

**ВСЕРОССИЙСКИЙ ТИМИРЯЗЕВСКИЙ КОНКУРС НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ,
ОПЫТНО-КОНСТРУКТОРСКИХ, ТЕХНОЛОГИЧЕСКИХ И СОЦИАЛЬНЫХ ПРОЕКТОВ
МОЛОДЕЖИ В СФЕРЕ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА**

«АПК – МОЛОДЕЖЬ, НАУКА, ИННОВАЦИИ»

Направление: Технологии воспитания и обучения

Тема: «Цифровые права несовершеннолетних: внесение поправок в законодательство о защите персональных данных и информационной безопасности»

Соискатель: Примова Виктория Максимовна, студентка «ФГБОУ ВО Омский ГАУ» группы Б-11ЮР

Научный руководитель: Старший преподаватель Бальтанова Гульмира Жумабековна

Место выполнения работы: «ФГБОУ ВО Омский ГАУ»

Аннотация

Работа представляет собой комплексное исследование, направленное на выявление системных пробелов в российском законодательстве, регулирующем защиту цифровых прав несовершеннолетних, и разработку конкретных законодательных инициатив для их устранения.

Что сделано: Проведен многоаспектный анализ действующего правового поля, включая Федеральный закон № 152-ФЗ «О персональных данных», отраслевое законодательство и recent changes 2024-2025 гг. Исследована правоприменительная практика Роскомнадзора и судов, проанализированы статистические данные об утечках данных и киберрисках для детей. Рассмотрены международные стандарты (GDPR, COPPA, рекомендации Совета Европы) и доктринальные подходы.

Что нового получено: Выявлена ключевая проблема – законодательная «слепота» к возрастной специфике субъекта данных, приводящая к формальному применению норм о родительском согласии и реальной незащищенности детей в цифровой среде. Установлено, что ужесточение штрафов, хотя и необходимо, не решает проблем превенции и построения этичной цифровой экосистемы.

Научная новизна заключается в разработке концепции **прогрессивной цифровой дееспособности несовершеннолетнего**, воплощенной в пакете конкретных поправок. Предлагается не просто ужесточить режим, а создать гибкую, соответствующую возрасту модель правовой защиты. Основные предложения:

1. Введение в ФЗ-152 специальной статьи, определяющей персональные данные несовершеннолетнего как объект повышенной охраны.
2. Создание **трехуровневой модели информированного согласия** с элементами совместного волеизъявления ребенка (с 10 и с 14 лет) и родителя.
3. Введение **административной и уголовной ответственности с квалифицирующим признаком «в отношении несовершеннолетнего»**.
4. Закрепление императивной обязанности **«защиты по умолчанию» (Privacy & Safety by Default)** для всех сервисов, потенциально используемых детьми.
5. Предложение о создании **государственного реестра «детских» цифровых сервисов**, прошедших аудит безопасности.

Практическая значимость: Работа представляет собой готовый инструментарий для законодателей, регулятора (Роскомнадзор) и правоприменителей. Разработанные формулировки статей, таблицы сравнительного анализа и модели согласий могут быть непосредственно использованы в нормотворческом процессе, что способствует построению в России безопасного и развивающего цифрового пространства для детей.

Содержание

Введение.....	4
Глава 1 Теоретико-правовые и социологические основания цифровых прав несовершеннолетних..	5
1.1. Генезис понятия «цифровые права».....	5
1.2. Структурный анализ цифровых прав несовершеннолетнего.....	7
1.3. Специфика правового статуса.....	9
1.4. Научные подходы	10
Глава 2. Критический анализ действующего законодательства РФ и правоприменительной практики.....	11
2.1. ФЗ-152: Анализ неадекватности.....	11
2.2. Родительское согласие: миф и реальность.....	12
2.3. Отраслевая специфика	13
Глава 3. Эмпирический срез: ключевые риски, статистика и оценка последних изменений (2024-2025 гг.).....	15
3.1. Картирование угроз.....	15
3.2. «Цифровой двойник».....	16
Глава 4. Концепция реформы и проекты конкретных законодательных поправок.....	19
4.1. Философия изменений.....	19
4.2. Блок поправок №1: Специализация ФЗ-152.....	19
4.3. Блок поправок №2: Инновационный механизм согласия.....	19
4.4. Блок поправок №3: Ответственность.....	19
4.5. Блок поправок №4: Безопасный дизайн.....	19
4.6. Прогноз последствий.....	20
Заключение.....	21
Библиографический список.....	22
Приложение.....	23

Введение

Актуальность. Цифровая среда перестала быть альтернативной реальностью для современного ребенка – она стала основным пространством социализации, обучения, творчества и коммуникации. Однако эта новая «цифровая экология» порождает беспрецедентные по масштабу и изощренности угрозы: от тотальной коммерческой слежки, формирующей цифровое досье с младенчества, до психологического насилия в киберпространстве. Российское законодательство, сконструированное в эпоху зарождения интернета, демонстрирует системный кризис адекватности. Оно упорно пытается вписать цифрового ребенка в прокрустово ложе традиционных гражданско-правовых конструкций недееспособности, игнорируя его фактическую автономию и уязвимость. Актуальность исследования обусловлена нарастающим разрывом между динамикой цифровых угроз и статичностью правовых защитных механизмов, что ставит под удар фундаментальные права и психологическое благополучие целого поколения.

Степень научной разработанности. Проблематика исследуется на стыке информационного, гражданского, семейного и ювенального права. Значительный вклад внесли отечественные ученые: Т.Н. Балашова (концепция цифровых прав), О.Л. Подустова (анализ рисков), А.А. Чурочкина (международные стандарты). Однако большинство работ носят констатирующий или описательный характер. Зарубежная доктрина (ЕС, США) ушла дальше в практических решениях – от СОРРА до «детского» дизайна GDPR (ст. 8), что требует критического осмысления и адаптации.

Объект исследования – комплекс общественных отношений, возникающих при обработке персональных данных несовершеннолетних, обеспечении их информационной безопасности и реализации их прав в цифровой среде на территории РФ.

Предмет исследования – нормы российского и международного права, регулирующие указанные отношения, правоприменительная практика судов и Роскомнадзора, данные социологических и криминологических исследований, а также доктринальные источники.

Цель исследования – разработать научно обоснованную и технически детализированную систему поправок в законодательство РФ, направленную на создание эффективного, сбалансированного и age-appropriate механизма защиты цифровых прав несовершеннолетних.

Задачи:

- Сформулировать и структурировать понятие «цифровые права несовершеннолетнего».
- Провести критический анализ действующих норм ФЗ-152, КоАП, УК РФ и выявить системные коллизии.
- Исследовать и классифицировать современные цифровые риски для детей на основе эмпирических данных.
- Дать оценку последним законодательным изменениям 2024-2025 гг.
- Разработать концепцию «прогрессивной цифровой дееспособности».
- Подготовить проекты конкретных поправок в законодательные акты с подробной аргументацией.

Методологическая основа: В работе использованы общенаучные (анализ, синтез, системный подход, моделирование) и частнонаучные методы: формально-юридический, сравнительно-правовой, историко-правовой, метод правового прогнозирования, анализ статистических данных.

Эмпирическая база: Материалы судебной практики (КАС, уголовные дела), отчеты Роскомнадзора и Лиги безопасного интернета, данные всероссийских социологических исследований (ВЦИОМ, ФОМ) по цифровой грамотности, аналитические отчеты компаний в сфере кибербезопасности (Positive Technologies, Group-IB).

Практическая значимость: Результаты работы могут быть использованы:

- Государственной Думой РФ и Советом Федерации для совершенствования законодательства.
- Роскомнадзором для разработки методических рекомендаций и приоритетов надзора.
- Министерством просвещения и Министерством цифрового развития для формирования государственной политики.
- IT-компаниями при разработке и доработке продуктов для детей.
- В учебном процессе юридических и педагогических вузов.

Глава 1. Теоретико-правовые и социологические основания цифровых прав несовершеннолетних

1.1. Генезис понятия «цифровые права»

Цифровые права (Digital Rights) не являются абсолютно инновационным правовым конструктом. По своей сути, они представляют собой естественную и закономерную проекцию классических, универсальных прав человека в цифровую среду, которая стала новой сферой существования, коммуникации и самореализации личности. Генезис этого понятия отражает динамичную адаптацию правовых рамок к технологическим революциям и сопутствующим им социальным вызовам. Его эволюцию можно проследить в несколько ключевых этапов, каждый со своим фокусом и доминирующей повесткой.

Этап 1: 1990-е – начало 2000-х: Право на доступ и «цифровой разрыв» (Digital Divide)

На заре массового распространения интернета центральной темой стало **право на доступ** к информационно-коммуникационным технологиям (ИКТ). Основной проблемой виделся «цифровой разрыв» – неравенство в возможностях использования цифровых благ между разными регионами, социально-экономическими группами, поколениями. Дискуссии вращались вокруг интернета как инструмента развития, образования и социальной инклюзии. Права в цифровой сфере понимались, прежде всего, как производные от социально-экономических прав.

Этап 2: 2000-е – 2010-е: Свобода выражения, информации и нейтралитет сети

С ростом проникновения интернета фокус сместился на **гражданские и политические права** в онлайн-среде. На первый план вышли:

- **Свобода выражения и мнения** (борьба с цензурой, блокировками).
- **Свобода информации и доступа к знаниям** (движение за открытый доступ, открытые данные).
- **Право на приватность**, однако в этот период оно часто уступало по актуальности вопросам открытости.
- **Принцип нейтральности сети (Net Neutrality)** как гарантия равных условий для распространения любого легального контента и сервисов.

Интернет воспринимался как глобальное публичное пространство, требующее особых, либеральных регуляторных подходов для защиты демократических ценностей.

Этап 3: 2010-е – 2020-е: Защита автономии, приватности и цифрового достоинства

Скандалы вокруг массовой слежки (Snowden, 2013) и манипуляций данными (Cambridge Analytica, 2018), а также доминирование платформенных гигантов привели к **кардинальному сдвигу парадигмы**. Основными векторами стали:

- **Защита персональных данных и приватности** как основа цифровой автономии личности. Внедрение жестких регуляторных стандартов (таких как GDPR в ЕС, 2018).
- **Цифровая безопасность** (безопасность коммуникаций, защита от киберпреступлений, государственного и корпоративного надзора).
- **Право на цифровое достоинство**, защита от онлайн-насилия, кибербуллинга, дискриминационных алгоритмов.
- **Право на алгоритмическую прозрачность и справедливость** – осознание власти алгоритмов, принимающих решения, влияющие на жизнь людей.

Повестка сместилась от «свободы от» вмешательства государства к «защите от» цифровых угроз как со стороны государств, так и со стороны частных корпораций.

Специфика цифровых прав ребенка: триада «Безопасность – Развитие – Участие»

Для несовершеннолетних пользователей эта общая эволюция трансформируется в уникальную триаду принципов, отраженную в современном международном праве:

1. **Безопасность:** Защита от вредоносного контента, эксплуатации, буллинга, груминга и иных цифровых рисков.
2. **Развитие:** Обеспечение доступа к образовательным, творческим ресурсам, создание условий для позитивной социализации и реализации потенциала в цифровой среде.
3. **Участие (Партисипация):** Признание права ребенка на выражение своего мнения в цифровых вопросах, его касающихся, и на участие в цифровом обществе. Это выводит ребенка из пассивной роли объекта защиты в активного субъекта цифрового мира.

Закрепление в международном праве: от рекомендаций к обязательствам

Международное право последовательно фиксирует эту эволюцию, придавая ей нормативный вес:

- **Рекомендация Комитета Министров Совета Европы CM/Rec(2018)7** «О руководящих принципах уважения, защиты и осуществления прав ребенка в цифровой среде» стала одним из первых комплексных документов, систематизирующих подход, основанный на триаде «безопасность-развитие-участие».
- **Замечание общего порядка №25 (2021) Комитета ООН по правам ребенка** «О правах детей в отношении цифровой среды» – это исторический документ, который прямо интегрирует цифровую среду в контекст Конвенции о правах ребенка. Он авторитетно подтверждает, что все права ребенка должны быть защищены и реализованы онлайн, и возлагает на государства-участники **прямую обязанность адаптировать законодательные, политические и образовательные меры** для обеспечения цифровых прав детей.

Таким образом, генезис понятия «цифровые права» – это путь от понимания интернета как инструмента к признанию его полноценной средой обитания человека, где действуют, но и требуют новой, специфической защиты все фундаментальные права и свободы. Современный этап характеризуется переходом от деклараций к конкретным юридическим и технологическим механизмам их имплементации, с особым акцентом на уязвимые группы, к которым, безусловно, относятся дети.

1.2. Структурный анализ цифровых прав несовершеннолетнего

Структурный анализ цифровых прав ребенка позволяет перейти от общих принципов к конкретным правомочиям и корреспондирующим им обязанностям государства, бизнеса и общества. Эти права образуют взаимосвязанную систему, где защита одних создает основу для реализации других.

1. Право на защиту персональных данных (ПДн) и цифровую приватность

Данное право для несовершеннолетнего носит **усиленный (преференциальный) характер** в силу возрастной психофизиологической незрелости, неспособности в полной мере (fully) осознать долгосрочные последствия распространения своей цифровой информации.

- **Расширенное понимание «персональных данных»:** Речь идет не только о классических данных (ФИО, адрес, фото), но и о более сложных категориях:
 - **Цифровой след и поведенческий профиль:** Данные о поисковых запросах, времени онлайн, предпочтениях в контенте, которые агрегируются для создания психологического портрета и таргетированного воздействия.
 - **Геолокация в реальном времени:** Информация о местоположении, создающая риски для физической безопасности.
 - **Биометрические данные:** Отпечатки пальцев, сканы лица, используемые для аутентификации.

- **Конфиденциальность коммуникаций:** Переписка в мессенджерах, личные переговоры по видеосвязи.
- **Обязанности операторов и «родительский контроль»:** Это право порождает обязанность платформ применять принцип **privacy by default** (конфиденциальность по умолчанию) для детских аккаунтов, минимизировать сбор данных, использовать прозрачные и понятные формулировки в пользовательских соглашениях. Роль родителей и педагогов трансформируется в роль **навигаторов и посредников**, помогающих ребенку осознать ценность и риски цифровой приватности.

2. Право на информационную безопасность и защиту от цифрового насилия

Это **позитивная обязанность государства и интернет-провайдеров** проактивно создавать безопасную цифровую среду, а не только реагировать на инциденты. Ключевые угрозы:

- **Кибербуллинг (травля в сети):** Это не «обычная детская жесткость», а качественно иное явление, характеризующееся:
 - **Публичностью и масштабом:** Аудитория травли потенциально неограниченна.
 - **Перманентностью:** Компрометирующие материалы могут сохраняться в сети бесконечно.
 - **Отсутствием «безопасного пространства»:** Травля проникает в дом, преследуя жертву круглосуточно.
 - **Анонимностью или ощущением безнаказанности агрессора**, что усиливает его поведение.
- **Иные формы насилия:** Груминг (установление доверительных отношений с ребенком для последующей эксплуатации), киберсталкинг (преследование), распространение материалов сексуального характера с участием несовершеннолетних (CSAM).
- **Инструменты защиты:** Законодательное закрепление ответственности за кибербуллинг, создание низкопороговых служб помощи и горячих линий, обязательная и эффективная система модерации и быстрого реагирования на платформах, образовательные программы по цифровой гигиене.

3. Право на цифровое развитие и доступ к качественному контенту

Это право выходит за рамки простого **доступа к информации** (преодоление digital divide) и акцентирует **качество и развивающий потенциал** цифровой среды:

- **Возрастная адекватность и культурная чувствительность:** Контент должен соответствовать этапу когнитивного и эмоционального развития ребенка.
- **Развитие «гибких навыков» (soft skills):** Позитивная цифровая среда должна способствовать развитию критического мышления, медиаграмотности, креативности, навыкам коллаборации, а не только потреблению развлекательного контента.
- **Образовательный потенциал:** Доступ к онлайн-курсам, электронным библиотекам, симуляторам и развивающим играм, которые дополняют и обогащают формальное образование.
- **Создание собственного контента:** Право не только потреблять, но и создавать — вести блоги, монтировать видео, заниматься цифровым творчеством в защищенной и поддерживающей среде.

4. Право на цифровое забвение (право на удаление информации)

Для несовершеннолетнего это право должно толковаться максимально широко, приближаясь к **абсолютному**. Его философская основа — **право на ошибку и возможность личного роста без «цифрового клейма»**.

- **Принцип:** Информация, размещенная ребенком или о ребенке в неосознанном возрасте (неудачные фото, агрессивные или глупые посты, компрометирующие видео), не должна бесконечно определять его цифровую репутацию и преследовать во взрослой жизни, например, при приеме на работу, поступлении в вуз или установлении личных отношений.
- **Механизмы реализации:** Облегченная процедура подачи запросов на удаление данных как к платформам, так и к поисковым системам. В правовых системах, подобных GDPR (Общий регла-

мент по защите данных ЕС), это право закреплено, и для детей его реализация должна быть приоритетной и упрощенной. Это также включает **право родителей или законных представителей** выступать с таким требованием от имени ребенка.

Синтез: Взаимосвязь прав

Эти права образуют единую экосистему: *защита ПДн и безопасность* создают безопасное пространство для *развития*. *Право на забвение* является корректирующим механизмом, исправляющим потенциальный вред, нанесенный в процессе реализации права на участие и самовыражение. Таким образом, структурный анализ подчеркивает необходимость не разрозненных мер, а целостной государственной и общественной политики, охватывающей все элементы этой системы.

1.3. Специфика правового статуса

Правовой статус несовершеннолетнего в цифровом пространстве характеризуется глубоким **внутренним противоречием (правовым парадоксом)**, что создает зону повышенного риска и уязвимости. Этот парадокс можно обозначить как конфликт между его **формально-юридической недееспособностью** и **фактически признаваемой полноценностью в качестве цифрового актора**.

Ребенок как «пользователь-инвестор»: экономическая модель вовлечения

Ребенок в сети — это не просто пассивный потребитель контента. Это **активный пользователь-инвестор**, который вкладывает в цифровую платформу ключевые ресурсы:

- **Персональные данные:** Формируют основу для таргетированной рекламы и развития бизнес-модели данных (data-driven economy).
- **Внимание и время:** Являются прямыми метриками вовлеченности (engagement), которые монетизируются через рекламные показы и определяют рыночную стоимость платформы.
- **Социальный капитал и контент:** Создаваемый и распространяемый ребенком контент, его лайки, репосты и связи усиливают сетевые эффекты и ценность всей экосистемы.

Взамен он получает *услугу доступа* к социальным взаимодействиям, развлечениям, информации. Однако эта сделка изначально неэквивалентна.

Парадокс «недееспособного контрагента»: дисбаланс в заключении «договора»

Формально, согласно **Гражданскому кодексу РФ (ст. 28)**, малолетние (до 14 лет) и несовершеннолетние (14-18 лет) лица обладают ограниченной дееспособностью. Крупные сделки, многие юридически значимые действия требуют согласия или одобрения законных представителей (родителей, опекунов).

Однако в цифровой среде этот принцип систематически игнорируется:

- **Юридическая фикция «информированного согласия»:** Доступ к услуге обусловлен принятием **пользовательского соглашения (Terms of Service)**. Это самый сложный юридический документ объемом в десятки страниц, написанный малопонятным языком. Его принимает 12-летний пользователь одним кликом («Я согласен»), что не может рассматриваться как действительное, осознанное волеизъявление.
- **Фактическое признание дееспособности:** Платформы, зная возраст пользователя (или преднамеренно не уточняя его), вступают с ним в фактические правоотношения, **обрабатывая его данные, формируя персонифицированную ленту, заключая сделку по отчуждению его внимания рекламодателям**. Рынок де-факто признает ребенка полностью дееспособным и ценным потребителем, в то время как де-юре он таковым не является.

Правовые последствия и «регуляторный вакуум»

Этот парадокс порождает серьезные правовые проблемы:

- **Недействительность согласия на обработку ПДн:** С точки зрения закона (например, GDPR в ЕС или ФЗ-152 «О персональных данных» в РФ), согласие, данное ребенком без ведома родителей, может быть признано недействительным. Это создает колоссальные риски для самих платформ.
- **Отсутствие действенных механизмов родительского контроля и согласия:** Существующие механизмы (родительский аккаунт, запрос согласия) часто носят формальный, легко обходимый характер и не обеспечивают реального участия законных представителей в цифровой жизни ребенка.
- **Сдвиг ответственности:** Бремя ответственности за последствия «несправедливого договора» (утечка данных, цифровая зависимость, вред от контента) ложится на ребенка и его семью, в то время как платформа, создавшая асимметричные условия, часто уходит от ответственности.

Специфика правового статуса заключается в **гибридной позиции ребенка**: он является экономически полноценным, но юридически ущербным субъектом цифровых отношений. Разрешение этого парадокса требует либо создания специальных **цифровых процедур эмансипации** (упрощенные, интуитивно понятные договоры, реальные механизмы подтвержденного родительского согласия), либо пересмотра подходов к ответственности платформ, которые должны нести повышенные обязательства при взаимодействии с несовершеннолетними пользователями. Ключевой вектор — приведение фактического положения ребенка в соответствие с юридическими гарантиями его защиты

1.4. Научные подходы

Подход	Суть	Критика	Представители
Протекционистский	Полный родительский контроль до 18 лет. Запреты, ограничения, родительский софт.	Игнорирует evolving capacities, приводит к конфликтам, не учит ответственности, techno-illiterate родители не могут обеспечить контроль.	Консервативные родительские ассоциации.
Либерально-эмансипационный	Признание цифровой дееспособности с раннего возраста (напр., с 13 лет – полная).	Игнорирует реальные психологические риски и манипулятивный потенциал платформ.	Часть IT-либертарианцев, некоторые правозащитники.
Сбалансированный	Постепенное расширение прав и ответственности по мере взросления + обязанность государства и бизнеса создавать безопасность.	Сложность правовой техники, необходимость тонкой возрастной градации.	Позиция автора. Совет Европы, современная европейская доктрина.

Глава 2. Критический анализ действующего законодательства РФ и правоприменительной практики

2.1. ФЗ-152: Анализ неадекватности.

Федеральный закон №152-ФЗ, являясь краеугольным камнем защиты приватности в России, демонстрирует **системную неадекватность при применении к цифровой среде несовершеннолетних**. Его базовые принципы, будучи универсальными, размываются и теряют эффективность перед лицом специфики детского онлайн-поведения и бизнес-моделей цифровых платформ.

1. Размывание базовых принципов обработки (ст. 5)

Закон декларирует основополагающие принципы: законность и справедливость, ограничение конкретными, заранее определенными целями, соразмерность объема. Однако их применение к детям сталкивается с критическими вопросами:

- **Какова «законная и справедливая цель»** массового сбора голосовых данных 8-летних в интерактивной игре-«песочнице»? Или отслеживания геолокации подростка в социальной сети? Формально цель может быть указана как «улучшение пользовательского опыта», но по сути это служит для тренировки алгоритмов, поведенческого профилирования и максимального удержания внимания, что часто противоречит **интересам развития и безопасности ребенка**.
- **Принцип соразмерности (минимальности данных)** игнорируется: для предоставления базовой игровой или коммуникационной функции необязательно собирать исчерпывающий поведенческий профиль, биометрию или историю перемещений, однако такая практика стала индустриальным стандартом, эксплуатирующим непонимание ребенка о последствиях.

2. Фиктивность «информированного согласия» (ст. 9)

Ключевой правовой основой обработки данных является согласие субъекта. Для его действительности закон предполагает:

- **Информированность:** Полное понимание субъектом целей, состава данных и возможных рисков.
 - **Свободу воли:** Возможность осознанного, безоговорочного и конкретного выбора.
- Оба условия по определению невыполнимы для ребенка:**
- **Для младшего возраста (до 12-13 лет):** Когнитивное развитие не позволяет в полной мере осознать долгосрочные последствия передачи данных. Длиннейшее пользовательское соглашение, написанное юридическим языком, против одного клика — это симуляция согласия, а не его получение.
 - **Для подростка (13-18 лет):** Свобода воли подвергается мощному **техно-социальному давлению**. Доступ к социально значимому сервису (общение со сверстниками, популярная игра) становится безальтернативной необходимостью для социализации. Отказ от предоставления данных де-факто означает цифровую изоляцию, что лишает «согласие» признака добровольности. Это не свободный выбор, а **вынужденная капитуляция** перед условиями доступа к цифровой публичной сфере.

3. Возрастная слепота и проблема верификации

ФЗ-152 не устанавливает **специальных повышенных стандартов защиты для данных несовершеннолетних**, в отличие от, например, GDPR, который определяет возраст цифрового согласия (в РФ этот вопрос законодательно не урегулирован четко). Это порождает проблему:

- **Фактическую невозможность определения возраста:** Большинство сервисов не имеют надежных механизмов возрастной верификации, полагаясь на самодекларацию пользователя, которую легко обойти.

- **Правовую неопределенность:** Если возраст пользователя неизвестен оператору, на него не могут быть возложены специальные обязанности по защите. Это создает лазейку для уклонения от ответственности и **де-факто легализует обработку данных детей по общим, заниженным стандартам.**

4. Несоответствие динамике угроз

Закон фокусируется преимущественно на формальных процедурах и статичной защите данных, но плохо адаптирован к **проактивным и манипулятивным рискам:**

- **Профилирование и таргетированная реклама:** Закон ограничивает автоматизированную обработку, но не запрещает создание поведенческих профилей детей, которые используются для микро-таргетинга рекламы, эксплуатации детских импульсов и формирования потребительских привычек с малых лет.
- **Отсутствие «права на забвение» для детей:** В российском законодательстве право на удаление данных (ст. 21 ФЗ-152) не имеет усиленного режима для несовершеннолетних. Ошибки цифровой юности могут преследовать человека, не будучи забытыми, что противоречит концепции лучших интересов ребенка.

ФЗ-152 в его текущем виде представляет собой **реактивный, формалистичный инструмент**, неспособный эффективно противостоять системным рискам, которым подвергаются несовершеннолетние в цифровой экономике, основанной на сборе и монетизации внимания и данных. Требуется не просто правоприменение, а **сужение (специализация) закона:** введение презумпции повышенной защиты данных ребенка, установление четкого возраста цифрового согласия с обязательной верификацией, запрет на профилирование и таргетированную рекламу для несовершеннолетних, а также закрепление абсолютного права на цифровое забвение для этой категории субъектов. Без этого закон останется благим, но нефункциональным декларативным актом в отношении самой уязвимой группы пользователей.

2.2. Родительское согласие: миф и реальность.

Позиция регулятора, в частности **Роскомнадзора**, в теории является безупречной и жесткой: согласие законного представителя на обработку персональных данных несовершеннолетнего — это **юридически значимое действие повышенной важности**. Оно часто сравнивается с согласием на медицинское вмешательство, что подчеркивает его фундаментальную роль в защите интересов недееспособного субъекта. Законодатель предполагает, что родитель, как ответственный арбитр, взвешенно разрешает или запрещает обработку данных, осознавая потенциальные риски.

Однако на практике этот механизм терпит системное фиаско, превращаясь из инструмента защиты в **ритуальную, проформу или вовсе неработающую конструкцию**. Возникает парадокс: чем жестче формальное требование, тем изощреннее пути его обхода и тем больше иллюзия защищенности.

1. Институциональное принуждение: ситуация в школах и образовательных учреждениях

- **Единый бланк «на все подряд»:** Родителям на подпись предлагается универсальное, неконкретное согласие, которое покрывает все возможные виды обработки данных ребенка: от размещения фото на сайте до передачи в непонятные «партнерские организации». Отказаться — значит немедленно создать для ребенка статус «**белой вороны**», поставить его в неравное положение (не попасть в списки на экскурсию, не участвовать в онлайн-олимпиадах). Это не свободное волеизъявление, а **вынужденная капитуляция** под давлением административной системы.
- **Отсутствие реального выбора и информированности:** Родитель не знает *кому именно, какие конкретно данные, на какой срок и для каких целей* они передаются. Механизм **«отозвать согласие»** на практике неработоспособен и грозит конфликтом с учреждением.

2. Цифровая реальность: массовый уход из-под юрисдикции в соцсетях и играх

- **Фальсификация возраста как социальная норма:** Подавляющее большинство детей, регистрируясь в соцсетях (где минимальный возраст, согласно правилам, 13-16 лет), указывают дату рождения, соответствующую совершеннолетию. Это **сознательный вывод себя из-под правовой защиты**, инициируемый самим ребенком.
- **Попустительство платформ:** Сервисы, заинтересованные в максимальной аудитории, не внедряют надежные механизмы возрастной верификации (например, через Госуслуги или банковское подтверждение), ограничиваясь легко обходимыми «чек-боксами». Таким образом, **институт родительского согласия де-факто уничтожается самими пользователями и молчаливо допускается операторами.**

3. Правовой и технический вакуум после дачи согласия

Даже если согласие было получено честным путем, система защиты рушится на следующем этапе. Существует **тотальный информационный и контрольный вакуум:**

- **Нет механизма прозрачности:** У родителя отсутствуют простые и легитимные инструменты, чтобы проверить: *Что именно собрано о моем ребенке? (голосовые сообщения, геолокация, метаданные переписки). Кому это передано (рекламным сетям, data-брокерам)? Как используется его поведенческий профиль?*
- **Нет эффективного механизма удаления (права на забвение):** Столкнувшись с недобросовестным оператором, который игнорирует запрос на удаление данных ребенка, родитель оказывается в правовой ловушке. Доказывание фактов нарушения и принуждение к исполнению через суд — это длительный, сложный и зачастую непосильный процесс для обычного человека.
- **Обработка данных на основе иного правового основания:** Оператор может перестать опираться на «согласие» и начать обрабатывать данные на основании **«законного интереса» (ст. 6 ФЗ-152)**, что еще больше выводит процесс из-под родительского контроля. Текущая модель родительского согласия — это **юридический ритуал**, не обеспечивающий реальной защиты. Он либо вынужденно-формален (в школах), либо массово игнорируется (в соцсетях), либо не подкреплён инструментами последующего контроля.

2.3. Отраслевая специфика

Сфера	Нормативная база	Проблема	Пример из практики
Образование	ФЗ «Об образовании», приказы Минпросвещения.	Смещение понятий: «образовательная услуга» vs. «коммерческая эксплуатация данных». Видеонаблюдение в классах: где грань между безопасностью и тотальным контролем?	Школа требует установить софт с доступом к камере и микрофону ноутбука ребенка для «контроля внимания».
Здравоохранение	ФЗ № 323-ФЗ, приказы Минздрава.	Обработка данных о здоровье (спецкатегория) ребенка, в т.ч. психическом. Риски утечек и стигматизации.	Создание единой цифровой медкарты ребенка: кто и при каких условиях имеет к ней доступ помимо лечащего врача?

Сфера	Нормативная база	Проблема	Пример из практики
Коммерческие сервисы	ФЗ-152, ФЗ «О защите прав потребителей».	Отсутствие обязанности по реальной верификации возраста. «Возрастные ворота» (age-gating) легко обходятся.	Игра для 6+ с внутриигровыми покупками и чатом. Сбор данных для «персонализации» без внятного объяснения.

Глава 3. Эмпирический срез: ключевые риски, статистика и оценка последних изменений (2024-2025 гг.)

3.1. Картирование угроз.

Угрозы, с которыми сталкивается несовершеннолетний в цифровом пространстве, носят системный и взаимосвязанный характер. Их можно классифицировать на три ключевых кластера: психосоциальное насилие, сексуальная эксплуатация и коммерческо-данная эксплуатация. Каждый из этих кластеров демонстрирует разрыв между скоростью развития технологических рисков и адекватностью правового и социального реагирования.

1. Кибербуллинг (Цифровая травля)

Более 40% российских подростков сталкивались с различными формами кибербуллинга (данные ВЦИОМ, 2024). Это не просто перенос школьных конфликтов в сеть, а качественно новое явление с катализирующими характеристиками:

- **Публичность и масштаб:** Оскорбления, компрометирующие материалы или слухи мгновенно разносятся в чатах, соцсетях и могут стать достоянием всей школы, города или даже страны, многократно усиливая психологический ущерб.
- **Перманентность:** Информация остается в сети навсегда, даже после удаления оригинального поста, продолжая влиять на репутацию жертвы.
- **Отсутствие «безопасного убежища»:** Травля проникает в личное пространство через смартфон, лишая ребенка возможности психологической перезагрузки.
- **Анонимность и ощущение безнаказанности агрессора,** что снимает социальные тормоза и поощряет наиболее жестокие формы поведения.

Правовая неадекватность: Ст. 5.61 КоАП РФ («Оскорбление») и ст. 152 ГК РФ («Защита чести, достоинства и деловой репутации») абсолютно не учитывают **сетеспецифику** травли: ее коллективный, вирусный и перманентный характер. Подать иск о защите чести и достоинства несовершеннолетнему крайне сложно процессуально (требуется представительство, сбор и фиксация цифровых доказательств, определение ответчика среди анонимных аккаунтов). Уголовная статья за клевету (ст. 128.1 УК РФ) также редко применяется к случаям подросткового буллинга. Возникает **правовой вакуум**, где тяжелейший психологический вред не находит соразмерного правового отражения.

2. Груминг (Онлайн-уговоры)

Это процесс установления доверительных отношений взрослым злоумышленником с ребенком в сети с целью последующей сексуальной эксплуатации, шантажа или получения материалов сексуального характера. Угроза основана на эксплуатации детской доверчивости, любопытства и потребности в общении.

- **Тактика:** Злоумышленники маскируются под сверстников, используют общие интересы (игры, музыка), проявляют гипервнимательность и сочувствие, постепенно стирая психологические границы.
- **Правовые лакуны:** Ст. 135 УК РФ («Развратные действия») вступает в силу лишь при очевидных действиях или предложениях. Однако **большую часть процесса — тонкую, длительную манипуляцию, психологическое давление, выманивание интимных фото «в доверие» — уголовный кодекс не покрывает.** До момента совершения явного деяния или отправки явно развратного контента действия грумера часто остаются в правовой серой зоне, что затрудняет превентивное вмешательство правоохранительных органов.

3. Коммерческая эксплуатация цифрового профиля

Персональные и поведенческие данные ребенка становятся высоколиквидным товаром на теневых цифровых рынках. Их эксплуатация выходит далеко за рамки таргетированной рекламы игрушек и принимает опасные формы:

1. **Фишинг и социальная инженерия:** Используя данные о друзьях, интересах и привычках ребенка, злоумышленники создают гиперперсонализированные атаки. Например, письмо «от лучшего друга» с просьбой срочно прислать код из СМС от родителя «для помощи в игре», или сообщение «от администрации соцсети» с угрозой удаления аккаунта.
2. **Кража цифровой личности (Identity Theft):** Похищенные данные (ФИО, дата рождения, данные паспорта родителей, СНИЛС) могут использоваться для оформления микрозаймов, регистрации фейковых аккаунтов для мошенничества или создания «цифрового двойника», чья репутация будет испорчена к моменту совершеннолетия жертвы.
3. **Таргетированная наводка деструктивного контента:** Алгоритмы, основанные на поведенческом профиле, могут целенаправленно подсовывать ребенку опасный контент. Это могут быть:
 - Пропаганда расстройств пищевого поведения («про-ана» сообщества).
 - Материалы, побуждающие к самоповреждению (селлинг) и суицидальному поведению.
 - Контент, разжигающий ненависть, экстремистские идеологии.
 - *Слип-реклама* — маркетинг «взрослых» товаров (азартные игры, БАДы, алкоголь), формирующая будущие потребительские паттерны.

3.2. «Цифровой двойник».

Феномен «цифрового двойника» (digital twin) несовершеннолетнего представляет собой наиболее комплексную и стратегически опасную угрозу, выходящую далеко за рамки конфиденциальности. Это **прогнозная поведенческая модель, алгоритмическая конструкция личности**, которая создается путем агрегации, анализа и синтеза данных из множества цифровых и офлайн-источников. Такой двойник не просто отражает текущее состояние, но и активно используется для прогнозирования и влияния на будущие решения в отношении ребенка, зачастую без его ведома и согласия.

1. Архитектура двойника: источники данных и их синтез

Цифровой профиль формируется из разнородных потоков информации, которые в совокупности дают беспрецедентно полную картину:

- **Образовательная сфера:** Электронный дневник, успеваемость, поведенческие отметки, участие в олимпиадах, записи камер наблюдения в школе.
- **Социальное взаимодействие и коммуникация:** Круг общения, частота и тональность переписки в мессенджерах и соцсетях, список групп и подписок, реакция на контент (лайки, репосты).
- **Поведенческие и биометрические данные:** Геолокация и маршруты перемещений, история поисковых запросов и просмотров, время активности, модели игрового поведения, биометрические параметры (по видео или в играх с VR).
- **Семейный и потребительский контекст:** Данные о платежеспособности семьи (через привязанные карты родителей), потребительские предпочтения, медицинская история (через запись к врачу онлайн или поиск симптомов).

Алгоритмы машинного обучения **синтезируют** эти данные, выявляя скрытые корреляции и строя предположения: о психологическом состоянии (склонность к депрессии по снижению социальной активности), интеллектуальном потенциале, социальной адаптивности, рискованном поведении.

2. Риски предопределения и алгоритмической дискриминации

Главная опасность цифрового двойника — **проактивное формирование жизненных траекторий и создание системной дискриминации.**

- **Образовательные траектории:** Алгоритмическая система может «посоветовать» не включать ребенка в программу для одаренных детей на основе анализа его цифровой активности, которая интерпретируется как «недостаточно усидчивая» или «не соответствующая профилю».
- **Финансовые и страховые риски:** В будущем страховые компании могут отказаться в выгодном полисе или назначить повышенный тариф, основываясь на прогнозной модели рисков, построенной в подростковом возрасте (анализ геолокации в «опасных» районах, интересы, связанные с экстремальным спортом, или даже эмоциональная нестабильность, выявленная по текстам).
- **Карьерные перспективы:** Решения HR-специалистов и систем скрининга резюме через 10-15 лет могут де-факто предопределяться цифровым следом, оставленным в юности. Неудачные шутки, участие в противоречивых сообществах, демонстрация «некорпоративного» поведения могут стать основанием для автоматического отказа, даже если сам кандидат давно изменился.
- **Социальное кредитование и репутация:** Внедрение систем социального рейтинга (явных или скрытых) может использовать историю поведения двойника для ограничения доступа к определенным услугам или возможностям.

3. Правовой вакуум и вызов автономии личности

- **Отсутствие субъектности и согласия:** Цифровой двойник создается **без осознанного, информированного согласия** как самого ребенка, так и его родителей, поскольку они не понимают ни масштабов сбора, ни принципов алгоритмического вывода.
- **Невозможность оспаривания и «права на ошибку»:** Ребенок лишен возможности оспорить выводы, сделанные алгоритмом на основе его данных. Он не может объяснить контекст, исправить неточность или доказать, что прогнозная модель ошибочна. **Право на забвение**, даже если оно существует, не работает против агрегированных и выведенных алгоритмически паттернов.
- **Нарушение права на свободное развитие:** Само существование цифрового двойника, предсказывающего будущее, подрывает фундаментальное право ребенка на свободное формирование личности, на совершение ошибок и изменение, без тотальной цифровой фиксации и оценки каждого шага.

3.3. Анализ последних изменений

Изменение (Закон)	Суть	Плюсы	Минусы и риски
№ 420-ФЗ (поправки в КоАП)	Штрафы для юрлиц до 20 млн. руб. за утечку данных несовершеннолетних.	Сдерживающий эффект. Компании начали audit своих процессов.	Риск «охоты на ведьм»: Штрафуют за формальные нарушения без real harm. Может stifle инновации в edtech.
№ 421-ФЗ (поправки в УК РФ)	Новые ст. 137.1, 272.1 – до 5 лет лишения свободы.	Сильный сигнал о серьезности. Потенциально против организованных групп, торгующих данными.	Сложность расследования киберпреступлений. Риск, что накажут «стрелочника» (сисадмина), а не владельца бизнеса.

Изменение (Закон)	Суть	Плюсы	Минусы и риски
№ 233-ФЗ (обезличивание для госорганов)	Обезличивание данных при межведомственном взаимодействии.	Снижает риски утечек из госсектора.	Угроза анонимности: При наличии достаточного набора обезличенных данных возможна реидентификация. Нужны strong техстандарты.

Вывод по главе: Изменения 2024-2025 гг. – это «тяжелая артиллерия», подвезенная к полю боя, где не хватает «пехоты» – четких, превентивных правил игры для бизнеса и инструментов для самих детей и родителей.

Глава 4. Концепция реформы и проекты конкретных законодательных поправок

4.1. **Философия изменений.**

Мы предлагаем отказаться от идеи, что ребенок – это «проблема», которую нужно изолировать от цифрового мира. Вместо этого – создать безопасную среду для его роста. **Принцип прогрессивной цифровой дееспособности:** Правовой статус ребенка в сети должен постепенно приближаться к статусу взрослого, по мере развития его когнитивных способностей и digital literacy, при этом среда должна компенсировать его уязвимость.

4.2. **Блок поправок №1: Специализация ФЗ-152. Проект статьи 10.1:**

1. **Персональные данные несовершеннолетнего** – любые данные, относящиеся к прямо или косвенно определенному или определяемому лицу, не достигшему восемнадцати лет.
2. Обработка ПДн несовершеннолетнего допускается только при условии обеспечения повышенных мер защиты, предусмотренных настоящим законом и принятыми в соответствии с ним нормативными актами.
3. Запрещается обработка ПДн несовершеннолетнего в целях, которые могут причинить вред его физическому, психическому или нравственному развитию, в том числе для принятия в отношении него автоматизированных решений, порождающих юридические последствия или иным образом существенно затрагивающих его права.

4.3. **Блок поправок №2: Инновационный механизм согласия**

- **10-13 лет:** Оператор обязан направить уведомление ребенку **в доступной форме (иконки, видео)** о том, какие данные и зачем запрашиваются. Обработка начинается **только после получения отдельного подтвержденного согласия родителя.**
- **14-17 лет:** Требуется **двойное подтверждение.** Ребенок дает согласие в интерфейсе сервиса, после чего на email/СМС родителя приходит запрос с ссылкой для подтверждения через ЕСИА. **Ребенок имеет безусловное право на отзыв согласия,** который прекращает обработку для прямого маркетинга и профилирования.

4.4. **Блок поправок №3: Ответственность.**

- **В КоАП:** Новая часть в ст. 13.11 – «Нарушение требований к обработке персональных данных несовершеннолетних». Штрафы: для должностных лиц – 100-300 тыс., для юрлиц – 5-20 млн. руб. или 3-5% от оборота.
- **В УК РФ:** Добавить в ст. 137, 138, 272, 273 УК РФ часть 3: «Те же деяния, совершенные в отношении заведомо несовершеннолетнего...» с повышением санкций на 1/3.

4.5. **Блок поправок №4: Безопасный дизайн.**

- Ввести в ФЗ-152 статью об обязанности операторов, чьи сервисы **привлекают или могут привлечь несовершеннолетних,** применять **настройки максимальной приватности и безопасности по умолчанию (private-by-default, safety-by-default).**

- Установить запрет на использование дизайнерских решений (dark patterns), эксплуатирующих невнимательность, доверчивость или возрастные особенности несовершеннолетних (напр., яркие кнопки «Разрешить все», скрытые галочки согласия, бесконечная прокрутка).

4.6. Прогноз последствий

Сфера	Краткосрочные последствия (1-2 года)	Долгосрочные последствия (3-5 лет)
Право-применение	Рост числа проверок РКН, первые крупные штрафы, судебные споры о толковании новых норм.	Формирование устойчивой положительной практики, снижение числа грубых нарушений.
Бизнес-среда	Рост затрат на compliance, возможный уход с рынка недобросовестных «быстрых» стартапов.	Формирование конкурентного преимущества у этических «безопасных» брендов, рост доверия пользователей.
Общественная сфера	Повышение осведомленности родителей, возможное сопротивление со стороны части подростков.	Повышение цифровой грамотности населения, формирование культуры ответственного отношения к данным с детства.

Заключение

Проведенное исследование продемонстрировало, что действующее правовое регулирование в области защиты цифровых прав несовершеннолетних в Российской Федерации носит реактивный, фрагментарный и зачастую формальный характер. Оно отстает не только от технологических вызовов, но и от эволюции понимания прав ребенка в международном праве.

Ключевой вывод: необходим парадигмальный сдвиг – от защиты **от** цифровой среды к защите **внутри** цифровой среды. Ребенок должен рассматриваться не как пассивный объект охраны, а как развивающийся субъект права, чьи автономия и достоинство должны уважаться в онлайн-пространстве.

Разработанный в работе пакет поправок представляет собой системное решение, построенное на принципах:

1. **Дифференциации** (учет возрастных градаций).
2. **Превенции** (принцип безопасности по дизайну и умолчанию).
3. **Сбалансированности** (сочетание повышенной ответственности операторов с расширением инструментов контроля для детей и родителей).
4. **Технологической нейтральности и эффективности** (нормы сформулированы так, чтобы быть применимыми к evolving технологиям).

Внедрение предложенных мер потребует coordinated усилий законодателя, регулятора, бизнеса и образовательного сообщества. Финансовые и административные издержки на первом этапе будут значительны. Однако альтернатива – растущее поколение, чьи приватность и психическое здоровье были разменяны на удобство и прибыль, – неприемлема с точки зрения национальной безопасности и устойчивого развития России. Защита цифрового детства – это инвестиция в цифровое будущее страны, основанное на доверии, безопасности и уважении к правам личности.

Библиографический список

Нормативные правовые акты Российской Федерации:

1. Конституция Российской Федерации.
2. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ.
3. Семейный кодекс Российской Федерации от 29.12.1995 № 223-ФЗ.
4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
5. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ.
6. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ.
7. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

Международные правовые акты и документы:

8. Конвенция о правах ребенка. Принята резолюцией 44/25 Генеральной Ассамблеи ООН от 20 ноября 1989 года.
9. Committee on the Rights of the Child. General comment No. 25 (2021) on children's rights in relation to the digital environment.
10. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation — GDPR).
11. Children's Online Privacy Protection Act of 1998 (COPPA).

Научная и учебная литература (монографии, учебники):

12. Балашова, Т. Н. Цифровое право: учебник для вузов. — Москва: Издательство Юрайт, 2023. — 389 с. (Серия: Высшее образование). — ISBN 978-5-534-15865-7.
13. Незнамов, А. В., Полякова, Т. А. Персональные данные: правовое регулирование. — 3-е изд., перераб. и доп. — Москва: Статут, 2024. — 480 с. — ISBN 978-5-8354-1738-3.

Научные статьи в журналах

14. Подустова, О. Л. Кибербуллинг несовершеннолетних: проблемы квалификации и противодействия // Государство и право. — 2024. — № 5. — С. 112–125.
15. Чурочкина, А. А. Принцип наилучших интересов ребенка в цифровой среде: имплементация в российское право // Журнал зарубежного законодательства и сравнительного правоведения. — 2025. — № 1.

Приложение:

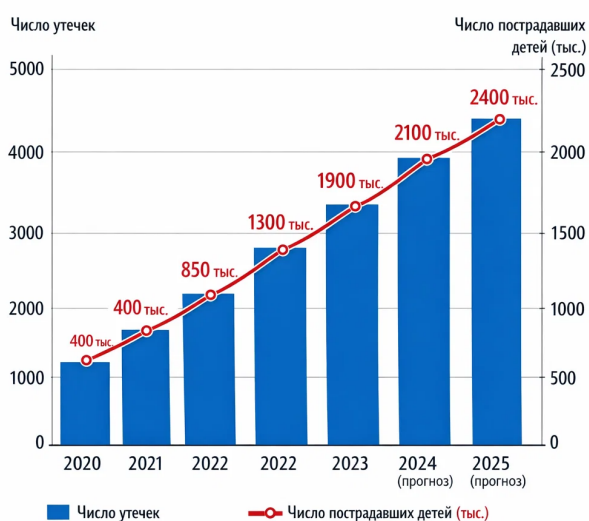
Приложение А: Сравнительная таблица регулирования защиты ПДн несовершеннолетних в РФ, ЕС (GDPR) и США (COPPA).

Критерий	Российская Федерация (152-ФЗ)	Европейский Союз (GDPR)	США (COPPA)
Возрастной порог	Не установлен специально. Общие нормы о недееспособности/ограниченной дееспособности (ст. 28 ГК РФ).	«Возраст цифрового согласия» от 13 до 16 лет (устанавливают государства-члены). До него необходимо согласие родителя.	Фиксированный возраст – младше 13 лет. Закон применяется к сбору данных о детях этой возрастной группы.
Требование к согласию	Для обработки данных несовершеннолетних необходимо согласие их законных представителей (родителей, усыновителей, попечителей).	Требуется, только если основанием обработки является согласие (ст. 8 GDPR). Требуется явное согласие родителя.	Обязательное верифицированное согласие родителя перед сбором данных.
Правовая основа и охват	Общий закон о защите ПДн (152-ФЗ). Защита несовершеннолетних — его частное применение.	Общий регламент (GDPR) с особыми гарантиями для детей (ст. 8, Преамбула 38). Принцип экстерриториальности.	Специализированный отраслевой закон. Применяется к сайтам/сервисам, направленным на детей, или тем, кто знает, что собирает данные ребенка.
Права несовершеннолетних	Общие права субъекта ПДн. Особого акцента на адаптацию информации для детей в 152-ФЗ нет.	Особое внимание: информация и уведомления должны быть на понятном для ребенка языке (ст. 12 GDPR).	Акцент на правах и контроле родителей (право на отзыв согласия, просмотр, удаление данных ребенка).

Критерий	Российская Федерация (152-ФЗ)	Европейский Союз (GDPR)	США (СОРРА)
Верификация согласия и возраста	Четкие методы не прописаны. На практике запрашиваются данные родителя.	Контролер должен приложить разумные усилия для проверки с учетом доступных технологий. С 2025 года — ужесточение (например, EU Digital Identity Wallet).	Закон предусматривает конкретные методы (например, оплата картой, заполнение формы, звонок, «email+»). FTC одобряет новые методы.
Ответственность и штрафы	Штрафы для юрлиц до 500 тыс. руб. (КоАП РФ, ст. 13.11).	Штрафы до 10 млн евро или 2% глобального годового оборота (ст. 83 GDPR). С 2025 года правила ужесточатся.	Гражданские штрафы до \$50,120 за каждое нарушение . Крупные дела (TikTok, YouTube) приводят к соглашениям на сотни миллионов долларов.

Приложение Б: Графики и диаграммы. (2 стр.)

Динамика утечек ПДн, затрагивающих несовершеннолетних, в РФ (2020-2025 гг., по данным РКН и утечек в публичном поле)





Приложение В: Проекты текстов поправок в законодательные акты.

1 Выдержки с новой редакцией статей ФЗ-152, КоАП, УК РФ.

Статья 1

Внести в Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» следующие изменения:

1. Статью 3 дополнить пунктом 11 следующего содержания:

«11) утечка персональных данных — несанкционированное раскрытие, предоставление, распространение либо доступ к персональным данным, повлекшие или способные повлечь нарушение прав и законных интересов субъекта персональных данных.»

2. Статью 5 изложить в следующей редакции:

«Статья 5. Принципы обработки персональных данных

1. Обработка персональных данных осуществляется на законной, справедливой и прозрачной основе.
2. Обработка персональных данных допускается только для достижения конкретных, заранее определённых и законных целей.
3. Не допускается обработка персональных данных, несовместимая с целями их сбора.
4. Содержание и объём обрабатываемых персональных данных должны соответствовать заявленным целям обработки и не быть избыточными.
5. Оператор обязан принимать необходимые правовые, организационные и технические меры для обеспечения безопасности персональных данных и предотвращения их утечки.»
6. Статью 6 дополнить частью 6 следующего содержания:

«6. Оператор обязан по требованию субъекта персональных данных или уполномоченного органа подтвердить законность обработки персональных данных и достаточность принимаемых мер по их защите.»

4. Статью 18 дополнить частью 4 следующего содержания:

«4. Оператор обязан уведомлять уполномоченный орган по защите прав субъектов персональных данных о факте утечки персональных данных не позднее чем в течение 72 часов с момента её обнаружения.»

5. Статью 19 изложить в следующей редакции:

«Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

1. Оператор обязан принимать необходимые и достаточные меры для защиты персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения.
2. Состав и содержание мер по обеспечению безопасности персональных данных определяются оператором с учётом актуальных угроз безопасности и категории обрабатываемых персональных данных.
3. Непринятие либо ненадлежащее принятие указанных мер влечёт ответственность, установленную законодательством Российской Федерации.»

Статья 2

Внести в Кодекс Российской Федерации об административных правонарушениях следующие изменения:

1. Дополнить главу 13 статьёй 13.11.1 следующего содержания:

«Статья 13.11.1. Нарушение требований законодательства Российской Федерации о персональных данных

1. Невыполнение оператором обязанностей по обеспечению безопасности персональных данных — влечёт наложение административного штрафа на должностных лиц в размере от 50 000 до 100 000 рублей; на юридических лиц — от 500 000 до 1 000 000 рублей.
2. Те же действия, повлекшие утечку персональных данных, — влекут наложение административного штрафа на должностных лиц в размере от 100 000 до 200 000 рублей; на юридических лиц — от 1 000 000 до 3 000 000 рублей.
3. Повторное совершение административного правонарушения, предусмотренного частями 1 или 2 настоящей статьи, — влечёт наложение административного штрафа на должностных лиц в размере от 200 000 до 300 000 рублей либо дисквалификацию на срок до трёх лет; на юридических лиц — от 3 000 000 до 5 000 000 рублей.»
4. В статье 4.3 часть 1 дополнить пунктом 8 следующего содержания:

«8) совершение административного правонарушения в сфере обработки персональных данных, повлекшего массовую утечку таких данных.»

Статья 3

Внести в Уголовный кодекс Российской Федерации следующие изменения:

1. Дополнить главу 19 статьёй 137.1 следующего содержания:

«Статья 137.1. Незаконная обработка персональных данных

1. Незаконный сбор, хранение, использование или распространение персональных данных без согласия субъекта персональных данных, если такие деяния повлекли причинение значительного вреда правам и законным интересам гражданина, — наказываются штрафом в размере до 500 000 рублей либо лишением свободы на срок до двух лет.
2. Те же деяния, совершённые: а) в отношении персональных данных двух и более лиц; б) лицом с использованием своего служебного положения; в) с использованием информационно-телекоммуникационных сетей, — наказываются штрафом в размере до 1 000 000 рублей либо лишением свободы на срок до четырёх лет.
3. Деяния, предусмотренные частями первой или второй настоящей статьи, повлёкшие тяжкие последствия, — наказываются лишением свободы на срок до шести лет.»

Статья 4

Настоящий Федеральный закон вступает в силу по истечении 180 дней со дня его официального опубликования.

Приложение Г: Модельные формы согласий. (2 стр.)

- **Образец формы «Уведомления несовершеннолетнего 10-13 лет и Запроса согласия законного представителя».**

1. УВЕДОМЛЕНИЕ НЕСОВЕРШЕННОЛЕТНЕГО

(в возрасте от 10 до 13 лет)

Уважаемый(ая) _____
(имя, фамилия несовершеннолетнего)

Настоящим сообщаем, что при использовании _____
(наименование сайта, сервиса, образовательной программы, мероприятия)

могут обрабатываться твои персональные данные.

Персональные данные — это информация о тебе, например:

- фамилия, имя;
- возраст, дата рождения;
- сведения об обучении, участии в мероприятиях;
- контактная информация (если предоставляется);
- иные данные, которые ты или твой законный представитель сообщаете добровольно.

Зачем обрабатываются твои персональные данные:

- для организации обучения, занятий или мероприятий;
- для связи с тобой и твоими законными представителями;
- для обеспечения твоего участия в программах и сервисах;
- для выполнения требований законодательства Российской Федерации.

Важно знать:

- твои персональные данные защищаются в соответствии с законом;

- ими пользуются только уполномоченные сотрудники;
- твои данные не будут переданы посторонним лицам без законных оснований;
- обработка данных возможна **только с согласия твоего законного представителя.**

Если у тебя есть вопросы, ты можешь задать их своему законному представителю или обратиться к ответственному лицу оператора персональных данных.

2. ЗАПРОС СОГЛАСИЯ ЗАКОННОГО ПРЕДСТАВИТЕЛЯ

на обработку персональных данных несовершеннолетнего

Я, _____
(фамилия, имя, отчество законного представителя)

паспорт: серия _____ № _____, выдан _____,

являясь законным представителем несовершеннолетнего:

Фамилия, имя ребёнка _____
Дата рождения _____,

настоящим **даю согласие** _____
(наименование оператора персональных данных)

на обработку персональных данных моего несовершеннолетнего ребёнка в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

Перечень персональных данных:

- фамилия, имя, отчество;
- дата рождения, возраст;
- сведения об обучении (участии в программах, мероприятиях);
- контактные данные (при необходимости);
- иные сведения, предоставляемые в рамках указанных целей.

Цели обработки персональных данных:

- организация и обеспечение участия ребёнка в программах, мероприятиях, сервисах;
- информационное сопровождение;
- выполнение требований законодательства Российской Федерации.

Способы обработки:

сбор, запись, систематизация, накопление, хранение, уточнение, использование, передача (в случаях, предусмотренных законом), обезличивание, блокирование, удаление, уничтожение.

Согласие действует **до достижения целей обработки** либо до момента его отзыва.

Я уведомлён(а), что:

- согласие может быть отозвано в любое время путём направления письменного заявления оператору;
- отзыв согласия не влияет на законность обработки, осуществлённой до его отзыва.

Подпись законного представителя _____ / _____ /

Дата «» _____ 20__ г.

- Образец формы «Совместного подтверждаемого согласия несовершеннолетнего (14+) и законного представителя».

1. СВЕДЕНИЯ О НЕСОВЕРШЕННОЛЕТНЕМ

Фамилия, имя, отчество _____

Дата рождения _____

Документ, удостоверяющий личность (при наличии):

наименование _____ серия _____ № _____, выдан _____

2. СВЕДЕНИЯ О ЗАКОННОМ ПРЕДСТАВИТЕЛЕ

Фамилия, имя, отчество _____

Статус законного представителя (родитель, опекун, попечитель) _____

Паспорт: серия _____ № _____, выдан _____

Адрес проживания _____

3. СВЕДЕНИЯ ОБ ОПЕРАТОРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Наименование оператора _____

Адрес _____

4. СОВМЕСТНОЕ СОГЛАСИЕ

Мы, нижеподписавшиеся:

несовершеннолетний, достигший возраста 14 лет, и его законный представитель,

настоящим **совместно и осознанно подтверждаем согласие** на обработку персональных данных несовершеннолетнего _____ (фамилия, имя, отчество)

оператором персональных данных _____ (наименование оператора)

в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

5. ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

Согласие даётся на обработку следующих персональных данных несовершеннолетнего:

- фамилия, имя, отчество;
- дата рождения, возраст;
- сведения об обучении, участии в программах, мероприятиях;
- контактные данные (адрес электронной почты, номер телефона — при наличии);
- фото- и видеоматериалы (при необходимости);
- иные сведения, предоставляемые в рамках заявленных целей.

6. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка персональных данных осуществляется в целях:

- организации и обеспечения участия несовершеннолетнего в образовательных, информационных или иных программах;
- информационного и организационного взаимодействия;
- выполнения требований законодательства Российской Федерации.

7. СПОСОБЫ И СРОК ОБРАБОТКИ

Обработка персональных данных может включать следующие действия:

сбор, запись, систематизацию, накопление, хранение, уточнение, использование, передачу (в случаях, предусмотренных законом), обезличивание, блокирование, удаление, уничтожение.

Согласие действует до достижения целей обработки персональных данных, если иной срок не установлен законодательством Российской Федерации, либо до момента его отзыва.

8. ПОДТВЕРЖДЕНИЕ ОСОЗНАННОСТИ СОГЛАСИЯ

Несовершеннолетний подтверждает, что:

- ему разъяснено, какие персональные данные обрабатываются и с какой целью;
- он понимает значение своих действий и выражает согласие добровольно.

Законный представитель подтверждает, что:

- ознакомлен с условиями обработки персональных данных;
- согласие даётся в интересах несовершеннолетнего;
- права несовершеннолетнего не нарушаются.

9. ПОРЯДОК ОТЗЫВА СОГЛАСИЯ

Согласие может быть отозвано полностью или частично в любое время путём направления письменного заявления оператору персональных данных. Отзыв согласия не влияет на законность обработки, осуществлённой до его отзыва.

10. ПОДПИСИ СТОРОН

Несовершеннолетний (14+)

Подпись _____ / _____ /

Дата «_» _____ 20__ г.

Законный представитель

Подпись _____ / _____ /

Дата «_» _____ 20__ г.