

Организационно-дидактические аспекты цифровизации образования / Organizational and Didactic Aspects of the Digitalization of Education

Научная статья

Original article

DOI: [10.12731/2658-4034-2026-17-1-971](https://doi.org/10.12731/2658-4034-2026-17-1-971)

EDN: [RNPJKG](https://edn.rnpjkg.ru)

УДК 37.04



Кибербезопасность обучающихся в цифровой образовательной среде: психолого-педагогические аспекты профилактики

В.В. Мантуленко

*Самарский национальный исследовательский университет имени академика
С.П. Королёва, Самара, Российская Федерация*

Аннотация

Обоснование. Цифровизация образования, ускоренная глобальными вызовами последних лет, привела к формированию и распространению гибридных и дистанционных моделей обучения, в которых пронизанная цифровыми ресурсами и информацией среда становится основным пространством учебной деятельности и социального взаимодействия. Параллельно с дидактическими возможностями данная среда порождает комплекс психологических рисков и угроз кибербезопасности личности, включая кибербуллинг, цифровую зависимость, утечку персональных данных, негативное воздействие контента, цифровую депривацию и проч. Несформированность цифровой культуры и медиаграмотности у значительной части школьников и студентов, а также недостаточная готовность педагогов к решению задач цифровой социализации создают предпосылки для роста психологического неблагополучия и виктимизации всех участников образовательного процесса.

Цель – обоснование и разработка психолого-педагогической модели профилактики угроз кибербезопасности обучающихся в цифровой образовательной среде, интегрирующей деятельность педагогов-психологов, родителей и администрации образовательных организаций.

Материалы и методы. Методологической основой исследования выступает системный подход, рассматривающий цифровую образовательную среду как единство технологических, социальных и психологических компонентов. В исследовании применялись методы анализа и синтеза научной литературы по вопросам цифровой педагогики, киберпсихологии, медиабезопасности, статистических

данных. Эмпирическую базу составили анкетирование обучающихся (студентов Самарских вузов), глубинные интервью педагогов, экспертные интервью со специалистами в области информационной безопасности образования.

Результаты. На основе полученных аналитических данных разработана многоуровневая психолого-педагогическая модель профилактики, включающая диагностический модуль, образовательно-развивающий модуль, социально-проектный модуль и антикризисный модуль. Особое внимание уделено необходимости формирования медиаграмотности всех участников образовательного процесса.

Ключевые слова: кибербезопасность личности; цифровая образовательная среда; психолого-педагогическая профилактика; цифровая гигиена; медиаграмотность; цифровая социализация

Для цитирования. Мантуленко, В. В. (2026). Кибербезопасность обучающихся в цифровой образовательной среде: психолого-педагогические аспекты профилактики. *Russian Journal of Education and Psychology*, 17(1-1), 215–236. <https://doi.org/10.12731/2658-4034-2026-17-1-971>

Cyber security of the learner's personality in the digital educational environment: psychological and pedagogical aspects of prevention

V.V. Mantulenko

*Samara National Research University named after Academician S.P. Korolev,
Samara, Russian Federation*

Abstract

Background. The digitalization of education, accelerated by global challenges in recent years, has led to the formation and widespread adoption of hybrid and distance learning models. In these models, an environment saturated with digital resources and information becomes the primary space for learning activities and social interaction. While offering significant didactic potential, this environment simultaneously generates a complex of psychological risks and personal cyber security threats, including cyber bullying, digital addiction, personal data leaks, exposure to harmful content, digital deprivation, and others. The lack of digital culture and media literacy among a significant portion of schoolchildren and students, coupled with insufficient preparedness of educators to address the challenges of digital socialization, creates preconditions for increased psychological distress and victimization among all participants in the educational process.

Purpose. The research purpose is to justify and develop a psychological and pedagogical model for preventing cyber security threats among learners in the digital educa-

tional environment, integrating the efforts of educators, psychologists, parents, and the administration of educational institutions.

Materials and methods. The methodological basis of the study is a systems approach, which considers the digital educational environment as a unity of technological, social, and psychological components. Methods of analysis and synthesis were applied to scientific literature on digital pedagogy, cyber psychology, media safety, and statistical data. The empirical base consisted of a survey of learners (students from Samara universities), in-depth interviews with educators, and expert interviews with specialists in the field of educational information security.

Results. Based on the obtained data, a multi-level psychological and pedagogical prevention model has been developed. It includes: a diagnostic module, an educational and developmental module, a social and project module, and an anti-crisis module. Particular attention is paid to the need to develop media literacy among all participants in the educational process.

Keywords: personal cybersecurity; digital educational environment; psychological and pedagogical prevention; digital hygiene; media literacy; digital socialization

For citation. Mantulenko, V. V. (2026). Cyber security of the learner's personality in the digital educational environment: psychological and pedagogical aspects of prevention. *Russian Journal of Education and Psychology*, 17(1-1), 215–236. <https://doi.org/10.12731/2658-4034-2026-17-1-971>

Введение

В условиях глобальной цифровизации нашего общества, определяющей повседневность современных детей и молодежи, традиционные учебные дисциплины утрачивают монополию на формирование ключевых, жизненно важных компетенций. Среди таких компетенций всё чаще упоминается цифровая грамотность (или медиаграмотность) как комплексный навык, необходимый для существования в современном мире. Данное понятие существенно шире базовой компьютерной компетентности и включает два основополагающих компонента: цифровую гигиену (обеспечение безопасности и защиты личного информационного пространства) и медиаграмотность (критическую навигацию в информационной и коммуникационной среде). Перед системой образования стоит задача не фрагментарного включения данных аспектов в учебный процесс, а их стержневой интеграции в образовательный процесс, направленной на формирование у обучающихся устойчивости к цифровым угрозам и манипулятивным практикам [1].

В современном контексте приватность обучающихся рассматривается не только как неприкосновенность личных записей, но как защита всей совокупности цифровых следов, генерируемых ими в сети: поисковых запросов, реакций (лайков), переписки в мессенджерах и данных с образовательных платформ. Эмпирические данные свидетельствуют о значительном уровне цифровых рисков. Согласно исследованию «Лаборатории Касперский» [2], свыше 60% респондентов в возрасте 7-18 лет сталкивались с различными онлайн-угрозами, включая кражу аккаунтов, кибербуллинг и мошеннические схемы. При этом лишь около трети подростков осознают риски, ассоциированные с публикацией геолокационных данных или личных изображений в открытом доступе.

Цифровая трансформация системы образования, декларируемая как национальный приоритет в рамках государственных программ в нашей стране, привела к масштабному внедрению цифровых платформ, электронных учебников, облачных сервисов и инструментов виртуальной коммуникации в повседневную педагогическую практику. Цифровая образовательная среда (ЦОС) перестала быть вспомогательным элементом, превратившись в обязательную инфраструктуру современного обучения. Однако, стремительная «технологизация» и часто нерегулируемое медиапользование детей и молодежи породили системный разрыв между техническими возможностями цифровых систем и психолого-педагогическим обеспечением безопасности их пользователей, прежде всего, это касается обучающихся, которые в онлайн проводят значительную часть своего учебного и досугового времени [3].

Понятие «кибербезопасность личности» в образовательном контексте выходит за рамки традиционной защиты от вирусов или хакерских атак. Оно включает в себя сохранение психического здоровья, эмоционального благополучия, личного достоинства и репутации обучающегося в условиях цифровых взаимодействий [4]. Современные угрозы носят комплексный характер: от внешних (деструктивный контент, мошенничество, деятельность злоумышленников) до внутренних, порождаемых самими пользователями в результате низкой цифровой культуры (кибербуллинг, избыточный обмен личной информацией, формирование интернет-зависимостей). Особую уязвимость демонстрируют подрост-

ки, для которых цифровое пространство является ключевой площадкой для самоидентификации и социального признания. Исследования показывают, что пережитый опыт кибервиктимизации коррелирует с ростом тревожности, депрессивных симптомов, снижением академической мотивации и даже суицидальными мыслями [5].

Несмотря на наличие значительного числа работ, посвященных техническим аспектам информационной безопасности в образовании, а также исследованиям Интернет-зависимости и буллинга, проблема комплексной психолого-педагогической профилактики угроз кибербезопасности личности в ЦОС остается недостаточно разработанной. Существующие подходы часто носят фрагментарный характер, сводятся к разовым мероприятиям или публикациям о правилах поведения в сети или техническим ограничениям доступа. Отсутствуют целостные модели, которые бы объединяли усилия всех субъектов образовательного процесса (педагога, психолога, родителя, самого обучающегося) на основе превентивной, а не запретительной парадигмы.

В этой связи *целью* данного исследования является обоснование и разработка психолого-педагогической модели профилактики угроз кибербезопасности личности обучающегося, интегрируемой в контекст цифровой образовательной среды.

Для достижения цели были поставлены следующие *задачи*:

- 1) проанализировать структуру и специфику цифровых рисков в образовании;
- 2) выявить уровень готовности педагогов к реализации профилактических функций в цифровой среде;
- 3) разработать структурные компоненты и содержательное наполнение многоуровневой профилактической модели;
- 4) определить критерии эффективности ее внедрения в практику образовательной организации.

Материалы и методы

Исследование опирается на междисциплинарный подход к анализу кибербезопасности, поскольку рассмотрение данного феномена в контексте образования не представляется возможным без синте-

за технических и гуманитарных исследований. Ведущим выступил системный подход, позволивший рассмотреть цифровую образовательную среду как сложную антропотехническую систему, где социальные практики, психологические особенности медиапользования, технологические возможности платформ, устройств и возникающие риски находятся в постоянном взаимодействии и взаимовлиянии. Теоретическую базу составили концепции цифровой социализации [6-8], исследования онлайн-рисков [9-11], а также разработки в области киберпсихологии [12-14].

Эмпирическая часть исследования проводилась в 2023–2025 годы и включала несколько этапов: ежегодные опросы студенческой молодежи (анкетирование) с целью выявления их цифровых практик, опыта столкновения с угрозами и уровня знаний в области искусственного интеллекта и кибербезопасности; опрос педагогов (интервьюирование) по теме распознавания цифровых рисков и организации профилактической работы; обобщение данных аналитических отчетов, актуальных научных исследований, экспертных интервью по теме работы.

Результаты и обсуждение

Структура и специфика цифровых рисков в образовании

Ключевая проблема, отражающая весь спектр существующих рисков сферы цифровизации образования, может быть описана как «парадокс приватности»: поколение «цифровых аборигенов» часто демонстрирует низкий уровень медиаграмотности в целом и осмотристельности в вопросах безопасности в частности [15]. Распространены практики использования простых и повторяющихся паролей, перехода по непроверенным гиперссылкам и предоставления приложениям избыточных разрешений без оценки последствий. Данная ситуация является следствием не только личной безответственности, но и результатом отсутствия системного формирования соответствующих компетенций в рамках образовательного процесса (обучения и воспитания).

На основе анализа актуальных исследований в области цифровых рисков детского и молодежного медиапользования нами были сформулированы следующие выводы:

– ранняя и тотальная цифровизация детства (возраст первого знакомства с гаджетами неуклонно снижается, гаджеты стали неотъемлемой частью жизни детей с самого раннего возраста) [16];

– эволюция роли гаджетов: от развлечения к универсальному инструменту (если в дошкольном возрасте основная функция цифровых устройств сводится к развлечениям, что, прежде всего, определяется ведущим видом деятельности, то с возрастом цифровое устройство трансформируется в инструмент для общения (89% старшеклассников), учебы (70%) и поиска информации [17];

– рост экранного времени и ослабление родительского контроля (ежедневное использование смартфона становится нормой к 11 годам, при этом контроль экранного времени со стороны родителей ослабевает: его ограничивают 84% родителей младших школьников и лишь 47% – старшеклассников [17; 18]);

– онлайн-среда сегодня – это полноценное пространство детской социализации и коммуникации (цифровое общение с родителями служит не только для решения практических задач (местоположение, быт), но и для поддержания эмоциональной связи (обмен шутками, мемами), а групповые чаты с одноклассниками (одногоруппниками) и друзьями становятся важным каналом коммуникации);

– снижение интереса к традиционным соцсетям и блогам, но рост значения мессенджеров (при этом мессенджеры выполняют не только свои прямые функции, но и становятся всё более популярными как источник новостей, что способствует риску попасть под влияние «фейковой» информации);

– повышение осторожности в вопросах конфиденциальности в социальных сетях на фоне роста родительского контроля (школьники и студенты стали реже указывать в соцсетях информацию о себе, ограничивают доступ к профилю, одновременно резко вырос родительский контроль: доля родителей, знающих пароли от аккаунтов детей, увеличилась с 19% (2023) до 29% (2024) [17]);

– высокая распространенность онлайн-угроз, эволюция их характера (каждый четвертый ребенок сталкивался с кибербуллингом, появляются новые угрозы, такие как травля с использованием

дипфейков, при этом дети активно используют искусственный интеллект в учебных целях: для поиска информации, для домашних заданий) [17-19];

– «парадокс осведомленности»: дети не сообщают родителям об опасных контактах в цифровой среде (это указывает на разрыв в коммуникации и недостаток доверия) [20];

– в целом, цифровая безопасность формируется как общая ответственность и сфера карьерных предпочтений (многие родители осознают необходимость защиты, но методы должны быть сбалансированы, чтобы не подрывать доверие; 47% родителей хотели бы для своих детей карьеры в IT, а 33% – конкретно в сфере кибербезопасности, видя в этом перспективное направление, тогда как среди детей этот интерес выражен слабее – 35% и 22% соответственно) [17].

Результаты анкетирования студентов, анализ актуальных исследований других авторов, статистических отчетов позволили нам выделить наиболее распространенные риски по степени их субъективной значимости и частоте возникновения:

- 1) кибербуллинг (травля в сети): дети и молодежь становятся объектами насмешек, оскорблений или распространения ложной информации о себе в мессенджерах или соцсетях [19; 20];
- 2) цифровая зависимость и прокрастинация: среди детей и молодежи все чаще наблюдаются признаки компульсивного использования смартфонов/соцсетей во время занятий и выполнения учебных заданий, синдром FOMO (Fear Of Missing Out – страх пропустить что-то важное), что приводит к фрагментации внимания и снижению глубины понимания материала [21];
- 3) низкий уровень цифровой гигиены: использование одинаковых паролей для разных образовательных платформ и личных аккаунтов, не использование двухфакторной аутентификации, размещение в открытом доступе информации о своем месте учебы, расписании, планах на выходные и проч. [22; 23];
- 4) контакты с незнакомцами и риск груминга: принятие запросов на дружбу в соцсетях от незнакомых взрослых, позиционирующих

себя как «репетиторы», «кураторы проектов», «потенциальные работодатели» и т.д. [24; 25];

- 5) эмоциональное выгорание от цифровой коммуникации: многие студенты отмечают рост усталости и раздражительности, связанный с необходимостью постоянного мониторинга множества учебных чатов, почты и LMS (Learning Management System) образовательного учреждения [26].

Данные опроса педагогов выявили существенный дефицит готовности к системной профилактической работе, основанный, в первую очередь, на их медиакомпетентности, несоответствующей современному уровню технологического развития.

Что касается когнитивного компонента готовности, педагогам необходимо знать основные нормативные документы, регулирующие цифровую безопасность в контексте образования, глубоко понимать сущность важнейших явлений (кибербуллинга, цифровой гигиены, онлайн груминга, цифровой зависимости и т.д.).

Процедурно-деятельностный компонент готовности включает в себя эффективное и этичное применение цифровых устройств в своей работе, проведение с обучающимися профилактических бесед, обсуждений актуальных тем, владение алгоритмом действий в случае наступления тех или иных цифровых рисков).

Эмоционально-ценностный компонент означает осознанное и ответственное отношение к вопросам кибербезопасности. Сегодня среди многих педагогов преобладает феномен «цифрового пессимизма» – восприятия цифровой среды преимущественно как источника угроз. С одной стороны, это явление имеет вполне объяснимые причины (высокая нагрузка современных педагогов, многозадачность, недостаток знаний о возможностях эффективной интеграции устройств и ресурсов в свою работу, и др.), с другой – в значительной степени блокирует проактивные воспитательные стратегии и стратегии обучению безопасному взаимодействию с медиа и информацией.

Интервью с педагогами подтвердили, что в программах повышения квалификации тема психолого-педагогического сопровождения кибербезопасности на сегодняшний момент представлена фрагментарно или отсутствует вовсе.

Психолого-педагогическая модель профилактики угроз кибербезопасности обучающихся в цифровой образовательной среде

На основе анализа эмпирических данных и теоретических положений разработана многоуровневая модель профилактики, состоящая из четырех взаимосвязанных модулей.

Модуль 1 – диагностико-аналитический. Целью модуля является систематический мониторинг цифрового климата и выявление групп/индивидуумов риска. Инструменты реализации данного блока включают анонимные срезы (опросы), составление карт наблюдения за поведением обучающихся во время занятий, анализ тональности общения в официальных учебных чатах (при соблюдении этических норм и с информированного согласия). В качестве ключевого показателя эффективности реализации данного модуля может быть взят «Индекс цифрового благополучия класса/группы», агрегирующий данные по шкалам безопасности, этичности и продуктивности онлайн-взаимодействий.

Модуль 2 – образовательно-развивающий – нацелен на формирование устойчивых компетенций кибербезопасности и цифровой культуры у всех участников ЦОС. Для процесса обучения это означает включение специальных блоков в предметное содержание (например, на занятиях по общественным наукам – анализ кейсов о защите цифровых прав, цифровых рисков; на занятиях по информатике – практикумы по созданию надежных паролей и настройке приватности; в рамках гуманитарных наук – обсуждение проблематики виртуальной идентичности в современной литературе, науке, бизнесе, авторского права в эпоху искусственного интеллекта). Специальное обучение основам кибербезопасности включает проведение практикумов по разбору принципов двухфакторной аутентификации, формирование навыков управления приватностью (развитие умения анализировать пользовательские соглашения и конфигурировать настройки конфиденциальности в социальных сетях для контроля видимости персональной информации).

В рамках внеурочной деятельности это могут быть тренинги по цифровому эмпатическому интеллекту (развитие навыков распознавания эмоций за текстовыми сообщениями, осознание последствий различных цифровых следов), критическому и системному мышлению,

продуктивным видам речевой деятельности и т.д. Воспитание ответственного отношения к цифровым данным включает осознание феномена «цифровой татуировки» – перманентности размещенной в сети информации – и обсуждение долгосрочных последствий ее публикации для репутации и карьерных перспектив.

Для педагогов в рамках данного модуля могут быть разработаны курсы повышения квалификации (например, «Цифровая педагогическая этика и безопасность», включающий разбор реальных кейсов, ролевые игры по разрешению цифровых конфликтов, освоение базовых навыков психологической поддержки жертвам кибербуллинга и проч.). Для родителей также важно предусмотреть отдельный модульный трек, который может включать (онлайн) лектории по вопросам родительского контроля цифровых взаимодействий детей и молодежи, практические рекомендации по созданию семейной цифровой культуры, распознаванию сигналов дистресса у ребенка после онлайн-активности и др.

Критериями эффективности реализации второго модуля могут быть:

- уровень цифровой грамотности (средний балл обучающихся, педагогов и родителей по итогам регулярного тестирования на знание основ кибергигиены, медиаграмотности и цифрового этикета (входной/выходной срез));

- изменение поведенческих паттернов (снижение доли обучающихся, использующих простые/повторяющиеся пароли; увеличение доли аккаунтов с настроенной двухфакторной аутентификацией и ограниченной приватностью; повышение частоты верификации информации перед её репостом/использованием);

- уровень информированности о рисках (число правильных ответов на кейс-вопросы по распознаванию фишинга, мошеннических схем, кибербуллинга и манипулятивного контента);

- субъективная оценка готовности педагогов (баллы в самоотчетах педагогов по шкалам «Самоеффективность в решении цифровых конфликтов», «Уверенность в проведении профилактической работы»);

- вовлеченность родителей (посещаемость родительских лекториев и активность в обсуждениях, обращения родителей за консультативной (а не экстренной) помощью по цифровым вопросам).

Модуль 3 – социально-проектный. Здесь целью является трансформация обучающихся: от пассивных объектов защиты до активных агентов создания собственной безопасной информационной и коммуникационной среды. Данный модуль может быть реализован через создание и поддержку школьных/студенческих «кибердружин» – волонтерских групп, которые под руководством психолога и IT-специалиста проводят консультации, создают просветительский контент (мемы, короткие видео, посты), организуют хакатоны по разработке различных тематических проектов. Все это будет способствовать развитию ответственности, лидерских качеств, превращению абстрактных норм безопасности в цифровой среде во внутренне принятые ценности сообщества.

Критерии эффективности третьего модуля:

- количественные и качественные показатели активности «кибердружин» (число проведенных консультаций, созданных просветительских материалов (постов, видео), организованных мероприятий (хакатонов, квизов), охват аудитории (число просмотров, участников), экспертная оценка качества созданного контента);
- уровень вовлеченности обучающихся в созидательную (продуктивную речевую, креативную) деятельность (доля учащихся, принимавших участие в проектах модуля);
- формирование просоциальных норм (число случаев, когда обучающиеся самостоятельно реагируют на проявления цифровой неэтичности в учебных чатах (корректные напоминания о правилах, поддержка жертвы));
- изменение социального статуса темы безопасности (частота упоминаний тем кибербезопасности и цифрового этикета в неформальном общении обучающихся, школьных/вузовских медиа).

Модуль 4 – антикризисный – подразумевает оперативное психолого-педагогическое вмешательство, экстренную помощь в кризисной ситуации. Цель – минимизация последствий произошедших инцидентов и восстановление психологической безопасности. Модуль должен включать в себя четкие, известные всем сотрудникам и обучающимся образовательной организации алгоритмы действий, включающие в себя стоп-сигналы (куда и как сообщить о проблеме), действия по точ-

ной фиксации цифровых следов инцидента (скриншоты), оценку (экспресс-диагностика тяжести ситуации педагогом-психологом), помощь (комплекс мер: от беседы с агрессором до подключения правоохранительных органов). Обязательным элементом является посткризисное сопровождение пострадавшего и работа с группой, в которой произошел инцидент, для восстановления социальных связей.

Критериями эффективности данного модуля могут быть:

- скорость реагирования (время от момента фиксации инцидента до начала реализации антикризисного алгоритма, целевой показатель, например, < 1 учебного дня);

- соблюдение процедуры (доля инцидентов, при работе с которыми были корректно применены все этапы утвержденного алгоритма (фиксация, оценка, помощь));

- эффективность разрешения ситуации (прекращение травли/агрессии в адрес пострадавшего в цифровой среде, отсутствие рецидивов со стороны агрессора в отношении той же жертвы в течение фиксированного периода);

- субъективная оценка пострадавшим уровня восстановленной безопасности (опрос);

- качество посткризисного сопровождения (наличие и выполнение индивидуального плана поддержки для пострадавшего, проведение групповых восстановительных мероприятий (медиаций, обсуждений) в коллективе, где произошел инцидент, отслеживание динамики психоэмоционального состояния пострадавшего: снижение показателей тревожности, депрессивных симптомов);

- доверие к системе (число обращений обучающихся и родителей за помощью через официальные каналы (к куратору, психологу, в специальную форму) при столкновении с угрозами, в сравнении с периодами до внедрения модели).

Общим, интегральным, критерием может стать снижение количества зафиксированных и подтвержденных цифровых инцидентов (кибербуллинг, взломы, мошенничество) в расчете на 100 обучающихся за учебный год/полугодие. Данный показатель напрямую демонстрирует общий профилактический эффект от внедрения разработанной модели.

Обсуждение результатов моделирования

Предложенная модель переводит профилактику из разряда разовых мероприятий в статус непрерывного сквозного процесса, встроенного в образовательную деятельность. Её отличительными чертами являются:

- проактивность (акцент смещен с ликвидации последствий на предупреждение рисков через развитие устойчивости (резильентности) личности к цифровым угрозам;

- коллаборативность (модель предполагает совместную ответственность и деятельность всех заинтересованных сторон, участников образовательного процесса);

- этическая ориентированность (в основе лежит не запрет и контроль, а воспитание цифрового гражданства, основанного на уважении, эмпатии и критическом мышлении);

- технологическая и психологическая сбалансированность (модель не отрицает необходимости технических средств защиты (фильтры, мониторинг), но ставит во главу угла человеческий и социальный капитал).

Внедрение модели требует определённых организационных изменений, например, назначения ответственного координатора, пересмотра учебных планов, выделения ресурсов на обучение кадров.

Заключение

Цифровая образовательная среда, при всех ее дидактических преимуществах, представляет собой пространство множественных психологических рисков для личности обучающегося, наиболее распространёнными из которых являются кибербуллинг, цифровая зависимость, нарушения цифровой гигиены и эмоциональное выгорание от гиперкоммуникации. Данные риски носят системный характер и напрямую влияют на психическое благополучие и академические результаты детей и молодежи.

Существующий потенциал системы образования по профилактике данных рисков реализуется не в полной мере, что во многом обусловлено дефицитом готовности педагогических кадров. У значительной части педагогов наблюдается низкий уровень знаний в области цифровых угроз, отсутствие уверенности в процедурах вмешательства и сме-

щение ответственности на других акторов. Это указывает на острую необходимость модернизации программ педагогического образования и повышения квалификации.

В качестве системного ответа на выявленные вызовы разработана многоуровневая психолого-педагогическая модель профилактики, интегрирующая диагностический, образовательно-развивающий, социально-проектный и антикризисный модули. Ядром модели является переход от парадигмы запрета и технического контроля к парадигме развития цифровой культуры, эмпатического интеллекта и ответственного гражданства у всех участников образовательной среды. Ключевым условием успешности модели является ее целостное восприятие и реализация как части воспитательной системы и образовательной политики организации, а не как набора разрозненных мероприятий. Это требует волевых управленческих решений, ресурсного обеспечения и формирования междисциплинарных команд (педагог-психолог-IT-специалист-родитель).

Дальнейшие исследования целесообразно направить на разработку и валидизацию диагностического инструментария для оценки «цифрового благополучия» образовательной среды, а также на изучение долгосрочных эффектов внедрения подобных моделей на психологический климат в коллективе и уровень цифровой резильентности обучающихся.

Задача институтов социализации (школы, вуза и семьи) заключается не только в привитии навыков цифровой гигиены, переводе её из области абстрактных предписаний в практическую плоскость, но и развитии медиаграмотности всех участников образовательного процесса. Если цифровая гигиена обеспечивает защиту личности, то медиаграмотность выступает инструментом защиты сознания от деструктивного информационного воздействия. Современный цифровой ландшафт характеризуется высокой скоростью распространения дезинформации, пропаганды и манипулятивных техник. Исследования свидетельствуют о том, что более 80% старшеклассников не способны надежно дифференцировать рекламный и новостной контент, а 60% склонны доверять изображениям в социальных сетях без верификации источника [1]. Незрелость критического анализа информации повышает уязвимость

молодежи к манипуляциям, способствует формированию искаженных когнитивных моделей и представляет угрозу гражданской солидарности. Медиаграмотность как комплекс инструментов верификации предполагает формирование следующих ключевых навыков:

- верификация источника информации (оценка авторитетности, репутации и возможной предвзятости автора/издания, проверка домена и истории публикаций);
- перекрестная проверка информации (сопоставление данных из множества независимых источников, включая официальные отчеты и реально существующие научные публикации);
- анализ манипулятивных техник (распознавание логических ошибок, эмоционально окрашенной лексики, использования фейковых экспертов и синтетического медиаконтента (дифейки));
- понимание работы различных алгоритмов (знание принципов функционирования рекомендательных систем, формирующих «информационные пузыри»).

В практической плоскости это означает системную работу по сравнительному анализу новостных материалов, упражнения по идентификации фейков и разбор реальных кейсов. Таким образом, цифровая гигиена и медиаграмотность являются взаимодополняющими и синергетическими компонентами единой медиакомпетенции, позволяющей противостоять цифровым рискам и угрозам.

Список литературы

1. Финансовый университет. *Цифровая гигиена и безопасность: защита приватности учащихся и формирование медиаграмотности как императив современного образования* [Электронный ресурс]. URL: <https://www.fa.ru/university/structure/university/uso/press-service/press-releases/tsifrovaya-gigiena-i-bezopasnost-zashchita-privatnosti-uchashchikhsya-i-formirovanie-mediagramotnost> (дата обращения: 12.01.2026).
2. Лаборатория Касперского. (2023). *Взрослые и дети в интернете: аналитический отчет 2023* [Электронный ресурс]. URL: https://kids.kaspersky.ru/article/vzroslye_i_deti_v_internete_analiticheskiy_otchet_2023 (дата обращения: 12.01.2026).
3. Мантуленко, В. В. (2024). Информационная безопасность личности в контексте российского образования на современном этапе. *Непрерывное образование:*

- XXI век*, 2(46), с. 124–138. <https://doi.org/10.15393/j5.art.2024.9491>. EDN: <https://elibrary.ru/RDQUUZ>
4. Зезюлько, А. В. (2023). Информационная безопасность и принципы её обеспечения в образовательном процессе. *Гуманитарные и социальные науки*, 6, с. 192–200. <https://doi.org/10.18522/2070-1403-2023-101-6-192-200>. EDN: <https://elibrary.ru/NMLLDH>
 5. John, A., Glendenning, A. C., Marchant, A., Montgomery, P., Stewart, A., Wood, S., Lloyd, K., & Hawton, K. (2018). Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review. *Journal of Medical Internet Research*, 20(4), e129. <https://doi.org/10.2196/jmir.9044>
 6. Petrukhin, D. Yu. (2022). Conceptual Field of Socialization for the Digital Generation in Russia. *Государственная служба*, 24(1(135)), с. 63–69. <https://doi.org/10.22394/2070-8378-2022-24-1-63-69>. EDN: <https://elibrary.ru/TKIVMN>
 7. Zhuang, W., & Norbu, S. V. (2024). Modern Educational Instruments and Means of Digital Socialization Amid the Implementation of Modern Education in China. В: *Россия и Китай: проблемы стратегического взаимодействия: сборник Восточного центра*, 27, с. 208–211. EDN: <https://elibrary.ru/XVEWFA>
 8. Микляева, А. В. (2024). Цифровое общество и цифровая социализация: перспективы социально-психологических исследований. *Социальная психология и общество*, 15(2), с. 5–11. <https://doi.org/10.17759/sps.2024150201>. EDN: <https://elibrary.ru/BNNAQQ>
 9. Бондаренко, Т. А. (2024). Рискогенность виртуального мира Интернета в формировании жизненных практик. *Научный альманах стран Причерноморья*, 10(2), с. 13–17. <https://doi.org/10.23947/2414-1143-2024-10-2-13-17>. EDN: <https://elibrary.ru/EJEDQN>
 10. Ломовская, С. А., & Синогина, Е. С. (2024). Риски современного интернет-пространства: результаты эмпирического исследования среди студентов педагогического вуза. В: Рубцов, В. В., Сорокова, М. Г., & Радчикова, Н. П. (ред.). *Цифровая гуманитаристика и технологии в образовании (DHTE 2024): сборник статей V Международной научно-практической конференции. 14–15 ноября 2024 г.* Москва: Издательство ФГБОУ ВО МГППУ, с. 509–518. EDN: <https://elibrary.ru/EEIEOI>
 11. Ромашкина, Г. Ф., & Хузяхметов, Р. Р. (2020). Риски интернет-зависимости: структура и особенности восприятия. *Образование и наука*, 22(8), с. 108–134. <https://doi.org/10.17853/1994-5639-2020-8-108-134>. EDN: <https://elibrary.ru/RNZNMJ>
 12. Нозикова, Н. В. (2022). Актуальность и перспективы становления педагогической киберпсихологии. *Гуманизация образования*, 2, с. 90–103. <https://doi.org/10.24411/1029-3388-2020-10235>. EDN: <https://elibrary.ru/WKHKEP>

13. Плешаков, В. А. (2023). Киберпсихология: вчера, сегодня, завтра. *Номо Cyberus*, 1(14), 1.
14. Рябов, В. Б. (2024). Киберпсихология вчера, сегодня и завтра. *Институт психологии Российской академии наук. Организационная психология и психология труда*, 9(3), с. 111–133. https://doi.org/10.38098/ipran.opwp_2024_32_3_005. EDN: <https://elibrary.ru/IKEDVS>
15. Мантуленко, В. В. (2023). Информационные перегрузки российской учащейся молодёжи: миф и реальность. *Россия: общество, политика, история*, 2(7), с. 38–53. [https://doi.org/10.56654/ROPI-2023-2\(7\)-38-53](https://doi.org/10.56654/ROPI-2023-2(7)-38-53). EDN: <https://elibrary.ru/ICENCR>
16. Кудрявцев, В. Т., Майорова-Щеглова, С. Н., Милехина, Т. А., Рожков, М. И., & Попкова, Т. Д. (2024). Цифровое детство. Междисциплинарная дискуссия. *Комплексные исследования детства*, 6(2), с. 73–84. <https://doi.org/10.33910/2687-02232024-6-2-73-84>. EDN: <https://elibrary.ru/MHZAYZ>
17. Лаборатория Касперского. (2025). *Взрослые и дети в Интернете: цифровые привычки, риски и безопасность* [Электронный ресурс]. URL: https://kids.kaspersky.ru/files/2025_02_Kaspersky_kids.pdf (дата обращения: 13.01.2026).
18. Дунаевская, Э. Б. (2024). Психологическое воздействие «экранного времени» и «зелёного времени» на детей и подростков. Обзор современных исследований. *Комплексные исследования детства*, 6(1), с. 33–39. <https://doi.org/10.33910/2687-02232024-6-1-33-39>. EDN: <https://elibrary.ru/PVZDAF>
19. Уполномоченный при Президенте Российской Федерации по правам ребёнка. (н. д.). *Кибербуллинг и Хартия «Цифровая этика детства» по защите детей в цифровой среде — разговор в студии телекомпании ОТВ* [Электронный ресурс]. URL: <https://deti.gov.ru/Press-Centr/region-news/6790> (дата обращения: 13.01.2026).
20. Батеева, А. А. (2025). Осведомлённость родителей о проблеме кибербуллинга: социологический анализ. *Социология и право*, 17(4), с. 520–533. <https://doi.org/10.35854/2219-6242-2025-4-520-533>. EDN: <https://elibrary.ru/NEFSRB>
21. Президентская Академия. *FOMO — синдром упущенной выгоды: признаки, последствия, как бороться* [Электронный ресурс]. URL: <https://www.ranepa.ru/blog/obrazovanie-i-samorazvitie/fomo-sindrom-upushchennoy-vygody-priznaki-posledstviya-kak-borotsya/> (дата обращения: 13.01.2026).
22. Pylkin, A., Serkova, V., Petrov, M., & Pylkina, M. (2021). Information Hygiene as Prevention of Destructive Impacts of Digital Environment. B: Bylieva, D., Nordmann, A., Shipunova, O., & Volkova, V. (eds.). *Knowledge in the Information Society. PCSF CSIS 2020. Lecture Notes in Networks and Systems*, vol. 184. Cham: Springer, pp. 30–27. https://doi.org/10.1007/978-3-030-65857-1_4. EDN: <https://elibrary.ru/FKMORD>

23. Gupta, S., & Furnell, S. (2022). From Cybersecurity Hygiene to Cyber Well-Being. B: Moallem, A. (ed.). *HCI for Cybersecurity, Privacy and Trust. HCII 2022. Lecture Notes in Computer Science, 13333*. Cham: Springer, pp. 124–134. https://doi.org/10.1007/978-3-031-05563-8_9
24. Melo Laclote, P., Martínez-Líbano, J., Céspedes, C., Fuentealba-Urra, S., Ramírez, N. S., Lara, R. I., & Yeomans-Cabrera, M.-M. (2025). Grooming Risk Factors in Adolescents with Abuse Histories: Insights from Chilean Reparative Programs. *Adolescents*, 5(1), 3. <https://doi.org/10.3390/adolescents5010003>. EDN: <https://elibrary.ru/DZIRBZ>
25. Киселёв, К. А. (2023). Социально-психологические последствия онлайн-группинга для учебной деятельности несовершеннолетнего. В: Рубцов, В. В., Сорокова, М. Г., & Радчикова, Н. П. (ред.). *Цифровая гуманитаристика и технологии в образовании (DHTE 2023): сборник статей IV Международной научно-практической конференции. 16–17 ноября 2023 г.* Москва: Издательство ФГБОУ ВО МГППУ, с. 483–492.
26. Ионов, А. Ю., & Ким, Ю. Х.-С. (2025). Цифровая усталость в реалиях современного образования. *Современное педагогическое образование*, 6, с. 203–205. <https://doi.org/10.24412/2587-8328-2025-6-203-205>. EDN: <https://elibrary.ru/OUYCIW>

References

1. Financial University. *Digital hygiene and security: Protecting students' privacy and building media literacy as an imperative of modern education* [Electronic resource]. Retrieved January 12, 2026, from <https://www.fa.ru/university/structure/university/uso/press-service/press-releases/tsifrovaya-gigiena-i-bezopasnost-zashchita-privatnosti-uchashchikhsya-i-formirovanie-mediagramotnost>
2. Kaspersky Lab. (2023). *Adults and children on the Internet: Analytical report 2023* [Electronic resource]. Retrieved January 12, 2026, from https://kids.kaspersky.ru/article/vzroslye_i_deti_v_internete_analiticheskiy_otchet_2023
3. Mantulenko, V. V. (2024). Information security of the individual in the context of Russian education at the present stage. *Lifelong Learning: The 21st Century*, 2(46), 124–138. <https://doi.org/10.15393/j5.art.2024.9491>. EDN: <https://elibrary.ru/RDQUUZ>
4. Zezyulko, A. V. (2023). Information security and principles of its provision in the educational process. *Humanities and Social Sciences*, (6), 192–200. <https://doi.org/10.18522/2070-1403-2023-101-6-192-200>. EDN: <https://elibrary.ru/NMLLDH>
5. John, A., Glendenning, A. C., Marchant, A., Montgomery, P., Stewart, A., Wood, S., Lloyd, K., & Hawton, K. (2018). Self-harm, suicidal behaviours, and cyberbullying in children and young people: Systematic review. *Journal of Medical Internet Research*, 20(4), e129. <https://doi.org/10.2196/jmir.9044>

6. Petrukhin, D. Yu. (2022). Conceptual field of socialization for the digital generation in Russia. *Public Administration*, 24(1(135)), 63–69. <https://doi.org/10.22394/2070-8378-2022-24-1-63-69>. EDN: <https://elibrary.ru/TKIVMN>
7. Zhuang, W., & Norbu, S. V. (2024). Modern educational instruments and means of digital socialization amid the implementation of modern education in China. In V. V. Rubtsov, M. G. Sorokova, & N. P. Radchikova (Eds.), *Russia and China: Problems of Strategic Interaction: Collection of the Eastern Center*, (27), 208–211. EDN: <https://elibrary.ru/XVEWFA>
8. Miklyaeva, A. V. (2024). Digital society and digital socialization: Prospects for socio-psychological research. *Social Psychology and Society*, 15(2), 5–11. <https://doi.org/10.17759/sps.2024150201>. EDN: <https://elibrary.ru/BNNAQQ>
9. Bondarenko, T. A. (2024). Riskiness of the virtual world of the Internet in the formation of life practices. *Scientific Almanac of the Black Sea Region Countries*, 10(2), 13–17. <https://doi.org/10.23947/2414-1143-2024-10-2-13-17>. EDN: <https://elibrary.ru/EJEDQN>
10. Lomovskaya, S. A., & Sinogina, E. S. (2024). Risks of the modern Internet space: Results of an empirical study among students of a pedagogical university. In V. V. Rubtsov, M. G. Sorokova, & N. P. Radchikova (Eds.), *Digital Humanities and Technologies in Education (DHTE 2024): Proceedings of the V International Scientific and Practical Conference* (pp. 509–518). Moscow: MGPPU Publishing House. EDN: <https://elibrary.ru/EEIEOI>
11. Romashkina, G. F., & Khuzyakhmetov, R. R. (2020). Risks of Internet addiction: Structure and features of perception. *Education and Science*, 22(8), 108–134. <https://doi.org/10.17853/1994-5639-2020-8-108-134>. EDN: <https://elibrary.ru/RNZNMJ>
12. Nozikova, N. V. (2022). Relevance and prospects for the development of pedagogical cyberpsychology. *Humanization of Education*, (2), 90–103. <https://doi.org/10.24411/1029-3388-2020-10235>. EDN: <https://elibrary.ru/WKHKEP>
13. Pleshakov, V. A. (2023). Cyberpsychology: Yesterday, today, tomorrow. *Homo Cyberus*, 1(14), 1.
14. Ryabov, V. B. (2024). Cyberpsychology yesterday, today and tomorrow. *Institute of Psychology of the Russian Academy of Sciences. Organizational Psychology and Labor Psychology*, 9(3), 111–133. https://doi.org/10.38098/ipran.opwp_2024_32_3_005. EDN: <https://elibrary.ru/IKEDVS>
15. Mantulenko, V. V. (2023). Information overload among Russian student youth: Myth and reality. *Russia: Society, Politics, History*, 2(7), 38–53. [https://doi.org/10.56654/ROPI-2023-2\(7\)-38-53](https://doi.org/10.56654/ROPI-2023-2(7)-38-53). EDN: <https://elibrary.ru/ICEHCR>
16. Kudryavtsev, V. T., Mayorova-Shcheglova, S. N., Milekhina, T. A., Rozhkov, M. I., & Popkova, T. D. (2024). Digital childhood: An interdisciplinary discussion. *Comprehensive Studies of Childhood*, 6(2), 73–84. <https://doi.org/10.33910/2687-02232024-6-2-73-84>. EDN: <https://elibrary.ru/MHZAYZ>

17. Kaspersky Lab. (2025). *Adults and children on the Internet: Digital habits, risks and security* [Electronic resource]. Retrieved January 13, 2026, from https://kids.kaspersky.ru/files/2025_02_Kaspersky_kids.pdf
18. Dunaevskaya, E. B. (2024). Psychological impact of “screen time” and “green time” on children and adolescents: A review of current research. *Comprehensive Studies of Childhood*, 6(1), 33–39. <https://doi.org/10.33910/2687-02232024-6-1-33-39>. EDN: <https://elibrary.ru/PVZDAF>
19. Commissioner for Children’s Rights under the President of the Russian Federation. (n.d.). *Cyberbullying and the “Digital Ethics of Childhood” Charter for child protection in the digital environment — a discussion in the OTV TV company studio* [Electronic resource]. Retrieved January 13, 2026, from <https://deti.gov.ru/Press-Centr/region-news/6790>
20. Bateeva, A. A. (2025). Parental awareness of the cyberbullying problem: Sociological analysis. *Sociology and Law*, 17(4), 520–533. <https://doi.org/10.35854/2219-6242-2025-4-520-533>. EDN: <https://elibrary.ru/NEFSRB>
21. Presidential Academy. *FOMO — fear of missing out: Signs, consequences, and ways to cope* [Electronic resource]. Retrieved January 13, 2026, from <https://www.ranepa.ru/blog/obrazovanie-i-samorazvitie/fomo-sindrom-upushchennoy-vygody-priznaki-posledstviya-kak-borotsya/>
22. Pylkin, A., Serkova, V., Petrov, M., & Pylkina, M. (2021). Information hygiene as prevention of destructive impacts of digital environment. In D. Bylieva, A. Nordmann, O. Shipunova, & V. Volkova (Eds.), *Knowledge in the Information Society. PCSF CSIS 2020* (Lecture Notes in Networks and Systems, Vol. 184, pp. 30–27). Cham: Springer. https://doi.org/10.1007/978-3-030-65857-1_4. EDN: <https://elibrary.ru/FKMORD>
23. Gupta, S., & Furnell, S. (2022). From cybersecurity hygiene to cyber well-being. In A. Moallem (Ed.), *HCI for Cybersecurity, Privacy and Trust. HCII 2022* (Lecture Notes in Computer Science, Vol. 13333, pp. 124–134). Cham: Springer. https://doi.org/10.1007/978-3-031-05563-8_9
24. Melo Laclote, P., Martínez Libano, J., Céspedes, C., Fuentealba Urrea, S., Ramírez, N. S., Lara, R. I., & Yeomans Cabrera, M. M. (2025). Grooming risk factors in adolescents with abuse histories: Insights from Chilean reparative programs. *Adolescents*, 5(1), 3. <https://doi.org/10.3390/adolescents5010003>. EDN: <https://elibrary.ru/DZIRBZ>
25. Kiselev, K. A. (2023). Socio-psychological consequences of online grooming for the academic performance of minors. In V. V. Rubtsov, M. G. Sorokova, & N. P. Radchikova (Eds.), *Digital Humanities and Technologies in Education (DHTE 2023): Proceedings of the IV International Scientific and Practical Conference* (pp. 483–492). Moscow: MGPPU Publishing House.

26. Ionov, A. Yu., & Kim, Yu. H. S. (2025). Digital fatigue in the realities of modern education. *Modern Pedagogical Education*, (6), 203–205. <https://doi.org/10.24412/2587-8328-2025-6-203-205>. EDN: <https://elibrary.ru/OUYCIW>

ДАННЫЕ ОБ АВТОРЕ

Мантуленко Валентина Вячеславовна, кандидат педагогических наук, доцент,
доцент кафедры педагогики
Самарский национальный исследовательский университет имени академика С.П. Королёва
Московское шоссе, 34, г. Самара, 443086, Российская Федерация
mantoulenko@mail.ru

DATA ABOUT THE AUTHOR

Valentina V. Mantulenko, Ph.D. in Pedagogical Sciences, Associate Professor, Associate Professor of the Department of Pedagogy
Samara National Research University named after Academician S.P. Korolev
34, Moskovskoye Shosse, Samara, 443086, Russian Federation
mantoulenko@mail.ru
SPIN-code: 4051-7935
ORCID: <https://orcid.org/0000-0003-4333-7159>
ResearcherID: B-6624-2014
Scopus Author ID: 57191170496

Поступила 14.01.2026

После рецензирования 05.02.2026

Принята 10.02.2026

Received 14.01.2026

Revised 05.02.2026

Accepted 10.02.2026