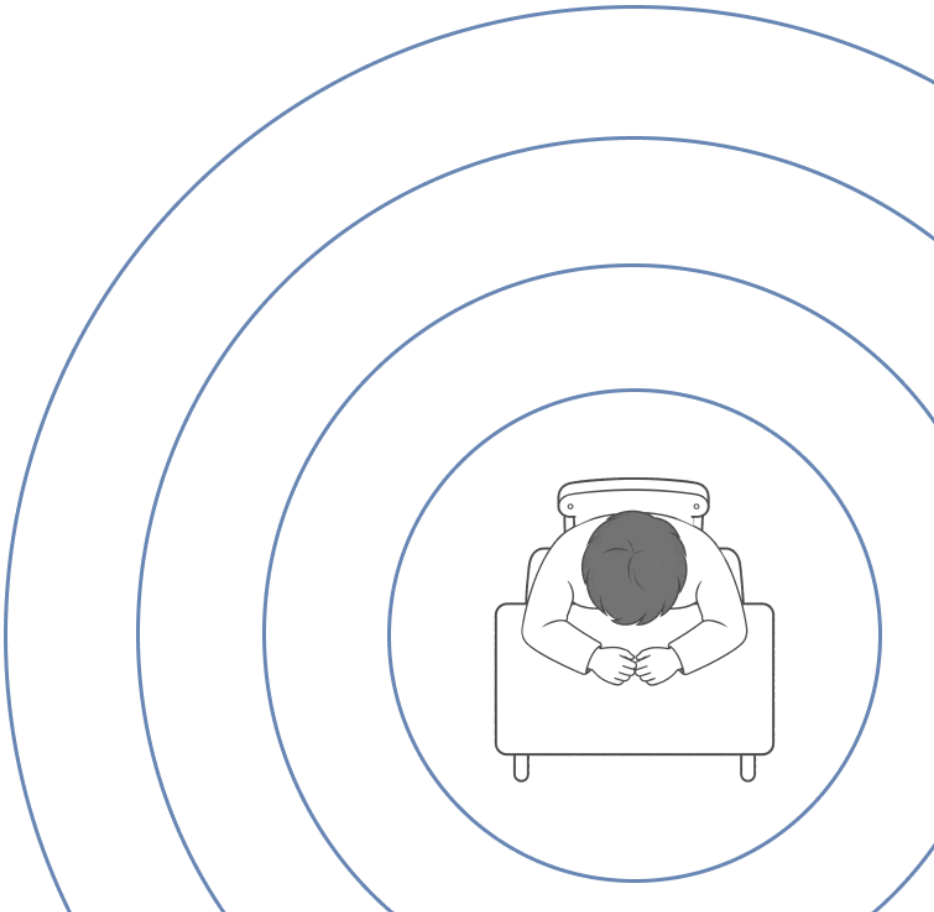
МЕМОРИАЛ
ЦЕНТР ЗАЩИТЫ ПРАВ ЧЕЛОВЕКА

АНАЛИТИЧЕСКИЙ ДОКЛАД | 2026

Четыре периметра цифровой слежки за детьми в российских школах

От профилирования и видеонаблюдения до госсертификатов шифрования и кибердоносительства

Константин Троицкий
Автор доклада



Содержание

Введение ... **3**
Основы цифровой слежки в школах ... **9**
Периметр 1. ФГИС «Моя школа» ... **13**
Данные об ученике и профилирование обучающихся ... 13
Школьные коммуникации: «Сферум» и «Макс» ... 15
Интеграция в единую государственную цифровую архитектуру ... 16
Периметр 2. Видеонаблюдение и аудиоконтроль ... **19**
Режимный доступ и биометрия ... 19
Камеры и микрофоны ... 19
Проекты видеоаналитики ... 22
Периметр 3. Школьные компьютеры и сети ... **25**
Сетевая централизация школ ... 25
Контент-фильтрация и сертификаты шифрования ... 26
Вытеснение личных устройств ... 27
Периметр 4. Мониторинг внешкольной сетевой активности ... **29**
Административно-педагогический мониторинг ... 29
Кибердружины ... 33
Федеральные нейросетевые комплексы и ГИС «Профилактика» ... 34
Строящиеся вспомогательные периметры ... **38**
Детские номера и контроль мобильной связи ... 38
Отслеживание передвижения ... 40
«Эмпатичные» чат-боты и аналитика души ... 41
Центральный пост управления ... 42
Заключение ... **43**
Процитированные источники ... **45**
Библиография ... 45
Документы государственных органов и муниципальных образований ... 50

Введение

В первой декаде XXI века многие эксперты, педагоги и родители приветствовали распространение в школах цифровых технологий, включая те, которые впоследствии стали инструментами слежки[1]. Люди надеялись, что эти изобретения приведут к резкому повышению качества образования и внесут решающий вклад в построение более справедливого, свободного и ненасильственного глобального общества. Однако вскоре эти

[1] Доклад исходит из следующего определения: государственная слежка (state surveillance) – любое рутинное, массовое, сфокусированное и систематическое внимание государственных органов и аффилированных с ними агентов к личным данным и поведению людей в целях сбора информации, управления и репрессий (ср. с Lyon David. *Surveillance*. Oxford: Oxford University Press, 2024).

надежды и воодушевляющие примеры использования новейших технологий были омрачены негативными эффектами их применения при обучении, нередкими случаями прямого злоупотребления ими, а также опасностью их выхода из-под человеческого контроля. Так, сначала демократические силы активно поддерживали распространение интернета, мобильной связи и цифровых медиа, ожидая, что они облегчат доступ к достоверной информации, помогут развить критическое мышление и укрепят уважение к правам и достоинству человека у школьников по всему миру. Однако в реальности авторитарные режимы, рассматривая детей как ресурс для своего самосохранения, смогли приспособить эти же технологии для создания небывалых по эффективности систем подчинения. Наиболее известен случай Китая, чей опыт цифровизации школ для социального инжиниринга несовершеннолетних встретил критику в демократических странах[2], но в то же время стал заимствоваться диктатурами по всему миру, включая российскую[3].

Взгляд российских властей на детей как на удобный материал для поддержания устойчивости режима во многом восходит к советской эпохе, в которой была выстроена беспрецедентная по охвату и мощи школьная система идеологической слежки, индоктринации и репрессий[4]. Пионерская и комсомольская организации, поощряемое государством доносительство, пристальный надзор за учебным процессом, единая образовательная программа и тотальная пропаганда были важными элементами этой системы. Исследователи нередко недооценивают силу советского социального инжиниринга, ссылаясь на то, что он не предотвратил крушение СССР. Но при этом упускается из виду, что советская школа «образовала» ключевые фигуры нынешнего российского режима, которые не только вспоминают о ней с ностальгией, но и стремятся к воспроизведению многих ее черт. Трагическая эффективность социального инжиниринга в СССР доказывается и тем, что после короткого периода демократизации и гуманизации российская школа, не сбросив тоталитарного наследия и несмотря на мужественное сопротивление отдельных директоров и учителей[5], в течение 2000-х годов все больше становилась оплотом правящей реакционной группы. В 2010-х и 2020-х годах школьная система стала частью государственного аппарата, выполняя разнообразные политические задачи, включая те, что прямо нарушают права человека: от фальсификации выборов и организованного участия в «путингах» до индоктринации обучающихся и дискриминации детей мигрантов[6]. Особенно ярко деградация школьной системы проявилась

---

[2] См., например: Ottinger Lily. “China's AI Education Experiment”. *ChinaTalk*, April 3, 2026, https://www.chinatalk.media/p/chinas-ai-education-experiment (дата обращения: 06.08.2026); Shi Chen and Jianhua Xu. “Surveillance Cameras and Resistance: A Case Study of a Middle School in China”. *The British Journal of Criminology*, Vol. 64, No. 5 (2024): 1150–1170.

[3] Примечательно, что в начале 2026 года китайские и российские власти объявили о начале Годов российско-китайского сотрудничества в области образования в рамках чего правительства двух стран планируют провести многочисленные мероприятия.

[4] Kelly Catriona. *Children's World: Growing Up in Russia, 1890-1991*. New Haven: Yale University Press, 2007.

[5] В отдельных случаях сопротивление учителей тоталитаризации и особенно милитаризации российской школы продолжилось и после начала российскими властями открытой войны против Украины в феврале 2022 года (см., например: ОВД-инфо. *«Либо государственное мнение, либо никакого»: как преследуют преподавателей, которым вменили антивоенную позицию.* ОВД-инфо от 1 сентября 2024 года. https://reports.ovd.info/teachers (дата обращения: 17.08.2026).

[6] См., например: Colin, Alexander. “Mr. Nobody Against Putin gives an insight into the propaganda in Russian schools”. The Conversation, July 3, 2025 https://theconversation.com/mr-nobody-against-putin-gives-an-insight-into-the-propaganda-in-russian-schools-260162 (дата обращения: 26.11.2025); Amnesty International Statement. *"Только официальные источники": Индоктринация в российской системе образования*. Amnesty International от 1 июня 2026 года; Троицкий Константин. *Тестирование детей-иностранных граждан на знание русского языка: нарушение права на образование, слежка и российская репрессивная миграционная политика*. Центр защиты прав человека «Мемориал», 2026. https://memorialcenter.org/ru/analytics/narushenie-prava-na-obrazovanie-dlya-detej-inostrannyh-grazhdan (дата обращения: 18.08.2026).

после начала российскими властями открытой и полномасштабной войны против Украины в феврале 2022 года[7].

С конца 2010-х годов российские власти активно испытывают на детях новые технологии и методы контроля. Среди них: аутентификация через биометрию, видеонаблюдение, отслеживание всех перемещений (геотрекинг), мониторинг сетевой активности, жесткий надзор за использованием мобильных устройств и, наконец, цифровое профилирование, включающее в себя не только сбор огромного массива данных, но и поведенческую аналитику, прогнозирование и предиктивный скоринг. Примечательно, что это те же самые технологии и методы, которые чиновники тестируют на мигрантах[8], хотя риторика, сопровождающая их внедрение, отличается в зависимости от того, на кого они направлены. Так, если в отношении иностранных граждан эти технологии применяются на фоне апелляции властей к борьбе с нелегальной миграцией, то в случае с детьми государство действует, прикрываясь мнимой заботой об их здоровье, а также защитой от терроризма, наркопреступности и педофилии. Однако, как будет видно ниже, анализ практики показывает, что декларируемые чиновниками мотивы резко расходятся с реальностью. И даже если принимаемые меры ведут к локальному снижению рисков, что совсем не очевидно, то это проявляется в виде побочного эффекта процесса тоталитаризации, направленного на установление абсолютного госконтроля над школой в частности и российским обществом в целом. Подобная модель безопасности через изоляцию и цифровой гипернадзор сближает школу с современными колониями строгого режима: в них риски нарушений тоже стремятся к нулю, но это не делает их средой, пригодной для детей.

К середине 2020-х годов большинство российских школ превратилось в зоны жесткого надзора. Этот процесс не вызвал подлинного сопротивления в зачищенном политическом пространстве, а скоординированную вербальную оппозицию в Российской Федерации ему выражали лишь представители некоторых фундаменталистских течений в политической элите. Но надо учитывать, что эта «оппозиция»: во-первых, никогда не была принципиальной и не критикует верхушку российской власти; во-вторых, используется для имитации протеста; в-третьих, выступает открытым адвокатом милитаризма и тоталитаризма; в-четвертых, является органической частью текущего режима; в-пятых, на практике совмещает архаическую риторику с продвижением цифровой пропаганды (например, фабрик-троллей), кибернадзора (например, Лига безопасного интернета) и технологий интернет-контроля (например, фильтрация трафика, черные списки и деанонимизация пользователей). Деятельность этих номенклатурных традиционалистов, группирующихся, когда речь идет об образовании, вокруг таких фигур, как Сергей Кургинян, Никита Михалков и Екатерина Мизулина, таких бутафорских и парагосударственных организаций, как

---

[7] См., например: Медуза. «“Мы просто физически не успеваем вести свои обычные уроки”. Как изменилось школьное образование в России за годы войны?» *Медуза,* 8 сентября 2025 года, https://meduza.io/feature/2025/09/08/my-prosto-fizicheski-ne-uspevaem-vesti-svoi-obychnye-uroki (дата обращения: 18.08.2026); Alava Jonna. “From Patriotic Education to Militarist Indoctrination—Disciplinary Power and Silent Resistance in Russia after the Onset of the War against Ukraine”. *Problems of Post-Communism* 72, no. 5 (2025): 429–440; Мальгина Анна. «“Господин Никто против Путина”: как школьный педагог из Карабаша снял фильм, потрясший Запад. Интервью “Вот Так” с Павлом Таланкиным». *vot-tak.tv* от 3 июня 2025 года. https://vot-tak.tv/87052526/interviu-s-pavlom-talankinym (дата обращения: 20.08.2026); Аркман Арден. *Методичь. Как государственная пропаганда захватила российское образование — от детских садов до вузов*. Издание The Insider от 10 октября 2025 года. https://theins.ru/obshestvo/284870 (дата обращения: 20.08.2026); Amnesty International Statement. *"Только официальные источники": Индоктринация в российской системе образования*. Amnesty International от 1 июня 2026 года.

[8] Троицкий Константин. *Государственный информационный ресурс «Цифровой профиль иностранного гражданина» и формирование нового российского тоталитаризма.* Центр защиты прав человека «Мемориал», 2026. https://memorialcenter.org/uploads/Kopiya_Konstantin_Troiczkij_O_czifrovom_profile_inostrannogo_grazhdanin3_6_9157de992b.pdf (дата обращения: 03.08.2026).

«Общественный уполномоченный по защите семьи» (ОУЗС) и «Родительское Всероссийское Сопротивление», таких милитаристско-шовинистических медиа, как «Октагон», «Красная весна» и РИА «Катюша», — это внутриэлитное соперничество между «реакционерами» и «технократами» за ресурсы и влияние, в котором одни уделяют больше внимания идеологической и содержательной составляющей, а другие — технической и формальной. Иными словами, эта псевдооппозиция борется не за отмену курса на тотальный цифровой госконтроль, а за то, чтобы его безраздельно возглавили и продвигали наиболее репрессивные органы российской власти, то есть ФСБ, МВД, Следственный комитет и прокуратура. В то же время, несмотря на конкуренцию, структурно условные «реакционеры» и «технократы» — это две стороны единой гибридной системы, где одна предлагает суррогат ответа на вопрос «что», а другая — на вопрос «как». В отношении госконтроля над школьниками их роли распределяются так, что «реакционеры» превалируют в содержательных вопросах унификации и индоктринации, а также при определении критериев наказаний и целевых маркеров слежки, тогда как условные «технократы» разрабатывают и внедряют цифровую инфраструктуру для реализации всего этого.

Анализ структуры государственного контроля над ребенком в современной российской школе позволяет выделить несколько базовых элементов. Важнейшие из них:

- Унификация — стандартизация и дисциплинизация поведения.
- Индоктринация — директивное внедрение в психику детей официальных идеологических нарративов с запретом их критики.
- Комплекс поощрений и наказаний — система, направленная на стимулирование тех, кто следует унификации и усваивает идеологию и подавление тех, кто им противится.
- Слежка — инструмент, который позволяет оценивать, модифицировать и планировать применение трех других элементов контроля, выступая тем самым их основой.

Надо особенно подчеркнуть, что на основе данных, полученных в ходе слежки, формируются новейшие системы предиктивной аналитики, включающие социальный скоринг детей. Предиктивная аналитика тем самым становится пятым важнейшим элементом контроля, направляющая остальные элементы на будущее. Учитывая фундаментальное значение слежки и возрастающую роль в ней передовых технологий, именно процесс ее цифровизации и находится в центре внимания этого исследования.

О школьной слежке с использованием новых технологий писали разные издания, НКО и эксперты. Однако в фокус их внимания попадали лишь отдельные элементы и практики, в то время как феномен слежки в его целостности и взаимосвязи оставался вне рамок критического анализа. Исследователи упустили из виду ряд важных факторов, среди которых: старт разработки системы тотального мониторинга еще в конце 2010-х годов, ключевая роль цифрового профилирования детей, а также тот факт, что это профилирование стало возможным лишь в силу глубокой интеграции государственных информационных систем и подключению всех российских школ к Федеральной государственной информационной системе «Моя школа». Учитывая все это, неудивительно, что до сих пор неописанной оставалась крайне опасная тенденция последних лет — все более тесное объединение разных направлений школьной слежки в рамках единой и тотальной метасистемы контроля.

Важно подчеркнуть, что дело не в сборе данных школами как таковом. Это делают все образовательные организации мира, и этот факт использует российская пропаганда, чтобы отвлечь внимание от тоталитаризации и преуменьшить масштаб вторжения государства в в личную жизнь детей и их семей. Главные вопросы заключаются в том, (1) какие именно данные и (2) каким образом собираются, (3) кто управляет этим процессом и (4) для чего они

используются. Крайне серьезные проблемы, связанные с российским подходом к обращению с данными детей, заключаются в том, что:

1. О детях собираются избыточные данные (от предпочтений в столовой и личных сообщений до любимой музыки и лайков под оппозиционными видео).
2. При сборе данных грубо нарушаются права на конфиденциальность, свободу выражения мнения, поиск и получение информации, на защиту от дискриминации, а также право на информированное согласие детей и их родителей.
3. Определяющая роль в администрировании, агрегации и конечном использовании данных в последние годы перешла от школ и региональных органов образования к федеральным ведомствам: силовому блоку (МВД, ФСБ и прокуратура), структурам цензуры (Минцифры и Роскомнадзор) и аппарату пропаганды (Росмолодежь, Минпросвещения и управляемое ими «Движение Первых»).
4. Данные используются для профилирования детей с конечной целью установления тотального госконтроля над ними через развитие и внедрение систем слежки, индоктринации, унификации и комплекса поощрений и наказаний. Дополнительно данные детей задействованы для обучения моделей ИИ, чтобы сделать работу этих систем еще более эффективной.

Это исследование носит обзорный характер и не ставит своей целью раскрытие всех видов, методов и аспектов слежки в российских школах. Акцент сделан на описании четырех периметров слежки с использованием современных цифровых технологий. Хотя в этом докладе рассматривается слежка вне зависимости от категорий детей, надо иметь в виду, что власти по-разному фокусируются на разных группах. Так, например, они обращают усиленное внимание на детей-иностранных граждан в целом[9], а среди последних особо концентрируются на насильно русифицированных несовершеннолетних[10], которые были либо вывезены из Украины[11], либо остаются на украинских территориях, оккупированных российскими властями[12].

Задействование цифровых технологий качественно изменило слежку, что делает полезным концептуальное отделение личной или «традиционной слежки» (traditional surveillance), опирающейся на прямой визуальный или слуховой контакт и примитивные средства учета, от «новой слежки» (new surveillance), основывающейся на передовых технологиях[13]. Это, разумеется, не значит, что в российских школах «традиционная слежка» через личный надзор учителей и администрации исчезла. Напротив, старые методы интегрировались в цифровую среду, а сотрудники учебных заведений превратились в низовых операторов и поставщиков данных для этой высокотехнологичной системы. Так, учителя и школьная администрация вынуждают родителей создавать цифровые профили обучающихся, оценивают и заносят в

[9] Троицкий Константин. *Тестирование детей-иностранных граждан на знание русского языка: нарушение права на образование, слежка и российская репрессивная миграционная политика*. Центр защиты прав человека «Мемориал», 2026. https://memorialcenter.org/ru/analytics/narushenie-prava-na-obrazovanie-dlya-detej-inostrannyh-grazhdan (дата обращения: 18.08.2026).

[10] Yale School of Public Health. *Forced Passportization on Russia-Occupied Areas of Ukraine*. New Haven, Humanitarian Research Lab at Yale School of Public Health, August 2, 2023. https://files-profile.medicine.yale.edu/documents/891469c2-690f-4229-8ffc-35b1c3743744 (дата обращения: 24.08.2026).

[11] Медуза. «“Они могут начать противодействовать”. Российские власти боятся детей, насильно вывезенных из Украины. Их пытаются «перевоспитать» и поставить под жесткий цифровой контроль». *Медуза* от 11 марта 2024 года https://meduza.io/feature/2024/03/11/oni-mogut-nachat-protivodeystvovat (дата обращения: 20.08.2026).

[12] HRW. *Education under Occupation. Forced Russification of the School System in Occupied Ukrainian Territories*. Human Rights Watch, June 2024. https://www.hrw.org/sites/default/files/media_2024/06/ukraine_crd0624%20web_0.pdf (дата обращения: 24.08.2026).

[13] См., например: Marx Gary. *Windows into the Soul. Surveillance and Society in an Age of High Technology*. The University of Chicago Press, 2016. P. 15–18.

систему данные об успеваемости, поведении и внеучебной деятельности детей, а также согласовывают установку и участвуют в обслуживании систем видеонаблюдения. Кроме того, именно учителя и школьная администрация учат детей пользоваться школьными компьютерами и интернетом, ведут переписку в «Сферуме», организуют интерактивные уроки и даже порой занимаются мониторингом социальных сетей учеников.

Описание периметров и действующих систем слежки базировалось на анализе следующих источников:

- ➔ российских нормативных актов;
- ➔ презентаций, планов и заявлений официальных лиц и разработчиков;
- ➔ мнений экспертов и тематических сайтов;
- ➔ пользовательских инструкций;
- ➔ новостных изданий;
- ➔ журналистских расследований.

В докладе не описываются технические нюансы систем школьной слежки — это тема для более детальных и масштабных исследований. Здесь также не рассматриваются многие учебные ресурсы, чтобы не перегружать текст. Не игнорируя технический компонент и важность дополнительных изысканий, автор пытается обрисовать в общих чертах функциональные, политические и нормативные компоненты школьной инфраструктуры слежки с акцентом на ее все возрастающую сложность, тотальность и репрессивность.

Ниже представлен анализ системы государственной слежки за детьми в российских школах, направленной на установление тотального цифрового контроля. При этом цифровизация — это сложный технологический процесс, который наряду с удручающими примерами его задействования во зло и вдохновляющими случаями его применения во благо, требует осмысления сам по себе — в контексте прав человека, этики и сквозь призму христианской традиции понимания человеческого достоинства[14]. Доклад основывается на убеждении, что при описании конкретной системы нельзя забывать о более широких вопросах, которые ставят перед человечеством новые технологии.

[14] Leo XIV, Pope. 2026. *Magnifica humanitas: On Safeguarding the Human Person in the Time of Artificial Intelligence* (Encyclical Letter). May 15, 2026. The Holy See. https://www.vatican.va/content/leo-xiv/en/encyclicals/documents/20260515-magnifica-humanitas.html (дата обраения: 28.09.2026).

Основы цифровой слежки в школах

Выход слежки в российских школах на качественно новый уровень имеет множество причин, но ключевыми стали четыре фактора: 1) задействование новейших цифровых технологий, включая нейросети; 2) создание метасистемы государственного управления; 3) введение всеобщего профилирования; 4) техническое переоснащение образовательных организаций. Все эти факторы были реализованы российскими властями в короткий промежуток времени — в период с 2019 по 2024 год.

1. Использование новейших цифровых технологий

В XXI веке развитие цифровых технологий не только ускорилось, но и в значительной степени вытеснило аналоговые форматы. Это дало толчок датафикации — попытке перевести в код все, вплоть до человеческого ума, характера и поведения. Высокоскоростные сети, рост вычислительных мощностей и развитие искусственного интеллекта, особенно нейросетей, расширили возможности слежки. Так, эти технологии позволили построить принципиально новые платформы по сбору, хранению и обработке данных, которые, в свою очередь, стали основой систем распознавания лиц, автоматического мониторинга интернета и предиктивной аналитики.

2. Создание метасистемы государственного управления

Текущая слежка в российских школах стала результатом развертывания властями цифровой архитектуры государственного управления, включая централизацию и интеграцию многочисленных государственных систем. Этот процесс начался давно, но решающий импульс был задан в рамках проекта по созданию «Национальной системы управления данными» (далее — НСУД). Об идее построения этой метасистемы стало широко известно в 2018 году, когда появились первые официальные версии ее концепции[15]. Тогда же чиновники заявили, что базовые компоненты НСУД начнут работать в 2021 году, а к 2024 году в ее рамках должно произойти объединение основных государственных информационных систем[16]. При этом, хотя власти в своих публичных презентациях и комментариях пытались представить планируемую метасистему как инструмент, который сделает более удобным взаимодействие населения с государственными и коммерческими структурами[17], они особо не скрывали, что на самом деле в этом мегапроекте «*основные акценты сделаны на интересах государства и оптимизации межведомственного взаимодействия*»[18].

Итак, НСУД задает единые правила управления данными, стандарты качества информации и формирует цифровую федеративную архитектуру, которая обеспечивает централизацию

---

[15] Аналитический центр при Правительстве РФ. «Национальная система управления данными. Концепция». Проект от 25.11.2018 года, версия 5.14. https://digital.msu.ru/wp-content/uploads/%D0%9D%D0%A1%D0%A3%D0%94.-%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D0%B8%D1%8F_%D0%B28_25112018.pdf (Доступ: 20.04.2026).

[16] Краснушкина Надежда. «Госданным прописали архитектуру». *Издание* «*Коммерсантъ*» от 30 ноября 2018 года; Касми Эльяс. «Власти собираются объединить все данные граждан и бизнеса в огромное электронное досье». *Издание «CNews»* от 30 ноября 2018 года.

[17] См. страницы 21–24 здесь: Аналитический центр при Правительстве РФ. «Национальная система управления данными. Концепция». Проект от 25.11.2018 года, версия 5.14. https://digital.msu.ru/wp-content/uploads/%D0%9D%D0%A1%D0%A3%D0%94.-%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D0%B8%D1%8F_%D0%B28_25112018.pdf (Доступ: 20.04.2026).

[18] Бахур Владимир. «Эксперты: национальная система управления данными должна фокусироваться на пользе для бизнеса и граждан». *Издание «CNews»* от 29 ноября 2018 года.

сотен государственных систем[19]. Эта архитектура построена на ведомственных «витринах данных» — специализированных сегментах ИТ-инфраструктуры, позволяющих связывать, унифицировать и распределять информацию по запросу. Такой подход позволяет интегрировать разные системы с помощью перекрестных ссылок и обеспечивать управление данными практически в реальном времени, без создания единого физического хранилища. В НСУД реализована концепция «эталонных данных», закрепляющая за профильными ведомствами статус первоисточников информации о гражданах РФ, иностранных гражданах и организациях. Сравнение сведений из различных систем происходит автоматически на основе алгоритмов верификации. Если данные из разных источников расходятся, приоритет отдается ресурсу-эталону. Это позволяет проводить оперативную гармонизацию данных и создавать уникальные цифровые профили, объединяющие гигантские массивы информации[20].

3. Введение цифрового профилирования

Изначально одним из главных подпроектов в рамках развития НСУД было введение всеобщего государственного цифрового профилирования. В интернете распространено ошибочное представление, согласно которому система профилирования — это всего лишь большая база данных, а цифровой профиль — электронное досье на человека[21]. На самом деле цифровой профиль представляет собой уникальную кибернетическую модель человека, а система профилирования — динамическую цифровую инфраструктуру, в рамках которой непрерывно осуществляются сбор, обновление, корреляция и анализ данных. Система профилирования формирует прогностические модели, обеспечивает автоматическое реагирование, а в продвинутых версиях на ее базе ведется полномасштабное алгоритмическое управление людьми[22].

Всеобщее государственное цифровое профилирование с самого начала было приоритетом для российских властей, поскольку давало им в руки новые и невиданные по силе инструменты контроля. Учитывая это, неудивительно, что, когда в 2019 году Правительство РФ объявило о проведении «эксперимента» в рамках построения НСУД, первой же его задачей была обозначена «разработка инфраструктуры цифрового профиля»[23]. Примечательно, что если в изначальной редакции постановления об «эксперименте» выделялось семь «функциональных возможностей», которые должна была включать система профилирования, то в результате многочисленных правок в действующей на середину 2026 года редакции этот список вырос более чем в три раза[24].

---

[19] В 2021 году Коммерсантъ писал о более 800 государственных информационных системах (ГИС), планируемых быть интегрированными в рамках ЕИП НСУД (Галиева Диана. «Госданные приглашают на платформу». *Издание «Коммерсантъ»* от 4 мая 2021 года).

[20] Там же.

[21] См., например: Медуза. «Все иностранцы в России очень скоро окажутся под плотным контролем властей — на каждого человека составят максимально подробное досье». *Издание «Медуза»* от 28 января 2026 года https://meduza.io/cards/vse-inostrantsy-v-rossii-ochen-skoro-okazhutsya-pod-plotnym-kontrolem-vlastey-na-kazhdogo-cheloveka-sostavyat-maksimalno-podrobnoe-dosie (Доступ: 04.09.2026).

[22] Краткую историю профилирования и размышления над его сущностью см., например, здесь: Bernard Andreas. *Komplizen des Erkennungsdienstes. Das Selbst in der digitalen Kultur*. Frankfurt am Main: S. Fischer Verlag GmbH, 2017; Goldenfein Jake. *Monitoring Laws. Profiling and Identity in the World State*. Cambridge, Cambridge University Press, 2020.

[23] Постановление Правительства РФ от 03.06.2019 N 710 «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» (первоначальная редакция) https://ivo.garant.ru/#/document/77695224/paragraph/33:2 (Доступ: 17.09.2026).

[24] Постановление Правительства РФ от 03.06.2019 N 710 «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» (редакция от 17.11.2025) https://ivo.garant.ru/#/document/72262102/paragraph/9093:5 (Доступ: 17.09.2026).

Сначала речь шла лишь об общей инфраструктуре цифрового профиля, но уже в начале 2020-х годов в ней были выделены подпроекты для граждан РФ, иностранцев и юридических лиц. Быстрее всего развивалось и внедрялось профилирование иностранных граждан, на которых российские власти тестировали новые технологии контроля[25]. Но это не значит, что профилирование россиян стояло на месте.

Дети не освобождаются от этой процедуры. Уже несколько лет цифровой профиль автоматически создается при рождении ребенка через безальтернативное присвоение ему СНИЛС[26], который власти стали использовать в качестве единого уникального идентификатора человека на своих платформах, то есть как основу профиля[27]. Кроме того, запись в школы ведется через Федеральную государственную информационную систему «Единый портал государственных и муниципальных услуг (функций)» (далее — Портал «Госуслуги»), а регистрация на ней подразумевает активацию цифрового профиля или его создание, поскольку требует обязательного указания СНИЛС. Но это еще не все. При поступлении в школу происходит не только первая линейка и знакомство со сверстниками, но и еще одно примечательное событие. Дело в том, что российские власти продолжили дифференциацию цифровых профилей, и при зачислении ребенка на основе общего профиля формируется «профиль обучающегося», который, как будет видно далее, играет ключевую роль в школьной слежке. При этом нельзя забывать, что слежкой дело не ограничивается, поскольку профилирование направлено на полный контроль несовершеннолетних, включающее также упомянутые выше унификацию, индоктринацию, комплекс поощрений и наказаний, а также предиктивную аналитику. Цифровое профилирование обучающегося ведется в рамках Федеральной государственной информационной системы «Моя школа» (далее — ФГИС «Моя школа»), которая и составляет первый периметр слежки.

4. Техническая модернизация школ

Внедрение профилирования в школах и создание условий для использования новейших технологий слежки требовали инфраструктурного переоборудования российских учебных заведений, а именно их цифровизации. В конце 2010-х годов власти запустили несколько масштабных проектов для достижения этой цели, главный из которых носил название «Цифровая образовательная среда» (далее — ЦОС). Этот проект, который курировали

---

[25] Подробнее о цифровом профилировании см.: Троицкий Константин. *Государственный информационный ресурс «Цифровой профиль иностранного гражданина» и формирование нового российского тоталитаризма*. Центр защиты прав человека «Мемориал», 2026. https://memorialcenter.org/uploads/Kopiya_Konstantin_Troiczkij_O_czifrovom_profile_inostrannogo_grazhdanin3_6_9157de992b.pdf (дата обращения: 03.08.2026).

[26] См. пункты 5 и 15 раздела II Инструкции о порядке ведения индивидуального (персонифицированного) учета сведений о зарегистрированных лицах здесь: Приказ Минтруда России от 03.04.2023 N 256н «Об утверждении Инструкции о порядке ведения индивидуального (персонифицированного) учета сведений о зарегистрированных лицах» https://www.consultant.ru/document/cons_doc_LAW_447676/ (дата обращения: 21.08.2026).

[27] Власти официально изменили суть СНИЛС в 2019 году, готовя почву для введения всеобщего цифрового профилирования, которое началось в том же году. Среди прочего суть изменений заключалось в том, что лицевой счет стал открываться и СНИЛС а) присваиваться всем российским гражданам, а не только застрахованным, б) в ряде случаев автоматически (наприер, при рождении ребенка), в) использоваться в качестве уникального идентификатора российского гражданина в государственных системах. Последнее было введено через дополнение целей учета (раньше было страхования) следующей: «*использование страхового номера индивидуального лицевого счета для идентификации и аутентификации сведений о физическом лице при предоставлении государственных и муниципальных услуг и исполнении государственных и муниципальных функций*» (см. Федеральный закон от 01.04.2019 N 48-ФЗ «О внесении изменений в Федеральный закон “Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования” и отдельные законодательные акты Российской Федерации» https://www.consultant.ru/document/cons_doc_LAW_321413/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100031 (дата обращения: 22.08.2026).

Минпросвещения и Минцифры, входил в национальный проект «Образование» и начался в том же 2019 году, что и инициативы по НСУД и цифровому профилированию. Его бюджет превышал 80 млрд рублей только федеральных расходов.

Подавляющее большинство средств в рамках ЦОС было потрачено на цифровое оборудование (компьютеры, серверы, интерактивные доски, проекторы, видеокамеры и сетевую инфраструктуру), что обеспечило школам материальный фундамент для современных систем слежки[28]. Именно по итогам проекта ЦОС, закончившегося в 2024 году, были развернуты ФГИС «Моя школа», системы видеонаблюдения и централизованные сети режимного доступа к интернету[29]. Разумеется, окончание ЦОС не означало прекращения модернизации инфраструктуры или того, что цифровизация школ и раньше осуществлялась исключительно в рамках этого проекта.

[28] Распоряжение Минпросвещения России от 17.12.2019 N Р-135 «Об утверждении методических рекомендаций по приобретению средств обучения и воспитания для обновления материально-технической базы общеобразовательных организаций и профессиональных образовательных организаций в целях внедрения целевой модели цифровой образовательной среды в рамках региональных проектов, обеспечивающих достижение целей, показателей и результата федерального проекта “Цифровая образовательная среда” национального проекта “Образование”» https://www.consultant.ru/document/cons_doc_LAW_340889/ (дата обращения: 21.08.2026).

[29] Приказ Минпросвещения России от 02.12.2019 N 649 «Об утверждении Целевой модели цифровой образовательной среды» https://www.consultant.ru/document/cons_doc_LAW_341443/ad8f4e028380894173b4f017a56c42b4c5e4ad54/#dst100011 (дата обращения: 13.08.2026).

Первый периметр

ФГИС «Моя школа»

ФГИС «Моя школа» выполняет множество функций, но в контексте слежки следует выделить три ключевые: накопление данных и создание профилей обучающихся, организация онлайн-коммуникаций и интеграция в единую государственную цифровую архитектуру.

Данные об ученике и профилирование обучающихся

До появления ФГИС «Моя школа» сведения, собираемые о детях, оставались разрозненными, ограниченными и разнородными. Они не собирались в одном месте, будь то цифровое хранилище или бумажное дело ребенка, а в каждой школе и регионе существовали свои локальные методики фиксации и обработки информации. Из-за фрагментированности и отсутствия стандартизации этих данных ни администрация учебных заведений, ни тем более федеральные ведомства не имели детального описания несовершеннолетнего.

Децентрализацию первыми начали устранять отдельные регионы, среди которых первопроходцем выступила администрация Москвы. Сразу после прихода к власти в 2010 году Сергей Собянин потребовал, чтобы ему «*дали город онлайн*», и инициировал разнообразные проекты по установке полного цифрового контроля за москвичами и мигрантами[30]. Слежка за детьми была развернута в рамках платформы «Московская электронная школа» (МЭШ), которая во многом легла в основу системы ФГИС «Моя школа», призванной перенести московский опыт на все российские школы[31]. Новая федеральная система была задумана чиновниками как единый центр сбора, унификации и сквозной обработки данных обо всей деятельности учащихся. Без создания этого фундамента построение пристального цифрового надзора за школьниками было бы технически невозможно.

ФГИС «Моя школа» собирает широкий спектр данных, которые еще недавно терялись в папках и отчетах либо просто не фиксировались. Речь идет не только о базовых анкетных сведениях, успеваемости (оценках, экзаменах и зачетах) и посещаемости. Система фиксирует и навсегда интегрирует с цифровыми профилями такую информацию[32], как точное время входов и выходов из школы, причины отсутствия, показатели прохождения интерактивных опросов и заданий, выполнение домашних работ онлайн, занятия с учебными тренажерами, результаты диагностик функциональной грамотности и профориентационных тестов, сведения о родителях или опекунах, а также блок, посвященный внеучебной деятельности, включая участие в олимпиадах, кружках, секциях, конкурсах, экскурсиях и летних лагерях[33].

---

[30] Захаров Андрей. «“Умный город” или “Старший брат”? Как мэрия научилась знать о москвичах всё». *BBC News Русская служба* от 10 апреля 2020 года. https://www.bbc.com/russian/features-52219260 (дата обращения: 17.09.2026).

[31] D-Russia. «Подписано соглашение об использовании решений «Московской электронной школы» при развитии ФГИС “Моя школа”». *Издание «D-Russia»* от 2 сентября 2022 года.

[32] Перечень групп данных, собираемых и обрабатываемых в единой школьной системе, был намечен властями еще в 2019 году, см. Подпункт «а» пункта 4.3 приложения к Приказу Минпросвещения России от 02.12.2019 N 649 «Об утверждении Целевой модели цифровой образовательной среды» https://www.consultant.ru/document/cons_doc_LAW_341443/ad8f4e028380894173b4f017a56c42b4c5e4ad54/#dst100011 (дата обращения: 13.08.2026).

[33] С перечнем модулей, функций и систем ФГИС «Моя школа» на середину 2026 года можно ознакомится здесь: Министерство просвещения РФ / Министерство цифрового развития, связи и массовых коммуникаций РФ. (2026). Функциональные возможности ТОР. Школа // Краткое описание ФГИС «Моя школа» ТОР. Образование

Туда же заносятся данные о лицевом счете ребенка, о питании, льготах и тратах. С профилями связываются также листки здоровья детей, содержащие такие чувствительные данные, как хронические заболевания, аллергии, медицинские назначения и противопоказания[34]. Более того, система интегрирует с профилями социальный паспорт обучающегося, который отражает сведения о благосостоянии семьи, ее структуру, жилищные условия, заключения психологической диагностики, наличие у ребенка особого статуса (например, сирота, под опекой, с ограниченными возможностями здоровья), находится ли несовершеннолетний на профилактическом учете, а также, что будет рассмотрено подробнее в разделе «Периметр 4», результаты мониторинга онлайн-активности школьника.

Но даже этими сведения данные, связываемые с профилями обучающихся, не ограничиваются. В конце 2025 года власти запустили и начали активно продвигать сервис «Цифровой психолог», полностью интегрированный во ФГИС «Моя школа». Его суть заключается в возможности дистанционной записи и проведения онлайн-консультаций детей по широкому спектру вопросов и проблем. В то же время техническое устройство сервиса не только исключает реальную приватность, но и заставляет подозревать, что за бесплатными консультациями скрывается стремление властей собирать и анализировать данные о самых интимных переживаниях несовершеннолетних. Более того, сохранение подлинной конфиденциальности противоречило бы самой сути ФГИС «Моя школа» и всей государственной ИТ-архитектуре, куда она интегрирована и которая нацелена на унификацию, соединение и анализ любой поступающей информации о подрастающем поколении.

Так, для использования сервиса «Цифровой психолог» необходима идентификация через Единую систему идентификации и аутентификации Портала «Госуслуги» (далее — ЕСИА), что исключает анонимность и связывает факт обращения с цифровым профилем ребенка. Таким образом, даже без прямого анализа текста бесед система неизбежно фиксирует и агрегирует метаданные: частоту обращений, их длительность, темы и информацию о специалисте. В условиях единой платформы эти сведения немедленно становятся частью сквозной аналитики. Более того, инфраструктура сервиса «Цифровой психолог» в принципе позволяет властям в любой момент — если этот процесс еще не запущен — развернуть алгоритмический анализ содержания самих бесед.

Следует напомнить, что ФГИС «Моя школа» играет важную роль в унификации, индоктринации и комплексе наказаний и поощрений школьников, что пока не было описано в серьезных исследованиях. Здесь можно привести лишь один пример, который демонстрирует тесную связь всех элементов контроля. Так, цифровая библиотека этой платформы содержит единые идеологические материалы (книги, видео- и аудиозаписи), на базе которых учителя формируют шаблонные групповые и индивидуальные занятия для детей. Их использование опирается на цифровую слежку, поскольку система фиксирует, когда и на какое время ребенок открывал предложенный материал, а также (если контент предполагал практические задания) результаты их выполнения[35]. По итогам заданий учитель проводит оценивание, которое, с одной стороны, поощряет или наказывает обучающихся, а с другой, остается связанным с профилями детей и может служить для дальнейшей аналитики и подбора индивидуальных программ.

для субъектов РФ. Размещено на официальном сервере Правительства Смоленской области. https://obrpoch.admin-smolensk.ru/files/561/tor_kratko_av.pdf (дата обращения: 12.09.2026).

[34] Там же.

[35] Инструкция по работе с Универсальной библиотекой цифрового образовательного контента (УБ ЦОК). *Портал myschool.eduprosvet.ru* (дата обращения: 14.08.2026).

Школьные коммуникации: «Сферум» и «Макс»

Согласно Постановлению Правительства РФ № 1241, одной из задач ФГИС «Моя школа» является «*обеспечение эффективного взаимодействия и онлайн-коммуникаций пользователей*», что подразумевает широкий спектр сервисов, включающих чаты, видеозвонки, педагогические каналы и онлайн-уроки[36]. Этот функционал был развернут на базе Информационно-коммуникационной образовательной платформы «Сферум» (далее — «Сферум»), которая стала совместным проектом компаний VK и «Ростелеком» и с самого начала внедрялась в школы с применением административного ресурса[37]. В 2023 году «Сферум» официально был интегрирован с ФГИС «Моя школа»[38], а в 2025 году стал частью единого государственного мессенджера «Макс», образовав с ним единый общероссийский контур слежки[39].

Тут следует напомнить, что конгломерат VK, которому принадлежит мессенджер «Макс», вырос из социальной сети «ВКонтакте», с первых лет своего существования известной тесным сотрудничеством с российскими силовыми органами[40]. Это взаимодействие началось задолго до того, как компания в начале 2020-х годов перешла под полный и прямой контроль госструктур, а ее генеральным директором стал Владимир Кириенко — сын первого заместителя руководителя Администрации Президента РФ[41]. Развитие «Макса» велось в тесном взаимодействии со спецслужбами, что, помимо прочего, нашло отражение в его полной интеграции с системой СОРМ, сертификации криптографии со стороны ФСБ, а также во внедрении отслеживающих алгоритмов на базе рекомендаций этой службы госбезопасности[42]. Независимые эксперты не перестают находить в этом мессенджере все новые уязвимости и скрытый функционал[43]. В сентябре 2026 года лаборатория цифровой

[36] См. подпункт «д» пункта 5 Положения о Федеральной информационной системе «Моя школа» Постановления Правительства РФ от 13.07.2022 N 1241 «О федеральной государственной информационной системе “Моя школа”» https://www.consultant.ru/document/cons_doc_LAW_422207/ (дата обращения: 06.08.2026).
[37] Литой Александр. «Государство пришло в чат. Контроль над учителями, родителями и детьми». *Радио “Свобода”* от 30 ноября 2023 года. https://www.svoboda.org/a/gosudarstvo-prishlo-v-chat-kontrolj-nad-uchitelyami-roditelyami-i-detjmi/32426381.html (дата обращения: 17.08.2026).
[38] Пункт 3(1) Постановления Правительства РФ от 13.07.2022 N 1241 «О федеральной государственной информационной системе “Моя школа”» https://www.consultant.ru/document/cons_doc_LAW_422207/ (дата обращения: 06.08.2026).
[39] D-Russia. «Сервис для школ “Сферум” стал доступен из Max». *Издание «D-Russia»* от 9 октября 2025 года.
[40] Poupin Perrine. “Social media and state repression: The case of VKontakte and the anti-garbage protest in Shies, in Far Northern Russia?. *First Monday*, 26 (5) (2021). https://firstmonday.org/ojs/index.php/fm/article/view/11711/11233 (дата обращения: 18.08.2026); Dietrich Philipp. 2023. *The Key Player in Russia’s Cybersphere. What the West Needs to Know about VK Company*. German Council on Foreign Relations, September 20, 2023. https://dgap.org/en/research/publications/key-player-russias-cybersphere (дата обращения: 18.08.2026).
[41] Медуза. «VK перешел под контроль Газпромбанка и “Согаза” друга Путина Юрия Ковальчука. Гендиректором VK станет сын Сергея Кириенко». *Медуза* от 3 декабря 2021 года. https://meduza.io/feature/2021/12/03/vk-pereshel-pod-kontrol-gazprombanka-i-sogaza-druga-putina-yuriya-kovalchuka-gendirektorom-vk-stanet-syn-sergeya-kirienko (дата обращения: 19.08.2026).
[42] Александров Алексей. «В России начали широко рекламировать мессенджер Max. В чем его опасность и способен ли он стать аналогом китайского WeChat?». *Настоящее время* от 14 июля 2025 года. https://www.currenttime.tv/a/v-rossii-nachali-shiroko-reklamirovat-messendzher-max-v-chem-ego-opasnost-i-sposoben-li-on-stat-analogom-kitayskogo-wechat-/33472932.html (дата обращения: 23.08.2026); Enders Anna, Lea Horne, and Marla Rivera. *The Max Messenger: An Analysis of Russia’s State-Mandated Messaging Application*. InterSecLab, September 2026.
[43] См., например: Беларуская асацыяцыя журналістаў. «7 способов, которыми российский мессенджер Max следит за пользователями». *Беларуская асацыяцыя журналістаў* от 7 октября 2025 года, https://baj.media/be/karysnae/max-sledit-za-polzovateljami/ (дата обращения: 24.04.2026); Медуза. «Вы наверняка слышали, что “Макс” шпионит за пользователями. Но вряд ли представляете, сколько разных инструментов для слежки внедрено в мессенджер Возможно, разработчики даже использовали нейросеть для прослушки». *Медуза* от 22 мая 2026 года. https://meduza.io/feature/2026/05/22/vy-uzhe-navernyaka-slyshali-chto-maks-shpionit-za-svoimi-polzovatelyami-no-vr

безопасности InterSecLab опубликовала масштабный технический анализ мессенджера «Макс», наглядно демонстрирующий, как именно это приложение служит инструментом изощренной государственной слежки[44]. Таким образом, власти встроили «Сферум» в очень удобную для них инфраструктуру слежки, в рамках которой все коммуникации детей и взрослых тщательно модерируются, анализируются и становятся полностью прозрачными для сотрудников силовых ведомств и алгоритмов.

Интеграция в единую государственную цифровую архитектуру

Создание ФГИС «Моя школа» как отдельной информационной системы было бы недостаточным для общегосударственной слежки за школьниками. Даже после стандартизации и сбора сведений на единой учебной платформе эти данные оставались бы изолированными от баз других ведомств и находились вне досягаемости мощных алгоритмических моделей. Во многих демократических странах образовательные платформы намеренно обособлены от других систем именно в целях защиты частной жизни от таких злоупотреблений, как моделирование цифровых двойников и организация массового надзора за несовершеннолетними. Однако российские власти изначально планировали ФГИС «Моя школа» как органическую часть общегосударственной информационной архитектуры тотального контроля.

Хотя активация ФГИС «Моя школа» и ее нормативное закрепление произошли в начале 2020-х годов[45], разработка системы стартовала еще в конце 2010-х годов[46]. Это протекало параллельно с развертыванием НСУД, которой, как упоминалось выше, была отведена роль нормативного, методологического и технологического фундамента для объединения сотен систем в единый контур цифрового госуправления. Сначала ФГИС «Моя школа» создавалась на базе систем Минпросвещения. Однако Постановлением № 1241 Правительство передало их под управление Министерства цифрового развития, связи и массовых коммуникаций (далее — Минцифры)[47]. При этом Минцифры уже тогда выступало оператором Единой информационной платформы НСУД, то есть фактически отвечало за технологическую часть проекта[48]. Кроме того, Минцифры — ключевой элемент в системе российской государственной слежки. Деятельность этого министерства и его сателлита Роскомнадзора на этом направлении огромна и разнообразна: от создания информационных платформ и

---

yad-li-predstavlyaete-skolko-raznyh-instrumentov-dlya-slezhki-vnedreno-v-etot-messendzher (дата обращения: 22.05.2026); Стрельников Алексей. «Мессенджер-шпион Max? Как россияне переходят на “максофоны”». *Deutsche Welle* от 23 марта 2026 года. https://www.dw.com/ru/max-messendzerspion-pocemu-rossiane-perehodat-na-maksofony/a-76494140 (дата обращения: 23.04.2026).

[44] Enders Anna, Lea Horne, and Marla Rivera. *The Max Messenger: An Analysis of Russia’s State-Mandated Messaging Application*. InterSecLab, September 2026.

[45] Михальченко Елизавета и Ксения Миронова. «Школа хочет все знать о семье. В цифровую образовательную среду могут быть включены персональные данные учеников, учителей и родителей». *Издание «Коммерсантъ»* от 19 июня 2019 года; Степанова Юлия и Анастасия Гаврилюк. «Школьникам соберут портфолио. Российских учеников снабдят цифровым профилем». *Издание «Коммерсантъ»* от 8 июня 2021 года.

[46] См. раздел IV. «Региональные ИСиР» приложения к Приказу Минпросвещения России от 02.12.2019 N 649 «Об утверждении Целевой модели цифровой образовательной среды» https://www.consultant.ru/document/cons_doc_LAW_341443/ad8f4e028380894173b4f017a56c42b4c5e4ad54/#dst100011 (дата обращения: 13.08.2026).

[47] См. пункт 4 Постановления Правительства РФ от 13.07.2022 N 1241 «О федеральной государственной информационной системе “Моя школа”» https://www.consultant.ru/document/cons_doc_LAW_422207/ (дата обращения: 06.08.2026).

[48] См. пункт 2 Постановления Правительства РФ от 14.05.2021 N 733 «Об утверждении Положения о федеральной государственной информационной системе “Единая информационная платформа национальной системы управления данными” и о внесении изменений в некоторые акты Правительства Российской Федерации» https://www.consultant.ru/document/cons_doc_LAW_384215/ (дата обращения: 14.08.2026).

внедрения инфраструктуры по перехвату трафика (ТСПУ) до разработки отдельных программ и массового мониторинга сети с помощью алгоритмов ИИ[49].

Постановление № 1241 также устанавливает возведение ФГИС «Моя школа» на базе единой платформы «ГосТех»[50], которая служит еще одним важным элементом проекта по интеграции систем различных ведомств. Примечательно, что реализацию этой инициативы также контролирует Минцифры, которое в качестве подрядчика выбрало «Ростелеком» — технического разработчика и оператора многочисленных систем государственной слежки, который еще не раз будет упомянут в этом докладе. В декабре 2025 года чиновники назначили компанию единственным исполнителем работ[51]. Платформа «ГосТех» была задумана властями в конце 2010-х годов как унифицированная экосистема создания госсистем, а также единое облачное пространство для максимально быстрого обмена и аналитики данных, стандартизированных в рамках НСУД. Поскольку ФГИС «Моя школа» перешла под управление Минцифры, курирующего также и «ГосТех», школьная площадка стала одной из первых государственных систем, переведенных в это единое информационное пространство. Впрочем, после быстрого начала процесс застопорился. Конкуренция между ведомствами, опасения чиновников по поводу утечки данных, а также стремление властей внедрить новейшие технологии привели к реформированию проекта в 2025 году и появлению концепции «ГосТех 2.0»[52]. Обновление проекта быстро отразилось на развитии системы школьной слежки.

Так, в июне-июле 2026 года управления образованием и школы некоторых регионов в массовом порядке начали публиковать однообразный анонс перехода на Типовое облачное решение «Моя школа» (далее — ТОР). Этот процесс, по сути, «задним числом» был закреплен на федеральном уровне августовским постановлением Правительства РФ[53]. Сам ТОР создан на платформе «ГосТех» и представляет собой единый продукт для всех российских школ. Суть этого «решения» заключается в дальнейшей унификации образовательной цифровой экосистемы. Дело в том, что до этого данные во ФГИС «Моя школа» попадали из разных региональных и коммерческих систем, разрабатываемых на местах. В результате информация не была полностью стандартизирована, как и интерфейс ее подачи и функции, доступные образовательным организациям. ТОР полностью меняет эту ситуацию, знаменуя собой большой шаг российских властей к установлению тотального и централизованного контроля над школами в целом и детьми в частности. Летом 2026 года переход на ТОР совершили 20 «пилотных» регионов[54], и чиновники, судя по всему, планируют вскоре распространить его на все подконтрольные школы, исключая, видимо, Москву и несколько других субъектов федерации, чья развитая инфраструктура и без того полностью соответствует требованиям унификации.

---

[49] Литаврин Максим и Давид Френкель. «Нейроскомнадзор. Чем пользуется РКН, чтобы следить за интернетом — и кто ему в этом помогает». *Медиазона* от 8 февраля 2023 года. https://zona.media/article/2023/02/08/grccc (дата обращения: 10.08.2026); Агентство. «Крупнейший взлом российской цензуры: как она охраняет здоровье Путина, помогает Навке, заводит досье на журналистов и разводит ботов». *Издание «Агентство»* от 8 февраля 2023 года. https://www.agents.media/tsenzura/ (дата обращения: 10.08.2026).

[50] См. пункт 5 Постановления Правительства РФ от 13.07.2022 N 1241 «О федеральной государственной информационной системе “Моя школа”» https://www.consultant.ru/document/cons_doc_LAW_422207/ (дата обращения: 06.08.2026).

[51] Сизова Ника. «“Гостех 2.0” будет работать на решениях провайдера облачных технологий Cloud.ru». *Издание «Ведомости»* от 18 мая 2026 года.

[52] Петрова Венера и Олег Сапожков. «“Гостех”, раз-два». *Издание «Коммерсантъ»* от 22.09.2025.

[53] Постановление Правительства РФ от 01.08.2026 N 962 «О внесении изменений в постановление Правительства Российской Федерации от 13 июля 2022 г. N 1241» https://www.consultant.ru/document/cons_doc_LAW_541441/ (дата обращения: 12.09.2026).

[54] См., например, CNews. «Минцифры: приложением “Госуслуги Моя школа” пользуются более 12 млн человек». *Издание «CNews»* от 1 сентября 2026 года.

Не вдаваясь в детальное описание концепции «ГосТех 2.0», а также тех новшеств, которые вносит ТОР, стоит лишь отметить, что власти разрабатывают специальный кластер по работе с большими данными с активным использованием технологий ИИ, включая глубокую аналитику на базе нейросетей[55]. Для детей и их родителей это, по сути, означает, что, с одной стороны, данные о них будут подвергаться разнообразному алгоритмическому анализу, а с другой — служить материалом для обучения государственных моделей ИИ. Более того, предиктивная аналитика на базе цифровых профилей школьников уже ведется, и это не домыслы, а факт, подтверждаемый презентациями Минпросвещения и Минцифры[56]. Как итог, все уже указывает на глубокую интеграцию ФГИС «Моя школа» в федеральную архитектуру управления, включая общегосударственную систему слежки, что отчетливо прослеживается не только на техническом и функциональном, но и на организационном уровнях.

[55] Петрова Венера и Олег Сапожков. «“Гостех”, раз-два». *Издание «Коммерсантъ»* от 22.09.2025.
[56] Министерство просвещения РФ / Министерство цифрового развития, связи и массовых коммуникаций РФ. (2026). Памятка: Типовое облачное решение (ТОР) «Моя школа» [Внутренний регламент федерального ИТ-внедрения]. Размещено на официальном сервере Управления образования КУГО. https://obr-ku.ru/images/Documents/TOR/%D0%A2%D0%9E%D0%A0_%D0%9C%D0%BE%D1%8F_%D1%88%D0%BA%D0%BE%D0%BB%D0%B0_%D0%9F%D0%B0%D0%BC%D1%8F%D1%82%D0%BA%D0%B0.pdf (дата обращения: 12.09.2026).

Второй периметр

Видеонаблюдение и аудиоконтроль

Режимный доступ и биометрия

С инфраструктурой ФГИС «Моя школа» через региональные образовательные платформы интегрирована Система контроля и управления доступом (далее — СКУД), фиксирующая время прихода ребенка в школу и его ухода. Обычно это турникет или ворота, которые открываются при прикладывании к считывающему устройству карты, браслета или брелока с чипом RFID[57]. Данные немедленно поступают в цифровой профиль обучающегося, что позволяет отслеживать посещаемость, а также использовать эти показатели в качестве параметра для поведенческой аналитики: опаздывает ли ребенок, приходит ли сильно заранее, выходит ли из здания на переменах.

В последние годы комплексы СКУД на RFID постепенно замещаются идентификацией через системы распознавания лиц, интегрированные с Единой биометрической системой (далее — ЕБС)[58]. Несмотря на заявления властей о том, что биометрическая пропускная система внедряется только с согласия родителей, на деле для его получения еще с конца 2010-х годов применяются обман, манипуляции и административное давление[59]. Более того, в некоторых случаях (прежде всего в рамках функционирования системы «Безопасный город») технологии распознавания лиц детей в школах используют даже без уведомления родителей.

Камеры и микрофоны

Так, с одной стороны, СКУД связана с ФГИС «Моя школа», а с другой — все чаще становится элементом общей инфраструктуры видеонаблюдения образовательной организации и, что еще важнее, видеоаналитики. Например, даже если в школе не реализована система входа детей по биометрии, камеры видеонаблюдения, подключенные к программе распознавания лиц, могут определить, кто именно использует пластиковую карту на турникете. При этом видеокамеры в школах устанавливаются далеко не только на входах и выходах, а современные комплексы на базе ИИ способны фиксировать множество параметров, включая поведение учеников на переменах, время пребывания в столовой, степень вовлеченности в общественные мероприятия, манеру ходить и одеваться, а также «предосудительные» действия и круг общения.

Хотя чиновники заявляют о внедрении этих систем для безопасности учащихся, пресечения драк и предотвращения буллинга, в российской реальности власти настраивают новые технологии также, или, вероятно, даже в первую очередь, для контроля за лояльностью детей и их восприимчивостью к индоктринации. При том, что новейшие технологии ИИ имеют

[57] Постановление Правительства РФ от 13.07.2022 N 1241 «О федеральной государственной информационной системе "Моя школа"» https://www.consultant.ru/document/cons_doc_LAW_422207/ (дата обращения: 06.08.2026).
[58] Воронов Александр и Алексей Жабин. «Детские лица сканируют для взрослых схем. В правительстве РФ рассказали, как может заработать биометрия в школах». *Издание «Коммерсантъ»* от 3 декабря 2025 года.
[59] Позычанюк Валерия. «Операция “Детские ладошки”. Зачем “Сбер” собирает биометрические данные школьников». *The Bell* от 7 октября 2020 года. https://thebell.io/operatsiya-detskie-ladoshki-zachem-sber-sobiraet-biometricheskie-dannye-shkolnikov (дата обращения: 09.09.2026).

широчайший круг возможностей, нельзя забывать, что использование систем видеоаналитики и их конкретный функционал напрямую зависят от инфраструктуры учебного заведения, развитости операционных центров и политики местной администрации. В крупном региональном центре школы могут быть оснащены многочисленными видеокамерами, соединенными с алгоритмами, позволяющими определять вплоть до того, в каком настроении ребенок пришел, находился в школе и ушел из нее. В то же время в бедном сельском учебном заведении по кадрам из пары старых видеокамер может быть затруднительно даже отличить первоклассника от пятиклассника.

Установка видеокамер в школах имеет долгую историю, однако федеральный масштаб этот тренд приобрел с конца 2010-х годов. Так, летом 2019 года Правительство РФ выпустило постановление, которым обязало все образовательные организации установить видеокамеры в рамках «*мероприятий по обеспечению антитеррористической защищенности объектов (территорий)*»[60]. В начале 2020-х годов по проекту ЦОС аналоговые видеокамеры в школах стали заменяться цифровым HD-оборудованием, способным интегрироваться в облачные метаплатформы, содержащие аналитические ИИ-системы[61]. Москва вновь выступила в качестве передового региона и уже в 2021 году выделила три миллиарда рублей на оборудование столичных школ камерами с высоким разрешением[62]. Это объяснялось тем, что процесс монтажа устройств и подключения их к алгоритмам видеоанализа в столице начался задолго до анонса федеральных программ. Так, еще в 2012 году власти Москвы анонсировали проект подключения всех столичных образовательных организаций к Единому центру хранения и обработки данных (далее — ЕЦХД)[63].

Для того чтобы соответствовать текущим минимальным требованиям, типичная школа из одного здания должна иметь около 15–20 видеокамер. При этом во многих учебных заведениях это число значительно больше. Общее количество устройств, их технические характеристики и размещение различаются в зависимости от образовательной организации и региона. Согласно нормативам[64], установка видеокамер обязательна на входах и выходах, вдоль ограждения, а также внутри здания — в коридорах и местах массового нахождения людей (под чем власти на местах обычно понимают установка камер в актовых и спортивных залах, центральных гардеробах и столовых). Наряду с этим все чаще оборудование появляется также на лестничных площадках и в зонах около раздевалок. Практика размещения видеокамер в учебных классах, хотя и не является пока повсеместной, получает все большее распространение. Общефедеральный импульс этому дало требование по оснащению системами наблюдения аудиторий, в которых проводятся итоговые экзамены

---

[60] См. раздел III Постановления Правительства РФ от 02.08.2019 N 1006 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)» https://www.consultant.ru/document/cons_doc_LAW_331342/ (дата обращения: 30.07.2026).

[61] Приказ Минпросвещения России N 634, Минцифры России N 925 от 08.09.2021 «Об утверждении стандарта оснащения государственных и муниципальных общеобразовательных организаций, осуществляющих образовательную деятельность в субъектах Российской Федерации, на территории которых проводится эксперимент по внедрению цифровой образовательной среды, компьютерным, мультимедийным, презентационным оборудованием и программным обеспечением».

[62] Холупова Кристина. «В московских школах установят тысячи видеокамер за миллиарды рублей». *Издание «CNews»* от 21 августа 2021 года.

[63] Постановление Правительства Москвы от 07.02.2012 N 24-ПП «Об утверждении Положения о государственной информационной системе “Единый центр хранения и обработки данных”».

[64] Постановление Правительства РФ от 02.08.2019 N 1006 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)» https://www.consultant.ru/document/cons_doc_LAW_331342/ (дата обращения: 30.07.2026).

ОГЭ и ЕГЭ[65]. Как итог, нередко директора начинают использовать эти технические средства не только во время экзаменов, но и в повседневной практике, постепенно дополняя их камерами в других классах.

Надо также учитывать, что современные камеры зачастую оснащены чувствительными микрофонами, записи разговоров детей с которых могут быть распознаны и проанализированы с помощью алгоритмов ИИ. Маловероятно, что сейчас это массовая практика в силу сложности и затратности подобных систем. Пока власти официально заявляют лишь о фиксации звуковых аномалий (хлопки, взрывы, шум паники, триггерные выкрики) в некоторых школах[66]. Однако нельзя исключать, что в отдельных образовательных организациях аудиопотоки уже проходят и более глубокую аналитику, конечной целью которой является комплексный поведенческий анализ и интеграция полученных данных с цифровыми профилями детей.

К трансляциям и архивам записей имеют доступ различные ведомства и сотрудники, а их конкретный круг зависит от решения администрации учебного заведения, региональных властей и силовых ведомств. Все это делает конфиденциальность детских данных и регулирование их обработки крайне условными. Так, в школах просматривать видеопотоки и их архивы могут директора и их заместители, сотрудники охраны, системные администраторы (нередко эту роль выполняют учителя информатики), а порой и другой персонал (гардеробщики, сторожа, социальные педагоги, лаборанты кабинетов информатики)[67]. Более того, руководство школы зачастую оставляет за собой возможность по собственному разрешению — которое, впрочем, не регламентируется и носит, судя по всему, обычно устный характер — позволять знакомиться с отдельными фрагментами всем, кого сочтет нужным. Но и это еще не все. Если раньше трансляции и записи были ограничены школьными серверами и хранились на изолированном жестком диске, то сейчас по примеру московского ЕЦХД на уровне субъектов федерации идет активная консолидация сбора и обработки видеоданных.

Так, в рамках программ «Безопасный город» и «Безопасный регион» большинство российских регионов создали крупные центры хранения и аналитики данных, к которым активно подключаются образовательные организации. В результате этого процесса сотрудники ФСБ, МВД, Росгвардии, а порой и других ведомств имеют прямой доступ со своих терминалов к системам видеонаблюдения все большего числа школ[68]. Теперь для получения данных им больше не нужно оформлять запросы и приезжать в учебные заведения для копирования видеоархивов. Администрация образовательной организации совершенно

---

[65] Приказ Минпросвещения России N 233, Рособрнадзора N 552 от 04.04.2023 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего общего образования» https://www.consultant.ru/document/cons_doc_LAW_447215/ (дата обращения: 24.08.2026).

[66] См., например: Новые известия. «“Это - не слежка”: в школах Екатеринбурга впервые в России установили прослушку». *Новые известия* от 7 апреля 2022 года.

[67] См. нормативные документы школ из разных российских регионов, например: Приказ Директора ГБОУ РД «РЦО» № 109 от 30.08.2021 «Положение о системе видеонаблюдения»; Приказ Директора ГБОУ «СОШ № 4 г. Сунжа им. А.М. Калиматова» № 220/5 от 01.09.2022 «Положение о системе видеонаблюдения»; Приказ Директора МБОУ «Ковжинская средняя общеобразовательная школа» № 166 от 26.12.2023 «Положение о системе видеонаблюдения»; Приказ Директора МБОУ «СОШ № 4 г. Тосно от 02.09.2024 № 450 «Положение о системе видеонаблюдения».

[68] Сотрудники ФСБ, МВД и Росгвардии имеют расширенные полномочия в рамках так называемое «антитеррористической деяельности» и составляют костяк ведомств, имеющих прямой доступ к видео из школ. Однако список ведомств с таким доступом может быть шире, поскольку, например, Правительство Москвы оставляет за собой решение о предоставлении «*доступа на постоянной основе в режиме реального времени с функциями просмотра потоковой информации, просмотра архивной информации и к прочим сервисам государственной информационной системы “Единый центр хранения и обработки данных*”» на основе заявки. (см. Распоряжение Департамента информационных технологий г. Москвы от 31.07.2015 N 64-16-241/15).

исключена из этого процесса, и ни директор, ни тем более родители не знают, кто, когда, какие записи и в каких именно целях просматривает. Проблема, однако, не ограничивается упрощением доступа для силовиков. Огромные массивы поступающих видеоматериалов анализируются с помощью алгоритмов ИИ без какого-либо общественного контроля, а также служат базой для обучения нейросетей. Эта централизация произошла не сразу, поскольку сначала власти планировали развернуть обособленную школьную систему видеоаналитики.

Проекты видеоаналитики

В 2020 году стало известно, что в рамках нацпрограммы «Цифровая экономика» госкорпорации «Роснано» и «Ростех» получили контракт на массовую установку видеокамер в образовательных организациях. Особенность проекта заключалась в том, что оборудование подключалось к системе компьютерного зрения с говорящим названием «Оруэлл», которая, помимо прочего, включала модуль распознавания лиц, разработанный российской компанией NtechLab (технологический партнер «Ростеха»)[69]. Надо отметить, что NtechLab стала широко известна еще в конце 2010-х годов, поскольку именно с помощью ее технологий московские власти развернули масштабную кампанию по идентификации и преследованию мирных оппозиционеров и гражданских активистов[70]. К середине 2020 года системный интегратор «Элвис-Неотек» (аффилированный с «Роснано»), непосредственно занимавшийся реализацией проекта, отчитался об установке видеокамер в 1 608 школах в 12 субъектах федерации, имея при этом планы к 2024 году охватить все 43 тысячи российских школ[71]. Однако масштабная инициатива столкнулась с рядом препятствий: от резкого отторжения со стороны общественности и высокой стоимости до инфраструктурных барьеров и возникшего позже дефицита импортного оборудования.

Действительно, новости о массовом развертывании технологий по распознаванию лиц в школах вызвали сильную критику со стороны правозащитников, ИТ-экспертов и родительского сообщества. Это побудило представителей «Ростеха» выступить с двусмысленным заявлением о том, что устанавливаемые камеры якобы не содержат таких технологий[72]. Хотя подобная декларация, очевидно, служила лишь для отвода глаз (алгоритмы распознавания встраиваются не в саму камеру, а применяются на этапе обработки видеопотока на сервере), она продемонстрировала озабоченность чиновников ростом недовольства. И это был не единственный пример резко негативного отношения общественности к подобным инициативам. Когда в 2021 году стало известно, что власти Московской области планируют развернуть в нескольких школах эксперимент по внедрению ИИ для анализа поведенческих паттернов учеников и прогнозирования рисков, региональное руководство под давлением возмущенных родителей было вынуждено отказаться от этих планов[73].

---

[69] Кинякина Екатерина. «Умные камеры будут следить за российскими школьниками. Системой видеонаблюдения с функцией распознавания лиц оснастят все 43 000 школ». *Издание «Ведомости»* от 15 июня 2020 года.

[70] ОВД-инфо. *Как власти используют камеры и распознавание лиц против протестующих*. ОВД-инфо от 17 января 2022 года. https://reports.ovd.info/kak-vlasti-ispolzuyut-kamery-i-raspoznavanie-lic-protiv-protestuyushchih (дата обращения: 19.08.2026).

[71] Кинякина Екатерина. «Умные камеры будут следить за российскими школьниками. Системой видеонаблюдения с функцией распознавания лиц оснастят все 43 000 школ». *Издание «Ведомости»* от 15 июня 2020 года.

[72] Медиазона. «Ростех: устанавливаемые в школах камеры не предполагают технологию распознавания лиц». *Медиазона* от 16 июня 2020 года. https://zona.media/news/2020/06/16/technology (дата обращения: 20.08.2026).

[73] Касми Эльяс. «Искусственный интеллект начинает контролировать поведение детей. Эксперимент поставят на российских школьниках». *Издание* «*CNews*» от 1 июня 2021 года.

Помимо общественного недовольства, проект создания обособленной школьной видеоаналитики столкнулся с аппаратным тупиком. Первоначальная концепция предполагала локальное хранение данных на серверах самих образовательных организаций, что не устраивало силовые ведомства из-за сложности оперативного доступа. Кроме того, последовавшие санкции привели к критическому дефициту вычислительного «железа» и резкому удорожанию всего предприятия. Как итог, власти не только не создали к 2024 году единую федеральную систему школьного видеонаблюдения (что, в частности, продемонстрировали заявления менеджмента NtechLab)[74], но и решили полностью пересмотреть первоначальный проект. Это, однако, свидетельствовало о смене стратегии, а не об отказе властей от идеи видеоконтроля в учебных заведениях. Процесс принудительного оснащения образовательных организаций системами видеоаналитики переместился с федерального уровня на региональный. Фактически это означало сведение видеопотоков со школьных камер напрямую в региональные центры хранения и обработки данных (ЦОД). Регионы взяли за пример практику столичных властей, которые не только создали эффективную систему видеослежки в школах, но и внедрили ее практически без какого-либо сопротивления со стороны общественности. Так, в 2020 году мэрия Москвы заявила о намерении качественного развития предиктивной аналитики на базе видеоданных из школ, что вызвало недовольство родителей[75]. Но столичные чиновники свернули публичное обсуждение этого эксперимента, а образовательные организации просто продолжили обновлять оборудование под предлогом модернизации. Поскольку процессы обработки данных происходят в закрытом контуре ЕЦХД, общественность не знает ни того, какому именно анализу подвергается видео из школ, ни как фиксируются его результаты, ни для чего именно он проводится.

После того как в феврале 2022 года российские власти начали открытую войну против Украины, пространство для гражданского протеста в Москве и других российских регионах резко сократилось. На фоне непрекращающихся репрессивных мер и агрессивной государственной пропаганды сопротивление внедрению видеоаналитики в школах ослабело. Это привело к тому, что в последнее время региональные чиновники перестали скрывать подобные инициативы и, напротив, начали анонсировать в лояльных медиа проекты по установлению алгоритмического надзора в учебных заведениях[76]. Хотя госслужащие обычно ограничиваются общими тезисами о необходимости обеспечения безопасности детей, порой официальные лица бывают более откровенны.

В качестве иллюстрации достаточно привести два примера. Так, мэр Сургута, объявляя в 2025 году об оснащении 35 школ камерами, подключенными к системе распознавания лиц, прямо указал на главного бенефициара проекта и сообщил, что «*вся информация в режиме реального времени находится в управлении внутренних дел*»[77]. Еще более примечательны слова министра образования Свердловской области Светланы Тренихиной, которая весной 2026 года заявила: «*Мы бы хотели использовать искусственный интеллект для обеспечения безопасности в наших школах. Пускай вместе с дежурными на этажах камеры считывают противоправное поведение детей, ставят маркеры. Нам будет легче, и мы высвободим*

[74] Роскомсвобода. «Распознавание лиц внедрили в более чем 60 регионах России». *Роскомсвобода* от 24 октября 2023 года. https://roskomsvoboda.org/ru/post/syst-raspozn-62-region/ (дата обращения: 20.08.2026).
[75] Королев Никита и др. «Контрольная по биометрии». *Издание «Коммерсантъ»* от 7 сентября 2021 года.
[76] Учительская Россия. «Школы Новосибирска планируют оснастить камерами с ИИ для профилактики агрессивного поведения». *Учительская Россия* от 29 августа 2024 года; Гаспарян Тат. «В дагестанских школах появится Wi-Fi и умное видеонаблюдение до конца 2025 года». *Издание «Коммерсантъ»* от 3 июня 2025 года; Петрова Полина. «В школах Петербурга могут начать следить за поведением учеников с помощью искусственного интеллекта». *Петербургская газета* от 19 марта 2026 года.
[77] Дорошенко Дарья. «В школах Сургута установили умные камеры с функцией распознавания лиц». *Югорский снегирь* от 21 августа 2025 года.

наших учителей на более важные содержательные свершения»[78]. Министр не уточнила, о каких «маркерах» идет речь и что она подразумевала под «противоправным поведением» детей. Однако подобная риторика свидетельствует о том, что власти закладывают в алгоритмы ИИ скрытые от общественности и родителей технические критерии «нарушений». Данные о подобных инцидентах, которые нейросети помечают как «нарушение», вполне вероятно, уже заносятся в цифровые профили школьников, а также могут быть использованы, если этого уже не происходит, для составления негласных социальных рейтингов.

[78] Кустов Максим. «В свердловских школах планируют внедрить ИИ для выявления девиантных подростков». *Издание* «*Сигнал"* от 9 апреля 2026 года.

Третий периметр

Школьные компьютеры и сети

Действия учеников на школьных компьютерах уже давно прозрачны для системных администраторов и учителей информатики, но еще несколько лет назад этот надзор обычно ограничивался образовательной организацией.

Сетевая централизация школ

Хотя многие российские школы уже в середине 2010-х годов имели точки подключения к интернету, никакой единой системы сетевого контроля на тот момент не было. Существовали различные требования и рекомендации по доступному контенту в рамках Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию»[79], но администрации школ или региональные власти обычно сами решали, у кого покупать сетевое оборудование, как его настраивать и обслуживать[80]. В итоге активность детей в школьном интернете — особенно если речь шла о пользовании им с личных мобильных устройств — регулировалась слабо, почти не мониторилась и оставалась неизвестной федеральным ведомствам. Для изменения этой ситуации чиновники решили взять под тотальный контроль школьные сети и, надо признать, что достичь этой цели им оказалось гораздо легче, чем внедрить полномасштабную видеоаналитику, поскольку системы мониторинга интернета не бросаются в глаза, а принцип «контроль в обмен на удобство» продемонстрировал свою эффективность. Так, с одной стороны, чиновники, не афишируя, брали под полный контроль школьный сетевой трафик, а с другой — рекламировали бесплатный, защищенный и высокоскоростной интернет.

Итак, поворотной точкой стал все тот же 2019 год, когда власти в рамках проекта ЦОС (нацпроект «Образование») начали массовое оснащение школ унифицированными системами с последующим подключением их к Единой сети передачи данных (далее — ЕСПД)[81]. Эта закрытая специализированная федеральная сеть была официально запущена в начале 2015 года для контроля и защиты трафика государственных ведомств[82]. ЕСПД отделена от публичного интернета специальными криптошлюзами, а весь трафик проходит через специализированные узлы фильтрации[83]. Это делает происходящее внутри

---

[79] Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 N 436-ФЗ https://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 12.08.2026).
[80] Коломыченко Мария. «В России появится школьный реестр запрещенных сайтов». *Издание «CNews»* от 17 апреля 2014 года.
[81] Королев Игорь. «“Ростелеком” получит от властей 10 миллиардов на постройку интернета без Facebook, “Вконтакте” и танчиков». *Издание «CNews»* от 3 августа 2020 года.
[82] Постановление Правительства РФ от 24.11.2014 N 1240 «О некоторых вопросах по обеспечению использования сети передачи данных органов власти» https://www.consultant.ru/document/cons_doc_LAW_171430/ (дата обращения: 12.08.2026).
[83] Приказ Минцифры России N 417, Минпросвещения России N 221 от 30.04.2021 «Об утверждении требований к подключению и доступу, включая требования к передаче данных, государственных и муниципальных образовательных организаций, реализующих программы общего и среднего профессионального образования, избирательных комиссий субъектов Российской Федерации и территориальных избирательных комиссий к единой сети передачи данных». https://www.consultant.ru/document/cons_doc_LAW_388367/2ff7a8c72de3994f30496a0ccbb1ddafdaddf518/ (дата обращения: 26.08.2026).

инфраструктуры полностью прозрачным для тех, кто ее администрирует. Использование популярных мессенджеров (например, Signal, WhatsApp или Viber) в этой сети технически невозможно.

В 2019 году «Ростелеком», вовлеченный во множество других проектов по внедрению государственной слежки[84], включая установку видеокамер и видеоаналитику в рамках программы «Безопасный город»[85], был выбран Правительством РФ единственным исполнителем по подключению школ к ЕСПД[86]. В 2021 году власти назначили эту же госкомпанию единственным подрядчиком и по развертыванию школьных сетей Wi-Fi[87]. В то же время Минцифры, будучи давним партнером «Ростелекома», занималось определением нормативных требований и общим контролем процесса[88]. Уже к концу 2022 года «Ростелеком» отчитался о подключении всех школ к интернету[89], хотя качество этого подключения оставалось под вопросом. Так, в 2025 году в результате опроса Счетной палаты выяснилось, что 44,6% образовательных организаций считают скорость сети недостаточной для «нормальной работы»[90].

Контент-фильтрация и сертификаты шифрования

Уже в первоначальном проекте «Ростелекома» было прописано, что после подключения школ к ЕСПД он должен не только обеспечивать повышенную безопасность соединения и осуществлять жесткую контент-фильтрацию ресурсов, которые к 2025 году по факту были сведены к «белому списку»[91], но также вести «*журналирование поисковых запросов*», создавать «*персональные досье пользователей*» и фиксировать попытки зайти на заблокированные ресурсы[92]. Поскольку авторизация в школьных сетях ведется через Портал «Госуслуги» (а именно через ЕСИА, основным разработчиком которой выступает все тот же «Ростелеком»), это делает анонимный вход в сеть невозможным.

---

[84] См., например, Троицкий Константин. *Государственный информационный ресурс «Цифровой профиль иностранного гражданина» и формирование нового российского тоталитаризма*. Центр защиты прав человека «Мемориал», 2026. https://memorialcenter.org/uploads/Kopiya_Konstantin_Troiczkij_O_czifrovom_profile_inostrannogo_grazhdanin3_6_9157de992b.pdf (Доступ: 03.08.2026).

[85] См., например: Самсонова Анастасия. «“Ростелеком” укрепился в “Безопасном городе”». *Издание «COMNEWS* от 6 июня 2019 года.

[86] Распоряжение Правительства РФ от 21.11.2019 N 2757-р «Об определении публичного акционерного общества “Ростелеком” единственным исполнителем осуществляемых Минкомсвязью России в 2019–2020 годах для государственных и муниципальных образовательных организаций, реализующих программы общего и среднего профессионального образования, избирательных комиссий субъектов Российской Федерации и территориальных избирательных комиссий закупок услуг».

[87] Распоряжение Правительства РФ от 22.03.2021 N 713-р «Об определении публичного акционерного общества "Ростелеком" единственным исполнителем осуществляемых в 2021–2022 годах закупок товаров (работ, услуг), необходимых для осуществления мероприятий, связанных с формированием устойчивой информационно-коммуникационной инфраструктуры государственных и муниципальных общеобразовательных организаций».

[88] Постановление Правительства РФ от 24.11.2014 N 1240 «О некоторых вопросах по обеспечению использования сети передачи данных органов власти» https://www.consultant.ru/document/cons_doc_LAW_171430/ (дата обращения: 12.08.2026).

[89] CNews. «“Ростелеком” подключил к безопасному интернету более 47 тысяч школ и техникумов». *Издание «CNews»* от 28 февраля 2023 года.

[90] D-Russia. «Счётная палата: 44,6% школ и колледжей считают недостаточной скорость Интернета для обучения». *Издание «D-Russia»* от 26 июня 2025 года.

[91] Официальное сообщение Минпросвещения России от 14.11.2025 «О разрешенном перечне интернет-ресурсов для использования в образовательном процессе» https://www.consultant.ru/document/cons_doc_LAW_518910/ (Доступ: 25.08.2026).

[92] Королев Игорь. «“Ростелеком” получит от властей 10 миллиардов на постройку интернета без Facebook, “Вконтакте” и танчиков». *Издание «CNews»* от 3 августа 2020 года.

В отношении школьных компьютеров, включающих как стационарные ПК, так и ноутбуки с планшетами, власти пошли еще дальше. Чтобы расшифровывать HTTPS-трафик между браузерами устройств и сайтами, сделав тем самым сетевую активность детей полностью прозрачной, «Ростелеком» использовал технологию перехвата трафика, основанную на так называемой HTTPS-инспекции по принципу Man-in-the-Middle («человек посередине»). Так, провайдер обязал системных администраторов устанавливать на все школьные устройства с выходом в интернет специальный государственный корневой сертификат шифрования, направляя тем самым трафик через специализированный прокси-сервер[93]. В результате «Ростелеком» получил возможность дешифровать защищенное HTTPS-соединение в веб-браузерах и, по сути, видеть интернет глазами ученика, фиксируя в своих мониторинговых базах всю его веб-активность: от поисковых запросов и комментариев на форумах до лайков под постами и просмотренных видео.

Но даже после введения всех этих механизмов контроля препятствием для властей на пути к установлению тотальной слежки за сетевой активностью детей оставалась возможность доступа несовершеннолетних (даже в школьных сетях) к независимым веб-ресурсам и приложениям через собственные мобильные или стационарные устройства, которые не были превращены в инструменты госнадзора. Помимо сугубо школьных мер — подключения к ЕСПД и установки госсертификатов — власти опираются на механизмы, охватывающие все российское население. Речь идет об углублении общефедерального мониторинга сети, дальнейшем развитии Системы оперативно-розыскных мероприятий (СОРМ) и усилении интернет-цензуры. В то же время в отношении несовершеннолетних развиваются и специфические способы слежки. Во-первых, ведется целенаправленный мониторинг детской среды в интернете; во-вторых, внедряются так называемые «детские сим-карты»; в-третьих, законодательно ограничивается использование личных гаджетов в школах. Первые два направления описаны в следующих разделах, здесь же стоит остановиться на третьем, поскольку оно связано непосредственно с попытками властей понудить детей применять для выхода в интернет исключительно школьные компьютеры и сети.

Вытеснение личных устройств

Ограничения на использование детьми мобильных телефонов в школах — широко распространенная в мире практика. Поэтому, когда в 2023 году российские чиновники законодательно запретили пользование гаджетами во время уроков, мало кто возражал против этой меры[94]. Однако детали этой реформы демонстрируют, что российские власти лишь прикрываются заботой о благополучии детей, а их главным мотивом выступает подавление цифровой независимости учеников и установление централизованного контроля над их политическими предпочтениями. На первый взгляд такое утверждение может показаться конспирологией, но в пользу данной версии говорят сразу несколько фактов:

- Ограничения на мобильные телефоны были широко распространены в российских школах задолго до 2023 года. У администраций учебных заведений и родительских комитетов уже имелись все полномочия, чтобы закрепить эти нормы в локальных уставах без федерального вмешательства, что многие школы и делали[95].

[93] Требование Ростелекома по установке «корневых сертификатов» для подключения к ЕСПД сформулировано на официальном сайте этой госкомпании в разделе поддержки.
[94] Федеральный закон «О внесении изменений в Федеральный закон “Об образовании в Российской Федерации”» от 19.12.2023 N 618-ФЗ https://www.consultant.ru/document/cons_doc_LAW_464808/ (дата обращения: 17.08.2026).
[95] См., например: Лукьянова Ирина. «Закон о хорошем поведении. Как и зачем депутаты опять отнимают у школьников телефоны». *Новая газета* от 7 ноября 2023 года.

- Федеральному закону 2023 года непосредственно предшествовали два важных шага. В 2021 году Роспотребнадзор в рамках новых санитарных правил (СП 2.4.3648-20) запретил использовать личные смартфоны «для образовательных целей»[96], а на следующий год глава Минпросвещения напомнил о необходимости следовать этому запрету[97]. Акцент на запрете использования именно собственных мобильных устройств выдает стремление чиновников заставить детей пользоваться исключительно школьным оборудованием.
- Скоординированные действия Роспотребнадзора и Минпросвещения примечательным образом совпали по времени с завершением проекта «Ростелекома» по подключению школ к ЕСПД и принудительной установкой государственных корневых сертификатов, открывающих трафик для мониторинга.
- Заявления чиновников о вреде экранов выглядят двулично на фоне административного принуждения детей проводить в интернете продолжительное время. Так, школьников все больше обязывают читать, выполнять домашние задания, проходить опросы и общаться через ФГИС «Моя школа», а «учебные» ресурсы постоянно разрастаются, вбирая в себя неучебные функции (новостные ленты, блоги, чат-боты и игры).
- В начале 2026 года появились сообщения о планах властей полностью запретить мобильные телефоны детям до определенного возраста[98]. Примечательно, что эту инициативу вновь продвигает глава Минпросвещения Сергей Кравцов, который, видимо, готовит почву для новых ограничений прав и свобод. Параллельно с этим государство активно разрабатывает «детские сим-карты», а также форсирует развитие онлайн-обучения, из чего становится ясно, что под запретом мобильных телефонов чиновники имеют в виду вовсе не отказ от экрана. Речь, очевидно, идет о запрете или ограничении на использование несовершеннолетними личных устройств с «недетскими» сим-картами — то есть гаджетами, активность в которых государство не контролирует полностью.

Все это демонстрирует, что российские власти целенаправленно загоняют несовершеннолетних не только на официальные онлайн-платформы, но и на контролируемые физические устройства. Эти компьютеры и гаджеты не просто полностью открыты для надзора, но и используются в качестве поставщиков данных для предиктивного анализа и обучения государственных моделей ИИ.

---

[96] См. пункт 3.5.3 Постановления Главного государственного санитарного врача РФ от 28.09.2020 N 28 «Об утверждении санитарных правил СП 2.4.3648-20 “Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи”» (вместе с «СП 2.4.3648-20. Санитарные правила...»)
https://www.consultant.ru/document/cons_doc_LAW_371594/a87d3709aa01857b67d2d04477b1d8458572e62e/ (Дата обращения: 17.08.2026).

[97] Азаттык Азия. «В России запретили использовать телефоны на уроках в школе». Радио «Свобода» от 31 августа 2022 года. https://www.azattyqasia.org/a/32012530.html (Дата обращения: 19.08.2026).

[98] Ефремов Геннадий. «Некоторым россиянам хотят полностью запретить пользоваться сотовыми телефонами и смартфонами. Кого коснется». *Издание* «*CNews*» от 25 марта 2026 года.

Четвертый периметр

Мониторинг внешкольной сетевой активности

Пока чиновники окончательно не изолировали «российский сегмент» интернета от мирового и не ввели тотальный запрет на использование негосударственных гаджетов для всего зависимого населения, некоторые действия несовершеннолетних в сети все еще ускользают от надзора. Вне учебных заведений и официальных образовательных платформ контролировать поведение детей российским властям не так просто, что явно вызывает их глубокую озабоченность. Более того, даже если в практику войдут «детские сим-карты», отследить использование несовершеннолетними смартфонов или компьютеров взрослых вне школьных стен государственным структурам будет довольно сложно. Чтобы взять под контроль этот плохо обозримый сегмент, власти уже не первый год внедряют альтернативные практики слежки, активно вовлекая в них школы. Среди этих механизмов следует выделить три ключевых: административно-педагогический цифровой мониторинг, парагосударственные «кибердружины» и нейросетевые системы федеральных ведомств.

Административно-педагогический мониторинг

Во второй половине 2010-х годов, во многом из-за растущей популярности оппозиционных настроений среди подростков и молодежи[99], директора школ по распоряжению из региональных администраций начали в кулуарном порядке требовать от классных руководителей разыскивать аккаунты учеников и фиксировать их онлайн-активность[100]. Эту практику можно обозначить как «административный сталкинг», понимая под ним неформальное институциональное отслеживание цифрового следа учащихся, которое оборачивается грубым вмешательством в их частную жизнь.

Как и во многих других случаях, российские чиновники прикрываются аргументами о том, что все эти меры необходимы для спасения детей от суицидов, наркотиков и насилия. Однако эта апелляция быстро выдает свою неискренность. Превращение учителей в надзирателей разрушает остатки доверия и грозит еще большим замыканием сложных подростков в себе. Если бы власти действительно интересовало оказание психологической помощи несовершеннолетним в сложной ситуации, они не создавали бы атмосферу всеобщего недоверия, не насаждали бы культ подобострастия и доносительства, не пропагандировали бы милитаризм и не использовали бы учителей в качестве шпионов. В то же время регламенты демонстрируют, что учительский мониторинг в первую очередь нацелен не на психологическую помощь и реабилитацию, а на слежку и передачу данных в МВД с опорой на дисциплинарные и репрессивные меры. Необходимость эффективной профилактики деструктивного поведения и помощи подросткам в сложной жизненной ситуации — это долг родителей, близких, учителей и, в принципе, всех взрослых. Однако действия российских властей доказывают: трагедии детей обычно используются как предлог для введения все

[99] См., например: HRW. «Россия: Школьников и студентов преследуют после протестов». *Human Rights Watch* от 23 июня 2017 года. https://www.hrw.org/ru/news/2017/06/23/russia-children-students-targeted-after-protests (дата обращения: 17.08.2026).
[100] Литой Александр. «“Большой брат” от звонка до звонка. Как следят за соцсетями школьников». *Радио «Свобода»* от 22 декабря 2019 года. https://www.svoboda.org/a/30338558.html (дата обращения: 17.08.2026).

более жесткого надзора, который не улучшает, а усугубляет ментальное здоровье школьников.

К началу 2020-х годов административный сталкинг усилился и трансформировался в слежку и борьбу, по сути, с любой критикой режима со стороны школьников[101]. Вместе с этим власти стали постепенно легализовать эту деятельность, поэтому на уровне отдельных учебных заведений, муниципалитетов и регионов начали появляться локальные нормативные акты, закрепляющие обязательность «мониторинга социальных сетей»[102]. Эти документы, многие из которых остаются в действии, обычно содержат алгоритмы и методические рекомендации, предписывающие классным руководителям проводить регулярный аудит профилей своих учеников и фиксировать в специальных журналах учета круг общения ребенка, тематику групп, в которых он состоит, комментарии и даже лайки. Так, например, в образце, выпущенном в Саратовской области, в случае «*обнаружения на изучаемых страничках пользователей информации*» (от наличия «*терминологии, используемой в среде потребителей наркотических средств*» и выражения «*гнева*» до членства в группах, «*склоняющих к противоправным действиям*», и размытого «*и т.п.*») педагогу вменяется в обязанность сообщить об этом директору[103], которому, в свою очередь, предписывается сотрудничать с органами МВД[104]. Материалы содержат и практические советы учителям, фактически обучая их методам агентурного внедрения. Так, чтобы войти в доверие к учащимся и получить доступ к их закрытым страницам, сотрудникам школ рекомендуют «*не навязывать себя и свои взгляды подросткам... наблюдать... быть естественными и искренними*»[105].

В последние годы практика мониторинга интернета силами педагогов не только постепенно легализуется, но и получает централизованные алгоритмы и критерии. Так, в начале 2025 года Федеральное агентство по делам молодежи (Росмолодежь) разослало региональным властям письмо с просьбой распространить среди подведомственных организаций «*методические рекомендации и информационные материалы по профилактике распространения терроризма, экстремизма и неонацизма с учетом современных вызовов и угроз*»[106]. Хотя в теме документа сделан акцент на «профилактической работе» среди

---

[101] См., например: Луговская Елизавета. «За вашими детьми следят. Кто и зачем просит учителей мониторить соцсети учеников». *Издание «Мел»* от 28 апреля 2021 года; Савицкая Людмила. «Срочно удали лайк, иначе утром подают в полицию». *Радио «Свобода»* от 28 января 2021 года. https://www.svoboda.org/a/31074785.html (дата обращения: 26.05.2026).

[102] Управления образования и школы разных регионов начали массово публиковать приказы о проведении мониторинга социальных сетей, начиная с 2021 года. Вот лишь несколько иллюстраций: Приказ Комитета образования и науки Курской области от 20 мая 2021 года N 1-552 «Об организации в образовательных организациях Курской области мониторинга аккаунтов обучающихся в социальных сетях»; Приказ Управления образованием администрации Ивантеевского муниципального района Саратовской области от 10 ноября 2022 года N 211 «О проведении мониторинга социальных сетей несовершеннолетних» https://uoivanteevka.ucoz.ru/sport/prikaz_o_prov_mon_socset_22.pdf (дата обращения: 19.08.2026); Приказ Управления образованием Тавдинского городского округа Свердловской области от 19 февраля 2024 года N 109 «Об утверждении Порядка проведения мониторинга аккаунтов социальных сетей несовершеннолетних в образовательных организациях в новой редакции»; Приказ МБОУ "Лицей № 1" п. Добринка Липецкая область от 1 сентября 2025 года № 386 https://lic1dobrinka.gosuslugi.ru/netcat_files/196/2998/Prikaz_o_monitoringe_sotsial_nyh_stey_obuchayuschihsya.pdf (дата обращения: 19.08.2026).

[103] См., например: Приказ Управления образованием администрации Ивантеевского муниципального района Саратовской области от 10 ноября 2022 года N 211 «О проведении мониторинга социальных сетей несовершеннолетних» https://uoivanteevka.ucoz.ru/sport/prikaz_o_prov_mon_socset_22.pdf (дата обращения: 19.08.2026).

[104] Там же.

[105] Там же.

[106] Письмо Федерального агентства по делам молодежи от 27.02.2025 N ГГ/1449-06 «О направлении методических рекомендаций» https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=871483 (дата обращения: 11.09.2026).

молодежи с украинских территорий, оккупированных российскими властями, охват этих методичек гораздо шире, а заявленный фокус используется в качестве прикрытия для развертывания жесткого надзора. Этот циркуляр содержит рекомендации школам и другим государственным и муниципальным учреждениям касательно разных аспектов контроля, включая индоктринацию, унификацию, а также комплекс поощрений и наказаний[107].

Важное место в рекомендациях Росмолодежи занимают вопросы организации слежки как в виде личного наблюдения, так и через мониторинг социальных сетей. Последнему посвящен раздел 7, в котором создатели методических материалов инструктируют сотрудников школ, на что обращать внимание при мониторинге (статус, подписки, содержание публикаций, фотографии, картинки, видео, музыка). Они также выделяют шесть «*групп риска, разделяющих идеи терроризма, экстремизма, в том числе неонацизма и радикального национализма, представители которых могут быть выделены по результатам изучения аккаунтов соцсетей*»[108]. Приводя примеры маркеров, указывающих на принадлежность к одной из «групп риска», авторы рекомендаций среди прочего называют написание постов и комментариев, «*транслирующих мнение иноагентов*», любых публикаций, выражающих «*оппозиционные и антироссийские настроения*»[109], подписку на «*проукраинские сообщества*», а также любую критику войны, развязанной российскими властями против Украины[110]. Иными словами, для формирования «групп риска» сотрудники Росмолодежи использовали популярную тактику: с одной стороны, они смешивают понятия, чтобы приравнять полностью легитимную гражданскую, правозащитную или пацифистскую критику к неонацистскому шовинизму и иной деструктивной идеологии, а с другой стороны, вводят искаженные и размытые критерии «экстремизма», чтобы иметь возможность объявить экстремистом любого, чьи взгляды расходятся с шовинизмом и деструктивной идеологией самого российского режима. В материалах также отмечается, что мониторинг «*должен проводиться на постоянной основе в образовательных организациях, а по его данным должна корректироваться профилактическая работа*»[111]. При всем этом авторы Росмолодежи признают, что по факту «*профилактической работой*» управляют силовые ведомства[112].

Судя по алгоритму из семи шагов, представленному в том же разделе 7, центральное значение в фиксации результатов слежки играют социальные паспорта учащихся, «*составление и систематическое ведение*» которых предписывается сотрудникам образовательных организаций[113]. Это указывает на то, что российский режим встраивает социальные паспорта— введенные в конце 1990-х годов как инструмент социальной, гуманитарной и педагогической поддержки — в систему тотальной слежки. Так, информацию о социальном статусе семьи, ее составе, жилищных условиях, материальном благополучии, психологических или физиологических особенностях ребенка власти решили дополнить результатами мониторинга социальных сетей. Помимо этого, социальный паспорт учащегося оказывается технологически связан с: 1) социальным паспортом класса, 2) цифровым профилем обучающегося во ФГИС «Моя школа» и 3) карточкой учета в ГИС «Профилактика» (если на несовершеннолетнего таковая заведена), о которой пойдет речь ниже.

---

[107] Федеральное агентство по делам молодежи. *Методические рекомендации по профилактике распространения идеологии терроризма, экстремизма и неонацизма* [утв. письмом Росмолодежи от 27.02.2025 № ГГ/1449-06]. 2025.
[108] Там же. С. 37.
[109] Там же. С. 38–40.
[110] Там же.
[111] Там же. С. 35.
[112] Там же. С. 10, 22, 23, 25, 35–36.
[113] Там же. С. 36.

Наряду с распространением одиозных методических материалов[114] Росмолодежь предпринимает и другие шаги по централизации слежки, проводимой сотрудниками школ в социальных сетях. Так, в начале 2026 года стало известно, что руководство Татарстана через школы начало настоятельно требовать от родителей сведения обо всех сетевых аккаунтах детей, включая мессенджеры, социальные сети и телефонные номера. В качестве пояснения было заявлено, что это делается «*для целей межведомственного взаимодействия с Государственным бюджетным учреждением "Республиканский центр молодежных, инновационных и профилактических программ 'Навигатор'"*»[115]. Надо иметь в виду, что хотя юридически этот центр основан Министерством по делам молодежи Республики Татарстан, он вместе с тем интегрирован в общероссийскую повестку и систему проектов Росмолодежи. Практически одновременно с этим, будучи, видимо, еще одной частью единой федеральной кампании, администрация губернатора Свердловской области объявила о запуске системы автоматизированного мониторинга с охватом 4,6 миллиона аккаунтов несовершеннолетних[116]. Остаются неясными ни детали этого сканирования сетей, ни его конкретные параметры, ни чьи аккаунты входят в обозначенное число, учитывая то, что подростков в Свердловской области, согласно статистике, проживает около 150–200 тыс. Поскольку речь идет об общероссийском проекте, очень вероятно, что многие другие регионы также ведут подобную деятельность, но просто не объявляют об этом. В то же время некоторые субъекты федерации из-за слабой развитости инфраструктуры продолжают опираться на мониторинг с помощью учителей, как это демонстрирует, например, Белгородская область[117].

При оценке новой практики, объявленной властями Татарстана и Свердловской области, даже независимые медиа[118] упускают из виду ее важные особенности, а именно то, что мониторинг социальных сетей, во-первых, превратился в скоординированную деятельность школ, региональных администраций, филиалов Росмолодежи, ФСБ и МВД; во-вторых, включает родителей как невольных пособников в установлении тотальной слежки; в-третьих, распространяется не только на социальные сети, но и на весь доступный цифровой след несовершеннолетнего, а также на метаданные телефона; в-четвертых, в нем все более активно задействуют нейросети. В этой новой схеме администрациям школ и учителям отводится роль низовых сборщиков информации, в задачу которых входит получение от родителей номера мобильного устройства ребенка, а также сведений о его аккаунтах в социальных сетях и мессенджерах. Основную же аналитическую работу берут на себя профильные федеральные и региональные ведомства. В случае обнаружения контента, который власти квалифицируют как «деструктивный», запускается механизм скоординированного административного давления, в котором участвуют не только учителя и администрации школ, но и внешние структуры: региональные комиссии по делам

---

[114] Некоторые другие аспекты «Методических рекомендаций по профилактике распространения идеологии терроризма, экстремизма и неонацизма» Росмолодежи, а также рассмотрение методических материалов этого же ведомства, посвященных традиционному наблюдению, были рассмотрены Amnesty International (см.: Amnesty International. «"Только официальные источники": Индоктринация в российском системе образования». Amnesty International от 1 июня 2026 года. С. 16–19).

[115] Радио Свобода. «"Насилие не остановить ни мониторингом, ни запретом соцсетей". О попытках властей усилить контроль за школьниками в интернете». *Радио «Свобода»* от 17 февраля 2026 года. https://www.svoboda.org/a/nasilie-ne-ostanovit-ni-monitoringom-ni-zapretom-sotssetey-o-popytkah-vlastey-usilit-kontrol-za-shkolnikami-v-internete/33680397.html (дата обращения: 27.05.2026).

[116] Новая газета Европа. «Свердловские власти начали мониторить соцсети школьников на предмет "запрещенного" контента». *Новая газета Европа* от 11 марта 2026 года. https://novayagazeta.eu/articles/2026/03/11/sverdlovskie-vlasti-nachali-monitorit-sotsseti-shkolnikov-na-predmet-zapreshchennogo-kontenta-news (дата обращения: 19.08.2026).

[117] Издание «Мел». «Губернатору Белгородской области пожаловались, что учителей заставляют мониторить соцсети школьников и заполнять по ним отчеты». *Издание «Мел»* от 22 марта 2026 года.

[118] Радио Свобода. «"Насилие не остановить ни мониторингом, ни запретом соцсетей". О попытках властей усилить контроль за школьниками в интернете». *Радио «Свобода»* от 17 февраля 2026 года. https://www.svoboda.org/a/nasilie-ne-ostanovit-ni-monitoringom-ni-zapretom-sotssetey-o-popytkah-vlastey-usilit-kontrol-za-shkolnikami-v-internete/33680397.html (дата обращения: 27.05.2026).

несовершеннолетних (КДН), подразделения МВД по делам несовершеннолетних (ПДН) и органы опеки.

Все это, впрочем, не означает, что власти собираются освободить всех учителей от непосредственного мониторинга интернета. Решение о степени вовлеченности в этот процесс, видимо, зависит от региональных чиновников. Судя по всему, администрации некоторых субъектов федерации планируют продолжать продвигать эту активность в школах в прежнем виде, в том числе под вывеской так называемых «кибердружин».

Кибердружины

Еще до начала административного сталкинга особое внимание поведению несовершеннолетних в интернете и в первую очередь в социальных сетях стали уделять некоторые квазиобщественные структуры. Среди них выделялась парагосударственная Лига безопасного интернета (далее — ЛБИ), созданная околокремлевскими бизнес-организациями в тесной координации с МВД, Минцифры (на тот момент — Минкомсвязи) и Комитетом ГД по вопросам семьи, женщин и детей. Приоритетными направлениями деятельности ЛБИ изначально были слежка за поведением детей в сети, сотрудничество со школами и организация кибердружин[119]. Последние занялись передачей силовикам, и прежде всего МВД, информации о размещении в сетях контента, который чиновники обозначали как «запрещенный» или «деструктивный». Под этим предлогом, наряду с детской порнографией, торговлей наркотиками и пропагандой суицида, отслеживались критика власти, участие в оппозиционных движениях и планирование мирных акций протеста[120].

Долгое время деятельность ЛБИ и ее кибердружин[121] маскировалась под общественную, хотя уже со второй половины 2010-х годов многие субъекты федерации, муниципальные образования и школы открыто сотрудничали с этими структурами[122], а некоторые даже начали выпускать нормативные акты, закрепляющие это «взаимодействие» государственных учреждений с ними[123]. И не просто взаимодействовать. Документы из некоторых регионов демонстрируют, что еще в той же второй половине 2010-х годов власти начали использовать школы как базы для создания и развертывания кибердружин. Так, например, постановление муниципальной Комиссии по делам несовершеннолетних и защите их прав (КДНиЗП) Нефтеюганска от 17 марта 2022 года № 11 прямо ссылается на приказы окружного департамента образования еще от 2017–2018 годов, которые предписывали назначить муниципальных кураторов и развернуть кибердружины непосредственно «*на базе общеобразовательных организаций*»[124]. Судя по всему, процесс интенсифицировался в

---

[119] См., например: Daucé Françoise, Benjamin Loveluck, Bella Ostromooukhova, and Anna Zaytseva. “From Citizen Investigators to Cyber Patrols: Volunteer Internet Regulation in Russia”. *Laboratorium: Russian Review of Social Research* 11, (3) (2020): 46–70.

[120] Там же.

[121] ЛБИ задала пример создания «кибердружин», после нее их начали создавать другие преимущественно прокремлевские объединения в качестве своего рода боевых сетевых единиц. Например, особо активны в этой деятельности были так называемые «казачьи организации» (см., например: Daucé Françoise, Benjamin Loveluck, Bella Ostromooukhova, and Anna Zaytseva. “From Citizen Investigators to Cyber Patrols: Volunteer Internet Regulation in Russia”. *Laboratorium: Russian Review of Social Research* 11, (3) (2020): 46–70).

[122] Роскомсвобода. Регионы заводят себе кибердружины. *Роскомсвобода* от 9 октября 2019 года. https://roskomsvoboda.org/ru/50250/ (дата обращения: 27.08.2026).

[123] См., например: Постановление Правительства Белгородской области от 22 мая 2017 года № 181-пп «Об организации деятельности кибердружин Белгородской области»; Постановление Правительства Республики Бурятия от 12 июля 2019 года N 378 «Об утверждении Порядка взаимодействия с кибердружинами в Республике Бурятия»; Постановление Правительства Новгородской области от 23 сентября 2024 года N 457 «Об утверждении Регламента деятельности кибердружин в Новгородской области».

[124] Постановление муниципальной комиссии по делам несовершеннолетних и защите их прав в городе Нефтеюганске от 17.03.2022 года №11 "Об обеспечении информационной безопасности несовершеннолетних на

2022–2023 годах, хотя в зависимости от региона задействование школьников сильно отличалось. В некоторых субъектах федерации директора учебных заведений прямыми приказами создавали на своей базе кибердружины из числа сотрудников организации и старшеклассников[125]. Другие же регионы выбрали путь содействия вербовке школьников сторонними структурами — например, на базе «казачьих объединений» или по линии Росмолодежи.

В 2026 году российские власти решили ввести активность кибердружин в федеральное законодательство, что и было сделано с помощью Распоряжения Правительства РФ № 1030-р от 30 апреля 2026 года. В нем в качестве одной из государственных мер обозначена следующая: «*Организация проведения мероприятий по профилактике негативных социальных явлений с обучающимися на базе образовательных организаций, включая создание и (или) активизацию кибердружин с привлечением активных студентов профессиональных образовательных организаций и медиапатрулей*»[126]. Тем самым эта практика была не только закреплена на федеральном уровне — власти официально перевели квазиобщественные группы в категорию государственных структур. При этом, надо заметить, распоряжение не упоминает открыто школьников, а чиновники заверяют, что участие в подобных объединениях должно быть добровольным. Однако реальность вновь противоречит заявлениям властей, поскольку формирование «дружин» происходит при активном привлечении школьников, и все указывает на то, что это не случайные инициативы, а плановая, спущенная сверху кампания, реализуемая с интенсивным использованием административного ресурса.

Федеральные нейросетевые комплексы и ГИС «Профилактика»

Уже много лет активной и масштабной слежкой в интернете занимаются различные российские федеральные ведомства, и прежде всего МВД, Роскомнадзор, Администрация президента, Росмолодежь, ФСО и ФСБ[127].

С середины 2010-х годов все большее место в этой слежке занимают системы мониторинга на базе алгоритмов ИИ. Например, МВД активно применяет такие разработки, как Findface, «Инсайдер», «Крибрум», «СЕУС», «Серия», «Зеркало», «Клон» и «Конъюнктура»[128]. Роскомнадзор (в основном через Главный радиочастотный центр) использует, среди прочих,

---

территории города Нефтеюганска" https://www.admugansk.ru/uploads/2023/02/%E2%84%96_11_ot_17.03.2022.doc (дата обращения: 16.09.2026).

[125] См. некоторые примеры из разных областей: Приказ ГБОУ «Основная общеобразовательная школа» № 21 города Новокуйбышевска Самарской области № 104-ОД от 19.08.2022 http://nov21ooh.minobr63.ru/wp-content/uploads/2023/11/приказ-об-утверждении-кибердружины-буллинг.pdf (дата обращения: 18.08.2026); Приказ МОБУ «Средняя общеобразовательная школа № 23» города Таганрог от 01.09.2023 № 458 «О создании и деятельности кибердружины МОБУ СОШ № 23 в 2023-2024 учебном году». https://taganschool23.ru/2023-2024/Kiberdrujina/prikaz_o_sozdanii_kiberdruzhiny.pdf (дата обращения: 17.08.2026); Приказ МОУ «Средняя школа № 25 Кировского района Волгограда» № 75 от 23 апреля 2025 года «О создании и функционировании Кибердружины» https://sosh25-vlg2012.ucoz.ru/food2/prikaz_o_sozdanii_kiberdruzhiny.pdf (дата обращения: 18.08.2026).

[126] Распоряжение Правительства РФ от 30.04.2026 N 1030-р «Об утверждении комплекса мер по профилактике негативных социальных явлений в детской и молодежной среде на 2026–2030 годы» https://www.consultant.ru/document/cons_doc_LAW_533626/ (дата обращения: 17.08.2026).

[127] Краткий обзор российской государственной системы слежки см., например, здесь: Центр «Досье». «Глаза Кремля. Как устроен цифровой ГУЛАГ в России — и что мешает ему заработать в полную силу». *Центр «Досье»* от 11 марта 2024 года, https://dossier.center/sorm/ (дата обращения: 15.05.2026).

[128] См., например: Медуза. «Полиция по всей России покупает системы мониторинга соцсетей. Они помогают искать экстремизм “не выходя из рабочего кабинета”». *Медуза* от 16 октября 2018 года. https://meduza.io/feature/2018/10/16/politsiya-po-vsey-rossii-pokupaet-sistemy-monitoringa-sotssetey-oni-pomogayut-iskat-ekstremizm-ne-vyhodya-iz-rabochego-kabineta (Доступ: 15.05.2026).

программные комплексы «Окулус», «Вепрь» и «Чистый интернет»[129]. Список этих инструментов можно продолжать долго, но его масштаб и без того очевиден. Уже сейчас нейросети способны распознавать скрытый смысл сленговых выражений, определять протестную графику на снимках, устанавливать личность школьника по фотографиям плохого качества, а также выявлять связи с «нежелательными» организациями по ряду косвенных признаков.

Обозначенные выше системы не нацелены специально на детей. Если же говорить о слежке именно за несовершеннолетними, то основной госструктурой, которая координирует эту деятельность, как уже должно было стать понятно из вышесказанного, является Росмолодежь. В свою очередь, ключевое место в мониторинге сетей в структуре Росмолодежи занимает так называемый «Центр изучения и сетевого мониторинга молодежной среды» (далее — ЦИСМ). Он оперирует нейросетями, отслеживающими в режиме реального времени миллионы аккаунтов подростков и молодых людей в социальных сетях на наличие «деструктивного контента». В том числе для фиксации и структурирования этих данных ЦИСМ разработал Автоматизированную информационную систему «Профилактика» (АИС «Профилактика»). В 2025 году стало известно, что данная разработка была передана Минпросвещения, которое организовало тендер на 30,6 млн рублей с целью ее модернизации и масштабирования на федеральный уровень[130]. По итогам этих работ название системы поменялось на Государственную информационную систему «Профилактика» (далее — ГИС «Профилактика»), а ее официальный запуск состоялся 1 декабря того же года[131].

ГИС «Профилактика» имеет широкий функционал и создана как единая база учета. В ней аккумулируются сведения о безнадзорных и трудных подростках, о нарушениях несовершеннолетних, а также о неблагополучных семьях с целью последующей унификации, анализа и распределения этих данных. Согласно постановлению Правительства РФ № 411 от 1 апреля 2025 года, в формировании ГИС «Профилактика» принимает участие множество ведомств, которые делятся между собой очень разнообразной информацией, включающей анкетные данные детей и их законных представителей, факты об уходе несовершеннолетних из дома, употреблении ими наркотиков, жестоком обращении с ними и совершенных ими нарушениях. Туда же вносятся сведения об их помещении в приюты, реабилитационные и профилактические центры, о лишении родительских прав, о коррекционных мероприятиях и оказанной социальной помощи, а также многое другое. При этом ГИС «Профилактика» интегрирована в общую государственную информационную архитектуру[132]. Это означает, что через ЕСИА система связывает свои учетные карточки со СНИЛС и тем самым интегрирует их с цифровыми профилями детей (как общими, так и профилями обучающихся в рамках ФГИС «Моя школа»).

Хотя в правительственном постановлении об этом прямо не говорится, сложно сомневаться в том, что среди прочих данных в ГИС «Профилактика» к учетным карточкам несовершеннолетних прикрепляются сведения, полученные в ходе интернет-слежки — будь то административный сталкинг классных руководителей, деятельность «кибердружин» или мониторинг федеральных ведомств. Внесение результатов этого надзора, вероятно,

---

[129] См., например: Агентство. «Крупнейший взлом российской цензуры: как она охраняет здоровье Путина, помогает Навке, заводит досье на журналистов и разводит ботов». *Издание «Агентство»* от 8 февраля 2023 года. https://www.agents.media/tsenzura/ (дата обращения: 10.08.2026).
[130] Малева Юлия и Татьяна Акиншина. «Минпросвещения разработает ГИС для профилактики детской преступности». *Издание «Ведомости»* от 4 сентября 2025 года.
[131] Постановление Правительства РФ от 01.04.2025 N 411 «О государственной информационной системе профилактики безнадзорности и правонарушений несовершеннолетних» https://www.consultant.ru/document/cons_doc_LAW_502345/ (дата обращения: 20.08.2026).
[132] Там же.

осуществляется по нескольким категориям, выделенным документом Правительства РФ, а именно: «*правонарушения*», «а*нтиобщественные действия*», а также в рамках размытой канцелярской формулировки «*обстоятельства, способствующие возможности комиссии по делам несовершеннолетних и защите их прав рассмотрения вопроса о проведении с несовершеннолетним индивидуальной профилактической работы*»[133]. Под последним пунктом, судя по всему, чиновники понимают любые юридические и фактические основания (сигналы школ, рапорты «кибердружинников», акты по итогам работы мониторинговых систем), которые власти на местах считают достаточными для инициирования проверки ребенка, включая лайки, репосты и просмотры сайтов «нежелательных организаций».

Видимо, именно развертыванию ГИС «Профилактика», а также повышению эффективности мониторинга Росмолодежи и служили упомянутые чуть выше административные меры властей Татарстана и Свердловской области. Это указывает на то, что описанные процессы — вовсе не отдельные инициативы, хотя пропагандистские медиа и чиновники пытаются преуменьшить или опровергнуть вовлечение школ в слежку за детьми. То, что все это — общефедеральный проект, подтверждает то же самое распоряжение Правительства РФ № 1030-р, которое не только закрепляет деятельность кибердружин, но также призывает активизировать слежку, контроль и пропаганду среди несовершеннолетних и молодых людей. Так, ряд предусмотренных документом шагов направлен на усиление координации этих действий между региональными администрациями и другими органами, включая МВД и Росгвардию. Пункт под номером 38 касается непосредственно мониторинга интернета: место проведения обозначено как «субъекты Российской Федерации», а исполнителем указана Росмолодежь. То есть именно то ведомство, для которого татарстанские школы и собирают данные аккаунтов учеников[134]. Все это демонстрирует, что развитие мониторинга Росмолодежи, административное выдавливание в школах у родителей сведений об аккаунтах и телефонных номерах детей, а также модернизация ГИС «Профилактика» — части единого проекта по централизации и усилению системы слежки за несовершеннолетними.

Пока нет очевидных признаков того, что на начало осени 2026 года на основе ГИС «Профилактика» работала полномасштабная предиктивная аналитика поведения несовершеннолетних. Но архитектура и функции системы указывают на то, что власти движутся именно в этом направлении, а какие-то модули, возможно, уже тестируются. Уже сейчас ГИС «Профилактика» — это не просто единая база учета, хранения и обмена информацией о детях, требующих особого внимания. Это также цифровой органайзер с функциями оценки, который сигнализирует чиновникам и сотрудникам соответствующих ведомств о необходимости тех или иных профилактических действий (например, проведения беседы или запуска программы реабилитации), оценивает эффективность проведенной работы, рекомендует присвоение того или иного юридического статуса ребенку и помогает в составлении индивидуальных планов для различных ситуаций. Все это пока находится на уровне сложной, но классической автоматизированной системы. Однако очевидно, что конечная цель властей заключается в развертывании масштабной предиктивной аналитики, включая рейтинги детей — как в отношении тех, на кого заведены учетные карточки в ГИС «Профилактика», так и в целом всех, у кого есть цифровые профили.

Все вышеперечисленное демонстрирует выход государственного мониторинга активностей несовершеннолетних в интернете на качественно новый уровень, превращающий его в единый механизм, интегрированный, в свою очередь, в архитектуру тотального контроля. Наверху этой вертикали находятся федеральные органы власти (МВД, ФСБ, Роскомнадзор,

---

[133] Там же.

[134] Распоряжение Правительства РФ от 30.04.2026 N 1030-р «Об утверждении комплекса мер по профилактике негативных социальных явлений в детской и молодежной среде на 2026–2030 годы» https://www.consultant.ru/document/cons_doc_LAW_533626/ (дата обращения: 17.08.2026).

Росмолодежь, Росгвардия), которые, с одной стороны, сами занимаются мониторингом, а с другой — принимают отчеты и жалобы от нижестоящих инстанций. Следом располагаются парагосударственные цензурирующие организации вроде ЛБИ, действующей на общероссийском уровне. Чуть ниже находятся региональные администрации и их подразделения, отвечающие за «работу» с детьми и молодежью. На самом низовом уровне в слежке участвуют студенты, учителя и сами старшеклассники.

Строящиеся вспомогательные периметры

Целенаправленная государственная слежка за несовершеннолетними не ограничивается перечисленными выше периметрами. Власти вводят дополнительные меры и изобретают новые методы. В кратком обзоре невозможно описать все из них, но следует упомянуть несколько основных инициатив.

Детские номера и контроль мобильной связи

С середины 2025 года чиновники активно разрабатывают, а летом 2026 года официально начали внедрять так называемые «детские сим-карты». Это нововведение является частью еще более масштабного плана по жесткому прикреплению человека к его мобильному устройству и абонентскому номеру. В последние годы власти предприняли несколько серьезных шагов, направленных на реализацию этого плана. Среди них:

- Ограничение числа сим-карт, доступных для регистрации на одного пользователя[135].
- Связь сим-карты и телефона между собой, а также с их владельцем, которому за редким исключением запрещается передавать их третьим лицам[136].
- Введение дополнительных требований к проверке данных при оформлении всех договоров на оказание услуг мобильной связи, включая фиксацию процесса заключения контракта на видео в точках продаж (эта норма начала действовать на практике с 1 сентября 2025 года)[137].
- Принуждение сотовых операторов немедленно блокировать попытки использования абонентского номера на другом устройстве[138].
- Создание до весны 2027 года единой базы IMEI — иначе говоря, реестра, отслеживающего, кто каким мобильным устройством владеет[139].

На фоне развития этого плана летом и осенью 2025 года, опять же, Минцифры, прикрываясь заботой о защите детей от мошенников и опасных сайтов, заявило о разработке «детской сим-карты»[140]. Надо отметить, что российские операторы и до этого предлагали детские тарифы с родительским контролем. Это признал даже руководитель аппарата Правительства РФ Дмитрий Григоренко, добавив, что чиновники хотят «*закрепить эту практику и сделать*

---

[135] См. статью 1 Федерального закона от 08.08.2024 N 303-ФЗ «О внесении изменений в Федеральный закон “О связи” и отдельные законодательные акты Российской Федерации» https://www.consultant.ru/document/cons_doc_LAW_482565/ (доступ: 28.08.2026).

[136] См. статью 9 Федерального закона от 01.04.2025 N 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» https://www.consultant.ru/document/cons_doc_LAW_502182/ (доступ: 28.08.2026).

[137] Постановление Правительства РФ от 30.12.2024 N 1994 «Об утверждении Правил оказания услуг телефонной связи и перечня организаций, имеющих право осуществлять подтверждение сведений об абоненте - физическом лице» https://www.consultant.ru/document/cons_doc_LAW_495347/ (дата обращения: 20.08.2026).

[138] Федеральный закон от 26.06.2026 N 210-ФЗ «О внесении изменений в Федеральный закон “О связи” и отдельные законодательные акты Российской Федерации» https://www.consultant.ru/document/cons_doc_LAW_537891/ (доступ: 03.08.2026).

[139] Там же.

[140] Любавина Анна. «Школьников предлагают пересадить на специальные SIM-карты». *Издание* «*CNews*» от 25 сентября 2025 года.

ее системной»[141]. Как продемонстрировало развитие инициативы, власти опять использовали риторику защиты интересов детей для усиления и централизации тотального контроля — то есть как раз для того, что эти самые интересы грубо нарушает.

На нормативном уровне «детская сим-карта» была введена тем же федеральным законом, который объявил о создании единой базы IMEI, со вступлением обоих положений в силу с 1 марта 2027 года[142]. Этим власти «позволили» родителям уведомлять сотового оператора о том, что абонентский номер использует несовершеннолетний. После получения этой информации оператор обязан внести номер в соответствующий регистр и активировать для него определенные правила. В самом законе они не прописаны — там лишь упомянуто, что их устанавливает Правительство РФ[143].

Примечательно, что первоначально власти планировали обязать родителей регистрировать абонентские номера своих детей под угрозой санкций. Однако затем — очевидно, из-за крайней сложности реализации такой схемы — объявили о ее «добровольном» характере. Этот шаг назад не должен вводить в заблуждение. Российские власти редко отказываются от репрессивных мер, а «добровольность» обычно означает задействование механизмов «скрытого принуждения». В случае слежки за детьми, как демонстрируют многие примеры, приведенные выше, в этом принуждении почти всегда задействуются школы. То, что события развиваются именно по такому сценарию, подтверждают и заявления чиновников. В частности, на старте дискуссии о «детских сим-картах» председатель комиссии Общественной палаты РФ по демографии, защите семьи, детей и традиционных семейных ценностей Сергей Рыбальченко заявил, что власти планируют организацию доступа детей к школьным сетям и цифровым сервисам именно через них[144]. Соответственно, высока вероятность того, что чиновники намерены лишить доступа к бесплатному интернету в учебных заведениях, а возможно, и к ФГИС «Моя школа» тех детей, родители которых не оформили такие номера. Иными словами, формальный отказ от обязательности введен лишь для подготовки соответствующей инфраструктуры и регламентации правил, функционирование которых в российской реальности почти никогда не опирается на декларируемую чиновниками «добровольность».

Насколько известно на текущий момент, согласно плану властей, сотовый оператор, узнав, что абонентским номером пользуется ребенок, обязан зафиксировать эту информацию в своих системах и сообщить об этом в государственную систему мониторинга Роскомнадзора (ГИС «КСИМ»[145]). Кроме того, судя по принятому закону и готовящимся мерам, сотовые операторы будут обязаны:

- жестко фильтровать контент;
- предлагать специализированные детские тарифы;
- непрерывно отслеживать физическое перемещение;
- запрещать использование роуминга и блокировать номер при его смене;

---

[141] Швецова Анна. «Цифровой щит для ребенка. Что скрывается за идеей специальных детских SIM-карт». *Издание «COMNEWS»* от 13 апреля 2026 года.
[142] См. статью 11 Федерального закона от 26.06.2026 N 210-ФЗ «О внесении изменений в Федеральный закон «О связи» и отдельные законодательные акты Российской Федерации» https://www.consultant.ru/document/cons_doc_LAW_537891/ (дата обращения: 03.08.2026).
[143] См. статью 1 там же.
[144] Любавина Анна. «Школьников предлагают пересадить на специальные SIM-карты». *Издание* «*CNews*» от 25 сентября 2025 года.
[145] Постановление Правительства РФ от 18.03.2025 N 318 «О государственной информационной системе мониторинга исполнения операторами связи обязанностей при оказании услуг связи» https://www.consultant.ru/document/cons_doc_LAW_501497/ (дата обращения: 25.08.2026).

- допускать использование только тех соцсетей и мессенджеров, которые одобрены чиновниками («ВКонтакте», платформа «Сферум» и мессенджер «Макс»);
- блокировать звонки и сообщения с иностранных номеров, а также любые неавторизованные SMS-рассылки[146].

На практике это означает, что «детская сим-карта» не позволит зарегистрировать или обновить аккаунт в независимых мессенджерах и приложениях, требующих авторизации по SMS[147]. Хотя чиновники отрицают такое развитие ситуации, существует высокая вероятность, что власти планируют в обозримом будущем свести разрешенный контент к так называемому «белому списку» сайтов — аналогичному тому, который Минпросвещения уже закрепило (на основании общефедерального списка) для школьного интернета[148]. Родителям же оставят лишь возможность менять некоторые второстепенные настройки.

Отслеживание передвижения

Помимо фильтрации контента и углубленного мониторинга сетевой активности, власти планируют использовать «детские сим-карты» для пристального физического отслеживания несовершеннолетних, о чем объявляется открыто. Хотя это вновь преподносится чиновниками как услуга родителям и забота о безопасности детей, на самом деле весь смысл инициативы заключается в организации массовой и систематической государственной слежки за местонахождением и маршрутами перемещения детей вне школ. Опять же, на рынке уже давно распространены приложения, умные часы и отдельные устройства, которые выполняют эту функцию для родителей. Но проблема для чиновников была в том, что эти данные не были полностью интегрированы с государственными системами. Примечательно, что подобные технологии геотрекинга с 2025 года проходят тестирование на мигрантах, прибывающих в безвизовом режиме на длительный срок в Москву и Московскую область[149]. Очевидно, что следующая огромная группа, чьи физические передвижения и маршруты власти намерены взять под жесткий контроль, — это подростки.

Это не значит, что российские власти не демонстрируют интерес к слежке за передвижениями всего подконтрольного населения. Наоборот, именно этим, судя по всему, объясняется то, что они обязали сотовых операторов до 2027 года начать предоставлять полные данные геотрекинга всех своих клиентов в так называемое «озеро данных» (ЕИП НСУД)[150]. Но поскольку абонентский номер может купить один человек, а пользоваться им — другой, для массовой персонализированной слежки властям крайне важно знать, кто именно использует устройство. Для этого чиновники утвердили упомянутые выше общие меры, закрепляющие мобильные устройства и номера за конкретными людьми, а также приняли

---

[146] Проект Постановления Правительства РФ «О внесении изменений в постановление Правительства Российской Федерации от 30 декабря 2024 г. N 1994» (по состоянию на 06.07.2026) (подготовлен Минцифры России, ID проекта 02/07/07-26/00169086) https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PNPA&n=124111 (дата обращения: 25.08.2026).

[147] The Insider. «Минцифры предложило запретить детям получать SMS-рассылки. Операторы беспокоятся, что это может перекрыть им доступ к мессенджерам». *Издание «The Insider»* от 7 августа 2026 года. https://theins.ru/news/295794 (дата обращения: 25.08.2026).

[148] Официальное сообщение Минпросвещения России от 14.11.2025 «О разрешенном перечне интернет-ресурсов для использования в образовательном процессе» https://www.consultant.ru/document/cons_doc_LAW_518910/ (Доступ: 25.08.2026).

[149] Троицкий Константин. *Государственный информационный ресурс «Цифровой профиль иностранного гражданина» и формирование нового российского тоталитаризма.* Центр защиты прав человека «Мемориал», 2026. https://memorialcenter.org/uploads/Kopiya_Konstantin_Troiczkij_O_czifrovom_profile_inostrannogo_grazhdanin3_6_9157de992b.pdf (дата обращения: 03.08.2026).

[150] Любавина Анна. «На развитие российской системы управления данными выделят почти шесть миллиардов». *Издание «CNews»* от 7 марта 2025 года.

дополнительные — в отношении отдельных крупных групп, за которыми российские государственные органы следят с особым интересом: мигрантов и подростков.

«Эмпатичные» чат-боты и аналитика души

Еще одним масштабным и высокотехнологичным направлением установления тотального контроля над несовершеннолетними является внедрение чат-ботов на базе ИИ. При определенных настройках они служат крайне эффективным инструментом как для индоктринации и ведения предиктивной аналитики, так и для слежки. В мае 2026 года стало известно, что Росмолодежь разрабатывает чат-бот, который, согласно техническому описанию, должен обеспечивать «*устойчивую, персонализированную и эмпатичную поддержку*» подросткам и молодежи.[151] В отличие от других чат-ботов, которые уже используются на государственных учебных ресурсах, этот сервис должен поддерживать диалог на широкий спектр тем с фокусом на проблемах, тревогах и душевном состоянии старших школьников и студентов, стараясь тем самым просканировать и затем отслеживать самые сокровенные мысли и переживания[152].

Росмолодежь собирается внедрить этот чат-бот в мессенджер «Макс»[153], в который, как указывалось выше, интегрирован «Сферум», являющийся, в свою очередь, частью ФГИС «Моя школа». Как также говорилось, регистрация в «Сферуме» требует прохождения системы идентификации на Портале «Госуслуги»; это предполагает запись (логирование) системой чат-бота информации о том, с кем, когда и о чем шел разговор, привязывая данные к конкретному цифровому профилю пользователя. Если система заработает, то эти сведения будут доступны не только администраторам Росмолодежи, но и другим ведомствам-участникам проекта, а также силовикам (МВД, ФСБ, Следственному комитету и прокуратуре).

Поскольку спецификация также устанавливает, что «*система должна обеспечивать централизованное хранение, возможности для мониторинга и контроля обработки обращений*», а по итогам беседы будет проводиться анализ «*актуальных запросов, тематических трендов и поведенческих паттернов*»[154], становится очевидным: в чат-ботах Росмолодежи задействуют технологии предиктивной аналитики. Иными словами, власти намереваются использовать данные для составления рейтингов, прогнозирования рисков и обучения государственных нейросетей, что наряду со слежкой, судя по всему, и являлось изначально основной целью всего проекта.

Следует также отметить, что внедрением и управлением чат-ботами в структуре Росмолодежи занимается ЦИСМ — структура, уже активно вовлеченная в мониторинг сетей, о чем упоминалось в предыдущем разделе. Не секрет, что ЦИСМ имеет соглашения со многими силовыми ведомствами и тесно координирует свою деятельность с МВД, включая информирование о детях и молодежи, публикующих контент, который власти относят к «запрещенному» или «деструктивному»[155]. Чуть менее известно, что эта же структура нанимает в свои ряды хакеров, о чем стало известно после их кибератак на гражданскую

---

[151] Малева Юлия. «Молодежь планируют нравственно обогащать через чат-боты». *Издание «Ведомости»* от 12 мая 2026 года.
[152] Там же.
[153] Там же.
[154] Там же.
[155] Привин Максим. «Большой брат с функцией доноса. Как созданный Кремлем Центр изучения молодежи помогает возбуждать дела за комментарии в сети». *Vot-tak.tv* от 12 марта 2026 года. https://vot-tak.tv/92037582/cism-monitoring-molodezhi (дата обращения: 20.08.2026).

информационную инфраструктуру стран Европейского союза, Украины и США (транспорт, больницы, налоговые ведомства, суды, банки). Координацией этих атак, как установило следствие, занимались непосредственно генеральный директор ЦИСМ Максим Лупин и его заместитель Михаил Бурлаков, из-за чего они были объявлены Европолом в розыск[156].

Нельзя упускать из вида и тот факт, что параллельно с проведением тендера на запуск «эмпатичного» чат-бота Росмолодежь заявила о намерении «помочь» регионам в борьбе с «деструктивным контентом» в интернете[157]. Вызывает мало сомнений, что эти направления связаны, а сама система чат-бота задумана как элемент глобальной сети слежки, пропаганды, индоктринации и предиктивной аналитики, развернутой в рамках репрессивной госсистемы.

Центральный пост управления

Символом государственных мер по централизации и интеграции учебных платформ и мониторинга школ на данный момент стал официальный запуск Рособрнадзором с 1 июня 2026 года так называемой «Единой цифровой системы мониторинга образования». Эта система задумана для синхронизированного и централизованного отслеживания около 800 показателей в области образования, собираемых из различных ведомств и баз данных[158]. Перед тем как попасть на экран чиновника, ежедневная успеваемость и поведение школьников обрабатываются алгоритмами и автоматически превращаются в коэффициенты, которые встраиваются в графики на основе формул этой машины жесткого вертикального контроля. Вне зависимости от того, превратится ли текущая платформа в реальный управленческий инструмент, как это обещают чиновники, либо канет в небытие из-за технических недоработок, эта инициатива ясно демонстрирует усилия властей по созданию единой тотальной экосистемы. Ее вершиной становится небольшой виртуальный центр управления, в который стекаются все основные показатели. Речь идет о попытке установления надзора, знакомого разве что по наиболее мрачным дистопиям, в которых несколько анонимных фигур через нажатие кнопок на свое усмотрение, а порой просто из каприза меняют судьбы миллионов детей и взрослых.

---

[156] Затирко Андрей. «Раскрытая Евроюстом хакерская группировка оказалась связана с IT-структурой, созданной Путиным». *Издание «Агентство»* от 17 июля 2025 года. https://www.agents.media/raskrytaya-evroyustom-hakerskaya-gruppirovka-okazalas-svyazana-s-it-strukturoj-sozdannoj-putinym/ (дата обращения: 20.08.2026).

[157] Денисенко Антон. «Росмолодежь поможет регионам в борьбе с деструктивным контентом». *Издание «CNews»* от 6 мая 2026 года.

[158] Коммерсантъ. «В России заработала единая цифровая система мониторинга образования» *Издание «Коммерсантъ»* от 1 июня 2026 года.

Заключение

На наших глазах происходит радикальная перестройка российских школ и превращение образовательное среды в инструмент цифрового паноптикума нового типа. Еще 10–15 лет назад такие системы, как аналоговые видеокамеры, мониторинг школьного интернета и электронные дневники, обычно не были связаны друг с другом, имели разные форматы и ограничивались школой. Если кто-то и пытался связать эти системы в единое цело, то это был классный руководитель, но делал это со свойственными человеку особенностями, гоняясь за парой десятков своих учеников. Это было крайне далеко от «совершенных» методов обработки больших данных, но оставляло много места для человеческого и персонального подхода. Такое положение вещей не устраивало центральные власти, которые решили качественно перестроить систему сбора и обработки данных, сделав ее единой, тотальной и вертикальной.

Власти не просто внедрили новые технологии и системы, но кардинально изменили их архитектуру. В центре теперь находится цифровой профиль ребенка, в рамках которого не только интегрируются неведомые доселе массивы данных, но и производится их коррекция, оценка и аналитика. Классный руководитель из того, кто знал о ребенке больше всех, превратился в низшее звено цепочки слежки. Ему теперь отводится роль лишь одного из источников данных, и его фигура с развитием новых систем оценок, учебных ресурсов, онлайн-занятий и видеонаблюдения имеет все меньшее значение во все более цифровой и тотальной архитектуре управления.

Цифровые профили школьников ведутся в ФГИС «Моя школа», а также связываются с ГИС «Профилактика», если власти считают, что ребенку необходимо особое внимание. Эти две системы — не изолированные статичные реестры (одна для школьников, а другая — для неблагополучных семей, беспризорных, девиантных подростков и детей, находящихся в трудной жизненной ситуации), а два динамичных элемента единой цифровой архитектуры госуправления, включающей также нейросети, программы аналитики, инструменты мониторинга, сотни информационных платформ, тысячи баз данных и бесчисленные приложения. Построение этой единой архитектуры позволяет государственному аппарату вести и постоянно усложнять цифровое профилирование детей. Целью этого является развертывание поведенческого анализа, социального скоринга, автоматического назначения поощрений и наказаний, алгоритмического управления, а в конечном счете — воспитание и образование полностью прогнозируемого, контролируемого и послушного населения.

Как далеко российские власти от построения этой дистопии? Сложно сказать, но следует избегать как переоценки, так и недооценки. С одной стороны, есть школы, в которых интернет функционирует номинально, ФГИС «Моя школа» заполняется завучами вручную и нерегулярно, а камеры видеонаблюдения остаются аналоговыми и работают без записи. Но с другой стороны, есть тысячи учебных заведений, в которых ситуация обратная и уже внедрена предиктивная аналитика. В свете этого доклада очевидно, что формирование нового российского тоталитаризма, в котором полицейские дубинки дополняются нейронными сетями, идет быстро. Коррупция, дефицит кадров, плохая инфраструктура, межведомственная конкуренция, санкции и перебои с мобильным интернетом замедляют это движение, но не останавливают и тем более не обращают вспять. Чтобы убедиться в этом, достаточно посмотреть на развитие НСУД, судьбу платформы «ГосТех» либо просто оценить последние возможности и функции ФГИС «Моя школа» и ГИС «Профилактика», а потом осознать, что еще в конце 2010-х годов все это существовало лишь в планах их разработчиков.

Построение системы тотальной слежки за детьми ведется не только через стремительное внедрение высокотехнологичных платформ, но и через реформу управления. Информационные системы Минпросвещения отданы под контроль Минцифры — главного цифрового цензора страны. Повседневное видеонаблюдение в школах уже не ограничивается администрацией учебного заведения и даже вышестоящими органами образования. Потоки видеоданных через региональные хранилища попадают в полный доступ Росгвардии, МВД и ФСБ, превращая тем самым образовательные организации в режимные объекты под прямым контролем силовиков. Весь трафик школьных сетей процеживается через инфраструктуры основного технического разработчика и оператора госсистем слежки — «Ростелекома» — и главного интернет-надсмотрщика — Роскомнадзора. Но и это еще не все. Региональные власти, Росмолодежь и МВД, реализуя указания Кремля, используют школы для масштабного идеологического сыска, организуя «охоту» за подростками в интернете. К процессу привлекают как учителей, обязанных выискивать «деструктивный контент» в соцсетях учащихся, так и самих школьников, которых понуждают вступать в «кибердружины» и заниматься кибердоносительством на своих сверстников. Информационная «добыча» по результатам такой «охоты» (то есть данные о том, что власти расценивают как нарушения) стекается в единую межведомственную платформу ГИС «Профилактика», в которой решающую роль опять играют структуры МВД, ставшие тем самым главными российскими «воспитателями».

В заключение доклада хотелось бы подчеркнуть, что исследование систем массовой слежки за детьми позволяет осознать острую необходимость в радикальной альтернативе, базирующейся на принципах ненасилия, честности и уважения к человеческому достоинству.

Процитированные источники

Библиография

Агентство. «Крупнейший взлом российской цензуры: как она охраняет здоровье Путина, помогает Навке, заводит досье на журналистов и разводит ботов». *Издание «Агентство»* от 8 февраля 2023 года. https://www.agents.media/tsenzura/ (дата обращения: 10.08.2026).

Азаттык Азия. «В России запретили использовать телефоны на уроках в школе». *Радио «Свобода»* от 31 августа 2022 года. https://www.azattyqasia.org/a/32012530.html (Дата обращения: 19.08.2026).

Александров Алексей. «В России начали широко рекламировать мессенджер Max. В чем его опасность и способен ли он стать аналогом китайского WeChat?». *Настоящее время* от 14 июля 2025 года. https://www.currenttime.tv/a/v-rossii-nachali-shiroko-reklamirovat-messendzher-max-v-chem-ego-opasnost-i-sposoben-li-on-stat-analogom-kitayskogo-wechat-/33472932.html (дата обращения: 23.08.2026).

Аркман Арден. *Методичь. Как государственная пропаганда захватила российское образование — от детских садов до вузов*. Издание The Insider от 10 октября 2025 года. https://theins.ru/obshestvo/284870 (дата обращения: 20.08.2026).

Бахур Владимир. «Эксперты: национальная система управления данными должна фокусироваться на пользе для бизнеса и граждан». *Издание «CNews»* от 29 ноября 2018 года.

Беларуская асацыяцыя журналістаў. «7 способов, которыми российский мессенджер Max следит за пользователями». *Беларуская асацыяцыя журналістаў* от 7 октября 2025 года, https://baj.media/be/karysnae/max-sledit-za-polzovateljami/ (дата обращения: 24.04.2026).

Воронов Александр и Алексей Жабин. «Детские лица сканируют для взрослых схем. В правительстве РФ рассказали, как может заработать биометрия в школах». *Издание «Коммерсантъ»* от 3 декабря 2025 года.

Галиева Диана. «Госданные приглашают на платформу». *Издание «Коммерсантъ»* от 4 мая 2021 года

Гаспарян Тат. «В дагестанских школах появится Wi-Fi и умное видеонаблюдение до конца 2025 года». *Издание «Коммерсантъ»* от 3 июня 2025 года

Денисенко Антон. «Росмолодежь поможет регионам в борьбе с деструктивным контентом». *Издание «CNews»* от 6 мая 2026 года.

Дорошенко Дарья. «В школах Сургута установили умные камеры с функцией распознавания лиц». *Югорский снегирь* от 21 августа 2025 года.

Ефремов Геннадий. «Некоторым россиянам хотят полностью запретить пользоваться сотовыми телефонами и смартфонами. Кого коснется». *Издание* «*CNews*» от 25 марта 2026 года.

Затирко Андрей. «Раскрытая Евроюстом хакерская группировка оказалась связана с IT-структурой, созданной Путиным». *Издание «Агентство»* от 17 июля 2025 года. https://www.agents.media/raskrytaya-evroyustom-hakerskaya-gruppirovka-okazalas-svyazana-s-it-strukturoj-sozdannoj-putinym/ (дата обращения: 20.08.2026).

Захаров Андрей. «“Умный город” или “Старший брат”? Как мэрия научилась знать о москвичах всё». *BBC News Русская служба* от 10 апреля 2020 года. https://www.bbc.com/russian/features-52219260 (дата обращения: 17.09.2026).

Издание «Мел». «Губернатору Белгородской области пожаловались, что учителей заставляют мониторить соцсети школьников и заполнять по ним отчеты». *Издание «Мел»* от 22 марта 2026 года

Кармак Булат. «В Москве появится крупнейший в России кампус “Школы 21” В СберСити». *Издание «Ferra»* от 17 июля 2025 года.

Касми Эльяс. «Власти собираются объединить все данные граждан и бизнеса в огромное электронное досье». *Издание «CNews»* от 30 ноября 2018 года.

Касми Эльяс. «Искусственный интеллект начинает контролировать поведение детей. Эксперимент поставят на российских школьниках». *Издание* «*CNews*» от 1 июня 2021 года.

Кинякина Екатерина. «Умные камеры будут следить за российскими школьниками. Системой видеонаблюдения с функцией распознавания лиц оснастят все 43 000 школ». *Издание* «*Ведомости*» от 15 июня 2020 года.

Коломыченко Мария. «В России появится школьный реестр запрещенных сайтов». *Издание «CNews»* от 17 апреля 2014 года.

Коммерсантъ. «Госданные приглашают на платформу». *Издание «Коммерсантъ»* от 4 мая 2021 года.

Коммерсантъ. «В России заработала единая цифровая система мониторинга образования» *Издание «Коммерсантъ»* от 1 июня 2026 года.

Королев Игорь. «“Ростелеком” получит от властей 10 миллиардов на постройку интернета без Facebook, “Вконтакте” и танчиков». *Издание* «*CNews*» от 3 августа 2020 года.

Королев Никита и др. «Контрольная по биометрии». *Издание «Коммерсантъ»* от 7 сентября 2021 года.

Краснушкина Надежда. «Госданным прописали архитектуру». *Издание* «*Коммерсантъ*» от 30 ноября 2018 года.

Кустов Максим. «В свердловских школах планируют внедрить ИИ для выявления девиантных подростков». *Издание «Сигнал»* от 9 апреля 2026 года.

Литаврин Максим и Давид Френкель. «Нейроскомнадзор. Чем пользуется РКН, чтобы следить за интернетом — и кто ему в этом помогает». Медиазона от 8 февраля 2023 года, https://zona.media/article/2023/02/08/grccc (дата обращения: 10.08.2026).

Литой Александр. «“Большой брат” от звонка до звонка. Как следят за соцсетями школьников». *Радио* «*Свобода*» *от 22 декабря 2019 года.* https://www.svoboda.org/a/30338558.html (дата обращения: 17.08.2026).

Литой Александр. «Государство пришло в чат. Контроль над учителями, родителями и детьми». *Радио* «*Свобода*» от 30 ноября 2023 года. https://www.svoboda.org/a/gosudarstvo-prishlo-v-chat-kontrolj-nad-uchitelyami-roditelyami-i-detjmi/32426381.html (дата обращения: 17.08.2026).

Луговская Елизавета. «За вашими детьми следят. Кто и зачем просит учителей мониторить соцсети учеников». *Издание «Мел»* от 28 апреля 2021 года.

Лукьянова Ирина. «Закон о хорошем поведении. Как и зачем депутаты опять отнимают у школьников телефоны». *Новая газета* от 7 ноября 2023 года.

Любавина Анна. «На развитие российской системы управления данными выделят почти шесть миллиардов». *Издание «CNews»* от 7 марта 2025 года.

Любавина Анна. Счетная палата: Выделенные на школьный интернет деньги потрачены неэффективно. Учителя говорят, что пользоваться сетью невозможно. *Издание «CNews»* от 26 июня 2025 года

Любавина Анна. «Школьников предлагают пересадить на специальные SIM-карты». *CNews* от 25 сентября 2025 года.

Малева Юлия. «Молодежь планируют нравственно обогащать через чат-боты». *Издание «Ведомости»* от 12 мая 2026 года.

Малева Юлия и Татьяна Акиншина. «Минпросвещения разработает ГИС для профилактики детской преступности». *Издание «Ведомости»* от 4 сентября 2025 года.

Мальгина Анна. «“Господин Никто против Путина”: как школьный педагог из Карабаша снял фильм, потрясший Запад. Интервью “Вот Так” с Павлом Таланкиным». *vot-tak.tv* от 3

июня 2025 года. https://vot-tak.tv/87052526/interviu-s-pavlom-talankinym (дата обращения: 20.08.2026).

Медиазона. «Ростех: устанавливаемые в школах камеры не предполагают технологию распознавания лиц». *Медиазона* от 16 июня 2020 года. https://zona.media/news/2020/06/16/technology (дата обращения: 20.08.2026).

Медуза. «Полиция по всей России покупает системы мониторинга соцсетей. Они помогают искать экстремизм “не выходя из рабочего кабинета”». *Медуза* от 16 октября 2018 года. https://meduza.io/feature/2018/10/16/politsiya-po-vsey-rossii-pokupaet-sistemy-monitoringa-sotssetey-oni-pomogayut-iskat-ekstremizm-ne-vyhodya-iz-rabochego-kabineta (Доступ: 15.05.2026).

Медуза. «VK перешел под контроль Газпромбанка и “Согаза” друга Путина Юрия Ковальчука. Гендиректором VK станет сын Сергея Кириенко». *Медуза* от 3 декабря 2021 года. https://meduza.io/feature/2021/12/03/vk-pereshel-pod-kontrol-gazprombanka-i-sogaza-druga-putina-yuriya-kovalchuka-gendirektorom-vk-stanet-syn-sergeya-kirienko (дата обращения: 19.08.2026).

Медуза. «“Они могут начать противодействовать”. Российские власти боятся детей, насильно вывезенных из Украины. Их пытаются «перевоспитать» и поставить под жесткий цифровой контроль». *Медуза* от 11 марта 2024 года https://meduza.io/feature/2024/03/11/oni-mogut-nachat-protivodeystvovat (дата обращения: 20.08.2026).

Медуза. «“Мы просто физически не успеваем вести свои обычные уроки”. Как изменилось школьное образование в России за годы войны?» *Медуза,* 8 сентября 2025 года, https://meduza.io/feature/2025/09/08/my-prosto-fizicheski-ne-uspevaem-vesti-svoi-obychnye-uroki (дата обращения: 18.08.2026).

Медуза. «Все иностранцы в России очень скоро окажутся под плотным контролем властей — на каждого человека составят максимально подробное досье». *Издание «Медуза»* от 28 января 2026 года https://meduza.io/cards/vse-inostrantsy-v-rossii-ochen-skoro-okazhutsya-pod-plotnym-kontrolem-vlastey-na-kazhdogo-cheloveka-sostavyat-maksimalno-podrobnoe-dosie (Доступ: 04.09.2026).

Медуза. «Вы наверняка слышали, что “Макс” шпионит за пользователями. Но вряд ли представляете, сколько разных инструментов для слежки внедрено в мессенджер Возможно, разработчики даже использовали нейросеть для прослушки». *Медуза* от 22 мая 2026 года. https://meduza.io/feature/2026/05/22/vy-uzhe-navernyaka-slyshali-chto-maks-shpionit-za-svoimi-polzovatelyami-no-vryad-li-predstavlyaete-skolko-raznyh-instrumentov-dlya-slezhki-vnedreno-v-etot-messendzher (дата обращения: 22.05.2026).

Митрухин Сергей. «Видеокамеры в школах Новосибирска научатся распознавать драки и буллинг и отличать их от детских игра». *Сибирский новостной* от 27 августа 2025 года.

Михальченко Елизавета и Ксения Миронова. «Школа хочет все знать о семье. В цифровую образовательную среду могут быть включены персональные данные учеников, учителей и родителей». Издание «Коммерсантъ» от 19 июня 2019 года.

Новая газета Европа. «Свердловские власти начали мониторить соцсети школьников на предмет “запрещенного” контента». *Новая газета Европа* от 11 марта 2026 года. https://novayagazeta.eu/articles/2026/03/11/sverdlovskie-vlasti-nachali-monitorit-sotsseti-shkolnikov-na-predmet-zapreshchennogo-kontenta-news (дата обращения: 19.08.2026)

Новые известия. «“Это - не слежка”: в школах Екатеринбурга впервые в России установили прослушку». *Новые известия* от 7 апреля 2022 года.

ОВД-инфо. *Как власти используют камеры и распознавание лиц против протестующих*. ОВД-инфо от 17 января 2022 года. https://reports.ovd.info/kak-vlasti-ispolzuyut-kamery-i-raspoznavanie-lic-protiv-protestuyushchih (дата обращения: 19.08.2026).

ОВД-инфо. *«Либо государственное мнение, либо никакого»: как преследуют преподавателей, которым вменили антивоенную позицию.* ОВД-инфо от 1 сентября 2024 года. https://reports.ovd.info/teachers (дата обращения: 17.08.2026).

Петрова Венера и Олег Сапожков. «“Гостех”, раз-два». *Издание “Коммерсантъ”* от 22.09.2025.

Петрова Полина. «В школах Петербурга могут начать следить за поведением учеников с помощью искусственного интеллекта». *Петербургская газета* от 19 марта 2026 года.

Позычанюк Валерия. «Операция “Детские ладошки”. Зачем “Сбер” собирает биометрические данные школьников». *The Bell* от 7 октября 2020 года. https://thebell.io/operatsiya-detskie-ladoshki-zachem-sber-sobiraet-biometricheskie-dannye-shkolnikov (дата обращения: 09.09.2026).

Привин Максим. «Большой брат с функцией доноса. Как созданный Кремлем Центр изучения молодежи помогает возбуждать дела за комментарии в сети». *Vot-tak.tv* от 12 марта 2026 года. https://vot-tak.tv/92037582/cism-monitoring-molodezhi (дата обращения: 20.08.2026).

Роскомсвобода. Регионы заводят себе кибердружины. *Роскомсвобода* от 9 октября 2019 года. https://roskomsvoboda.org/ru/50250/ (дата обращения: 27.08.2026).

Роскомсвобода. «Распознавание лиц внедрили в более чем 60 регионах России». *Роскомсвобода* от 24 октября 2023 года. https://roskomsvoboda.org/ru/post/syst-raspozn-62-region/ (дата обращения: 20.08.2026).

Савицкая Людмила. «Срочно удали лайк, иначе утром подают в полицию». *Радио «Свобода»* от 28 января 2021 года. https://www.svoboda.org/a/31074785.html (дата обращения: 26.05.2026).

Самсонова Анастасия. «“Ростелеком” укрепился в “Безопасном городе”». *Издание «COMNEWS* от 6 июня 2019 года.

Сизова Ника. «“Гостех 2.0” будет работать на решениях провайдера облачных технологий Cloud.ru». *Издание «Ведомости»* от 18 мая 2026 года.

Степанова Юлия и Анастасия Гаврилюк. «Школьникам соберут портфолио. Российских учеников снабдят цифровым профилем». *Издание «Коммерсантъ»* от 8 июня 2021 года.

Стрельников Алексей. «Мессенджер-шпион Max? Как россияне переходят на “максофоны”». *Deutsche Welle* от 23 марта 2026 года. https://www.dw.com/ru/max-messendzerspion-pocemu-rossiane-perehodat-na-maksofony/a-76494140 (дата обращения: 23.04.2026).

Троицкий Константин. *Государственный информационный ресурс «Цифровой профиль иностранного гражданина» и формирование нового российского тоталитаризма.* Центр защиты прав человека «Мемориал», 2026. https://memorialcenter.org/uploads/Kopiya_Konstantin_Troiczkij_O_czifrovom_profile_inostrannogo_grazhdanin3_6_9157de992b.pdf (дата обращения: 03.08.2026).

Троицкий Константин. Тестирование детей-иностранных граждан на знание русского языка: нарушение права на образование, слежка и российская репрессивная миграционная политика. Центр защиты прав человека «Мемориал», 2026. https://memorialcenter.org/ru/analytics/narushenie-prava-na-obrazovanie-dlya-detej-inostrannyh-grazhdan (дата обращения: 18.08.2026).

Учительская Россия. «Школы Новосибирска планируют оснастить камерами с ИИ для профилактики агрессивного поведения». *Учительская Россия* от 29 августа 2024 года.

Холупова Кристина. «В московских школах установят тысячи видеокамер за миллиарды рублей». *Издание «CNews»* от 21 августа 2021 года.

Центр «Досье». «Глаза Кремля. Как устроен цифровой ГУЛАГ в России — и что мешает ему заработать в полную силу». *Центр «Досье»* от 11 марта 2024 года, https://dossier.center/sorm/ (дата обращения: 15.05.2026).
Швецова Анна. «Цифровой щит для ребенка. Что скрывается за идеей специальных детских SIM-карт». *Издание «COMNEWS»* от 13 апреля 2026 года.

Amnesty International. *"Только официальные источники": Индоктринация в российском системе образования*. Amnesty International от 1 июня 2026 года.
Alava Jonna. “From Patriotic Education to Militarist Indoctrination—Disciplinary Power and Silent Resistance in Russia after the Onset of the War against Ukraine”. *Problems of Post-Communism* 72, no. 5 (2025): 429–440.
Bernard Andreas. *Komplizen des Erkennungsdienstes. Das Selbst in der digitalen Kultur*. Frankfurt am Main: S. Fischer Verlag GmbH, 2017.
CNews. «“Ростелеком” подключил к безопасному интернету более 47 тысяч школ и техникумов». *Издание «CNews»* от 28 февраля 2023 года.
CNews. «Минцифры: приложением “Госуслуги Моя школа” пользуются более 12 млн человек». *Издание «CNews»* от 1 сентября 2026 года.
Colin Alexander. “Mr. Nobody Against Putin gives an insight into the propaganda in Russian schools”. The Conversation, July 3, 2025 https://theconversation.com/mr-nobody-against-putin-gives-an-insight-into-the-propaganda-in-russian-schools-260162 (дата обращения: 26.11.2025).
Daucé Françoise, Benjamin Loveluck, Bella Ostromooukhova, and Anna Zaytseva. “From Citizen Investigators to Cyber Patrols: Volunteer Internet Regulation in Russia”. *Laboratorium: Russian Review of Social Research* 11 (3) (2020): 46–70.
Dietrich Philipp. 2023. *The Key Player in Russia’s Cybersphere. What the West Needs to Know about VK Company*. German Council on Foreign Relations, September 20, 2023. https://dgap.org/en/research/publications/key-player-russias-cybersphere (дата обращения: 18.08.2026).
D-Russia. «Подписано соглашение об использовании решений “Московской электронной школы” при развитии ФГИС “Моя школа”». *Издание «D-Russia»* от 2 сентября 2022 года.
D-Russia. «Счётная палата: 44,6% школ и колледжей считают недостаточной скорость Интернета для обучения». *Издание «D-Russia»* от 26 июня 2025 года.
D-Russia. «Сервис для школ “Сферум” стал доступен из Max». *Издание «D-Russia»* от 9 октября 2025 года.
Enders Anna, Lea Horne, and Marla Rivera. *The Max Messenger: An Analysis of Russia’s State-Mandated Messaging Application*. InterSecLab, September 2026.
Goldenfein Jake. *Monitoring Laws. Profiling and Identity in the World State*. Cambridge, Cambridge University Press, 2020.
HRW. «Россия: Школьников и студентов преследуют после протестов». *Human Rights Watch* от 23 июня 2017 года. https://www.hrw.org/ru/news/2017/06/23/russia-children-students-targeted-after-protests (дата обращения: 17.08.2026).
HRW. *Education under Occupation. Forced Russification of the School System in Occupied Ukrainian Territories*. Human Rights Watch, June 2024. https://www.hrw.org/sites/default/files/media_2024/06/ukraine_crd0624%20web_0.pdf (дата обращения: 24.08.2026).
Радио Свобода. «“Насилие не остановить ни мониторингом, ни запретом соцсетей”. О попытках властей усилить контроль за школьниками в интернете». *Радио «Свобода»* от 17 февраля 2026 года. https://www.svoboda.org/a/nasilie-ne-ostanovit-ni-monitoringom-ni-zapretom-sotssetey-o-p

opytkah-vlastey-usilit-kontrol-za-shkolnikami-v-internete/33680397.html (дата обращения: 27.05.2026).
Kelly Catriona. *Children's World: Growing Up in Russia, 1890-1991*. New Haven: Yale University Press, 2007.
Leo XIV, Pope. 2026. *Magnifica humanitas: On Safeguarding the Human Person in the Time of Artificial Intelligence* (Encyclical Letter). May 15, 2026. The Holy See. https://www.vatican.va/content/leo-xiv/en/encyclicals/documents/20260515-magnifica-humanitas.html (дата обраения: 28.09.2026).
Lyon David. *Surveillance*. Oxford: Oxford University Press, 2024.
Marx Gary. *Windows into the Soul. Surveillance and Society in an Age of High Technology*. The University of Chicago Press, 2016.
Ottinger, Lily. "China's AI Education Experiment". *ChinaTalk*, April 3, 2026, https://www.chinatalk.media/p/chinas-ai-education-experiment (дата обращения: 06.08.2026).
Poupin Perrine. "Social media and state repression: The case of VKontakte and the anti-garbage protest in Shies, in Far Northern Russia?. *First Monday*, 26 (5) (2021). https://firstmonday.org/ojs/index.php/fm/article/view/11711/11233 (дата обращения: 18.08.2026).
Shi, Chen and Jianhua Xu. "Surveillance Cameras and Resistance: A Case Study of a Middle School in China". *The British Journal of Criminology*, Vol. 64, No. 5 (2024): 1150–1170.
The Insider. «Минцифры предложило запретить детям получать SMS-рассылки. Операторы беспокоятся, что это может перекрыть им доступ к мессенджерам». *Издание «The Insider»* от 7 августа 2026 года. https://theins.ru/news/295794 (дата обращения: 25.08.2026).
Yale School of Public Health. *Forced Passportization on Russia-Occupied Areas of Ukraine*. New Haven, Humanitarian Research Lab at Yale School of Public Health, August 2, 2023. https://files-profile.medicine.yale.edu/documents/891469c2-690f-4229-8ffc-35b1c3743744 (дата обращения: 24.08.2026).

Документы государственных органов и муниципальных образований

Аналитический центр при Правительстве РФ. «Национальная система управления данными. Концепция». Проект от 25.11.2018 года, версия 5.14. https://digital.msu.ru/wp-content/uploads/%D0%9D%D0%A1%D0%A3%D0%94.-%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D0%B8%D1%8F_%D0%B28_25112018.pdf (Доступ: 20.04.2026).
Инструкция по работе с Универсальной библиотекой цифрового образовательного контента (УБ ЦОК). *Портал myschool.eduprosvet.ru* (дата обращения: 14.08.2026).
Министерство просвещения РФ / Министерство цифрового развития, связи и массовых коммуникаций РФ. (2026). Памятка: Типовое облачное решение (ТОР) «Моя школа» [Внутренний регламент федерального ИТ-внедрения]. Размещено на официальном сервере Управления образования КУГО. https://obr-ku.ru/images/Documents/TOR/%D0%A2%D0%9E%D0%A0_%D0%9C%D0%BE%D1%8F_%D1%88%D0%BA%D0%BE%D0%BB%D0%B0_%D0%9F%D0%B0%D0%BC%D1%8F%D1%82%D0%BA%D0%B0.pdf (дата обращения: 12.09.2026).
Министерство просвещения РФ / Министерство цифрового развития, связи и массовых коммуникаций РФ. (2026). Функциональные возможности ТОР. Школа // Краткое описание ФГИС «Моя школа» ТОР. Образование для субъектов РФ. Размещено на официальном сервере Правительства Смоленской области.

https://obrpoch.admin-smolensk.ru/files/561/tor_kratko_av.pdf (дата обращения: 12.09.2026).

Официальное сообщение Минпросвещения России от 14.11.2025 «О разрешенном перечне интернет-ресурсов для использования в образовательном процессе» https://www.consultant.ru/document/cons_doc_LAW_518910/ (Доступ: 25.08.2026).

Письмо Федерального агентства по делам молодежи от 27.02.2025 N ГГ/1449-06 «О направлении методических рекомендаций» https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=871483 (дата обращения: 11.09.2026).

Постановление муниципальной комиссии по делам несовершеннолетних и защите их прав в городе Нефтеюганске от 17.03.2022 года №11 "Об обеспечении информационной безопасности несовершеннолетних на территории города Нефтеюганска" https://www.admugansk.ru/uploads/2023/02/%E2%84%96_11_ot_17.03.2022.doc (дата обращения: 16.09.2026).

Проект Постановления Правительства РФ «О внесении изменений в постановление Правительства Российской Федерации от 30 декабря 2024 г. N 1994» (по состоянию на 06.07.2026) (подготовлен Минцифры России, ID проекта 02/07/07-26/00169086) https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PNPA&n=124111 (дата обращения: 25.08.2026).

Постановление Главного государственного санитарного врача РФ от 28.09.2020 N 28 «Об утверждении санитарных правил СП 2.4.3648-20 “Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи”» (вместе с «СП 2.4.3648-20. Санитарные правила...») https://www.consultant.ru/document/cons_doc_LAW_371594/a87d3709aa01857b67d2d04477b1d8458572e62e/ (Дата обращения: 17.08.2026).

Постановление Правительства Белгородской области от 22 мая 2017 года № 181-пп «Об организации деятельности кибердружин Белгородской области».

Постановление Правительства Москвы от 07.02.2012 N 24-ПП «Об утверждении Положения о государственной информационной системе “Единый центр хранения и обработки данных».

Постановление Правительства Республики Бурятия от 12 июля 2019 года N 378 «Об утверждении Порядка взаимодействия с кибердружинами в Республике Бурятия».

Постановление Правительства Новгородской области от 23 сентября 2024 года N 457 «Об утверждении Регламента деятельности кибердружин в Новгородской области».

Постановление Правительства РФ от 24.11.2014 N 1240 «О некоторых вопросах по обеспечению использования сети передачи данных органов власти» https://www.consultant.ru/document/cons_doc_LAW_171430/ (дата обращения: 12.08.2026).

Постановление Правительства РФ от 03.06.2019 N 710 «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» (первоначальная редакция) https://ivo.garant.ru/#/document/77695224/paragraph/33:2 (Доступ: 17.09.2026).

Постановление Правительства РФ от 03.06.2019 N 710 «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» (редакция от 17.11.2025) https://ivo.garant.ru/#/document/72262102/paragraph/9093:5 (Доступ: 17.09.2026).

Постановление Правительства РФ от 02.08.2019 N 1006 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов

(территорий)»https://www.consultant.ru/document/cons_doc_LAW_331342/ (дата обращения: 30.07.2026).
Постановление Правительства РФ от 14.05.2021 N 733 «Об утверждении Положения о федеральной государственной информационной системе “Единая информационная платформа национальной системы управления данными” и о внесении изменений в некоторые акты Правительства Российской Федерации» https://www.consultant.ru/document/cons_doc_LAW_384215/ (дата обращения: 14.08.2026).
Постановление Правительства РФ от 13.07.2022 N 1241 «О федеральной государственной информационной системе “Моя школа”» https://www.consultant.ru/document/cons_doc_LAW_422207/ (дата обращения: 06.08.2026).
Постановление Правительства РФ от 30.12.2024 N 1994 «Об утверждении Правил оказания услуг телефонной связи и перечня организаций, имеющих право осуществлять подтверждение сведений об абоненте - физическом лице» https://www.consultant.ru/document/cons_doc_LAW_495347/ (дата обращения: 20.08.2026).
Постановление Правительства РФ от 18.03.2025 N 318 «О государственной информационной системе мониторинга исполнения операторами связи обязанностей при оказании услуг связи» https://www.consultant.ru/document/cons_doc_LAW_501497/ (дата обращения: 25.08.2026).
Постановление Правительства РФ от 01.04.2025 N 411 «О государственной информационной системе профилактики безнадзорности и правонарушений несовершеннолетних» https://www.consultant.ru/document/cons_doc_LAW_502345/ (дата обращения: 20.08.2026).
Постановление Правительства РФ от 01.08.2026 N 962 «О внесении изменений в постановление Правительства Российской Федерации от 13 июля 2022 г. N 1241» https://www.consultant.ru/document/cons_doc_LAW_541441/ (дата обращения: 12.09.2026).
Приказ ГБОУ «Основная общеобразовательная школа» № 21 города Новокуйбышевска Самарской области № 104-ОД от 19.08.2022 http://nov21ooh.minobr63.ru/wp-content/uploads/2023/11/prikaz-ob-utverzhdenii-kiberdruzhiny-bullinг.pdf (дата обращения: 18.08.2026).
Приказ Директора ГБОУ РД «РЦО» № 109 от 30.08.2021 «Положение о системе видеонаблюдения».
Приказ Директора ГБОУ «СОШ № 4 г. Сунжа им. А.М. Калиматова» № 220/5 от 01.09.2022 «Положение о системе видеонаблюдения».
Приказ Директора МБОУ «Ковжинская средняя общеобразовательная школа» № 166 от 26.12.2023 «Положение о системе видеонаблюдения».
Приказ Директора МБОУ «СОШ № 4 г. Тосно от от 02.09.2024 № 450 «Положение о системе видеонаблюдения».
Приказ Комитета образования и науки Курской области от 20 мая 2021 года N 1-552 «Об организации в образовательных организациях Курской области мониторинга аккаунтов обучающихся в социальных сетях».
Приказ МБОУ «Лицей № 1» п. Добринка Липецкая область от 1 сентября 2025 года № 386 https://lic1dobrinka.gosuslugi.ru/netcat_files/196/2998/Prikaz_o_monitoringe_sotsial_nyh_stey_obuchayuschihsya.pdf (дата обращения: 19.08.2026).
Приказ Минпросвещения России от 02.12.2019 N 649 «Об утверждении Целевой модели цифровой образовательной среды» (Зарегистрировано в Минюсте России 24.12.2019 N 56962) https://www.consultant.ru/document/cons_doc_LAW_341443/ad8f4e028380894173b4f017a56c42b4c5e4ad54/#dst100011 (дата обращения: 13.08.2026).

Приказ Минпросвещения России от 30.06.2021 N 396 «О создании федеральной государственной информационной системы Минпросвещения России “Моя школа”» https://www.consultant.ru/document/cons_doc_LAW_395336/ (дата обращения: 10.08.2026).

Приказ Минцифры России N 417, Минпросвещения России N 221 от 30.04.2021 «Об утверждении требований к подключению и доступу, включая требования к передаче данных, государственных и муниципальных образовательных организаций, реализующих программы общего и среднего профессионального образования, избирательных комиссий субъектов Российской Федерации и территориальных избирательных комиссий к единой сети передачи данных». https://www.consultant.ru/document/cons_doc_LAW_388367/2ff7a8c72de3994f30496a0ccbb1ddafdaddf518/ (дата обращения: 26.08.2026).

Приказ Минпросвещения России N 634, Минцифры России N 925 от 08.09.2021 «Об утверждении стандарта оснащения государственных и муниципальных общеобразовательных организаций, осуществляющих образовательную деятельность в субъектах Российской Федерации, на территории которых проводится эксперимент по внедрению цифровой образовательной среды, компьютерным, мультимедийным, презентационным оборудованием и программным обеспечением».

Приказ Минпросвещения России N 232, Рособрнадзора N 551 от 04.04.2023 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам основного общего образования» https://www.consultant.ru/document/cons_doc_LAW_447000/ (дата обращения: 24.08.2026).

Приказ Минпросвещения России N 233, Рособрнадзора N 552 от 04.04.2023 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего общего образования» https://www.consultant.ru/document/cons_doc_LAW_447215/ (дата обращения: 24.08.2026).

Приказ Минтруда России от 03.04.2023 N 256н «Об утверждении Инструкции о порядке ведения индивидуального (персонифицированного) учета сведений о зарегистрированных лицах» https://www.consultant.ru/document/cons_doc_LAW_447676/ (дата обращения: 21.08.2026).

Приказ МОБУ «Средняя общеобразовательная школа № 23» от 01.09.2023 № 458 «О создании и деятельности кибердружины МОБУ СОШ № 23 в 2023-2024 учебном году». https://taganschool23.ru/2023-2024/Kiberdrujina/prikaz_o_sozdanii_kiberdruzhiny.pdf (дата обращения: 17.08.2026).

Приказ МОБУ «Средняя общеобразовательная школа № 23» города Таганрог от 01.09.2023 № 458 «О создании и деятельности кибердружины МОБУ СОШ № 23 в 2023-2024 учебном году» https://taganschool23.ru/2023-2024/Kiberdrujina/prikaz_o_sozdanii_kiberdruzhiny.pdf (дата обращения: 17.08.2026).

Приказ МОУ «Средняя школа № 25 Кировского района Волгограда» № 75 от 23 апреля 2025 года «О создании и функционировании Кибердружины"» https://sosh25-vlg2012.ucoz.ru/food2/prikaz_o_sozdanii_kiberdruzhiny.pdf (дата обращения: 18.08.2026).

Приказ Управления образованием администрации Ивантеевского муниципального района Саратовской области от 10 ноября 2022 года N 211 «О проведении мониторинга социальных сетей несовершеннолетних» https://uoivanteevka.ucoz.ru/sport/prikaz_o_prov_mon_socset_22.pdf (дата обращения: 19.08.2026).

Приказ Управления образованием Тавдинского городского округа Свердловской области от 19 февраля 2024 года N 109 «Об утверждении Порядка проведения мониторинга аккаунтов социальных сетей несовершеннолетних в образовательных организациях в новой редакции».

Распоряжение Департамента информационных технологий г. Москвы от 31.07.2015 N 64-16-241/15 «Об утверждении регламента доступа пользователей к информации, содержащейся в государственной информационной системе “Единый центр хранения и обработки данных”, регламента передачи информации об объектах видеонаблюдения в государственную информационную систему “Единый центр хранения и обработки данных” из внешних систем видеонаблюдения, регламента передачи в государственную информационную систему “Единый центр хранения и обработки данных” информации об объектах видеонаблюдения на основании заключенных Департаментом информационных технологий города Москвы государственных контрактов».

Распоряжение Минпросвещения России от 17.12.2019 N Р-135 «Об утверждении методических рекомендаций по приобретению средств обучения и воспитания для обновления материально-технической базы общеобразовательных организаций и профессиональных образовательных организаций в целях внедрения целевой модели цифровой образовательной среды в рамках региональных проектов, обеспечивающих достижение целей, показателей и результата федерального проекта “Цифровая образовательная среда” национального проекта “Образование”» https://www.consultant.ru/document/cons_doc_LAW_340889/ (дата обращения: 21.08.2026).

Распоряжение Правительства РФ от 21.11.2019 N 2757-р «Об определении публичного акционерного общества “Ростелеком” единственным исполнителем осуществляемых Минкомсвязью России в 2019–2020 годах для государственных и муниципальных образовательных организаций, реализующих программы общего и среднего профессионального образования, избирательных комиссий субъектов Российской Федерации и территориальных избирательных комиссий закупок услуг».

Распоряжение Правительства РФ от 22.03.2021 N 713-р «Об определении публичного акционерного общества “Ростелеком” единственным исполнителем осуществляемых в 2021–2022 годах закупок товаров (работ, услуг), необходимых для осуществления мероприятий, связанных с формированием устойчивой информационно-коммуникационной инфраструктуры государственных и муниципальных общеобразовательных организаций».

Распоряжение Правительства РФ от 30.04.2026 N 1030-р «Об утверждении комплекса мер по профилактике негативных социальных явлений в детской и молодежной среде на 2026–2030 годы» https://www.consultant.ru/document/cons_doc_LAW_533626/ (дата обращения: 17.08.2026).

Федеральное агентство по делам молодежи. *Методические рекомендации по профилактике распространения идеологии терроризма, экстремизма и неонацизма* [утв. письмом Росмолодежи от 27.02.2025 № ГГ/1449-06]. 2025.

Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 N 436-ФЗ https://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 12.08.2026).

Федеральный закон от 01.04.2019 N 48-ФЗ «О внесении изменений в Федеральный закон “Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования” и отдельные законодательные акты Российской Федерации» https://www.consultant.ru/document/cons_doc_LAW_321413/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100031 (дата обращения: 22.08.2026).

Федеральный закон «О внесении изменений в Федеральный закон “Об образовании в Российской Федерации”» от 19.12.2023 N 618-ФЗ https://www.consultant.ru/document/cons_doc_LAW_464808/ (Дата обращения: 17.08.2026).

Федеральный закон от 08.08.2024 N 303-ФЗ «О внесении изменений в Федеральный закон “О связи” и отдельные законодательные акты Российской Федерации» https://www.consultant.ru/document/cons_doc_LAW_482565/ (доступ: 28.08.2026).

Федеральный закон от 01.04.2025 N 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» https://www.consultant.ru/document/cons_doc_LAW_502182/ (доступ: 28.08.2026).

Федеральный закон от 26.06.2026 N 210-ФЗ «О внесении изменений в Федеральный закон “О связи” и отдельные законодательные акты Российской Федерации» https://www.consultant.ru/document/cons_doc_LAW_537891/ (дата обращения: 03.08.2026).