

Цифровые образовательные среды и цифровые ресурсы в образовании / Digital Educational Environments and Digital Resources in Education

Научная статья

Original article

DOI: [10.12731/2658-4034-2026-17-1-877](https://doi.org/10.12731/2658-4034-2026-17-1-877)

EDN: [NMGHEQ](https://edn.rjep.ru/NMGHEQ)

УДК 378.14



Риски цифрового следа и кибербезопасность будущих педагогов

О.Ю. Герасимова

*Набережночелнинский государственный педагогический университет,
Набережные Челны, Российская Федерация*

Аннотация

Обоснование. Цифровизация образования привела к формированию обширного цифрового следа педагогов, включающего персональные данные учеников и их семей. Педагоги, имея доступ к ценной информации о несовершеннолетних, не обладают достаточными компетенциями для защиты собственного цифрового следа, что создает серьезные киберугрозы для всей образовательной системы. Особую опасность представляет «цифровая тень» – неконтролируемая часть данных, формирующаяся автоматически и создающая основу для таргетированных атак.

Цель – проанализировать структуру цифрового следа педагога, классифицировать связанные с ним риски и оценить готовность будущих педагогов к управлению информационной безопасностью в профессиональной деятельности.

Материалы и методы. Комплексное исследование включало теоретический анализ научной литературы по проблемам цифровизации образования и кибербезопасности, изучение нормативно-правовой базы. Эмпирическая часть реализована методом анкетирования 150 студентов четвертых курсов педагогических направлений с использованием авторского опросника.

Результаты. Выявлен критический дефицит понимания цифрового следа у будущих педагогов (38% корректное понимание), размывание границ между личным и профессиональным онлайн-пространством (68%), значительный разрыв между высокой интенсивностью использования цифровых инструментов и низкими компетенциями в области кибербезопасности. Разработана структурная классификация компонентов цифрового следа педагога.

Ключевые слова: цифровой след педагога; информационная безопасность; цифровая тень; персональные данные; киберугрозы в образовании; цифровая грамотность; подготовка педагогов

Для цитирования. Герасимова, О. Ю. (2026). Риски цифрового следа и кибербезопасность будущих педагогов. *Russian Journal of Education and Psychology*, 17(1-2), 190–209. <https://doi.org/10.12731/2658-4034-2026-17-1-877>

Digital footprint risks and cybersecurity for future teachers

O.Y. Gerasimova

*Naberezhnye Chelny State Pedagogical University, Naberezhnye Chelny,
Russian Federation*

Abstract

Background. The digitalization of education has led to the formation of an extensive digital footprint of educators, including personal data of students and their families. Teachers, having access to valuable information about minors, lack sufficient competencies to protect their own digital footprint, which creates serious cyber threats for the entire educational system. The «digital shadow» poses a particular danger – an uncontrolled portion of data that forms automatically and creates a basis for targeted attacks.

Purpose – to analyze the structure of a teacher’s digital footprint, classify associated risks, and assess the readiness of future educators to manage information security in their professional activities.

Materials and methods. The comprehensive study included theoretical analysis of scientific literature on educational digitalization and cybersecurity issues, examination of the regulatory framework. The empirical part was implemented through a survey of 150 fourth-year students in pedagogical programs using an original questionnaire.

Results. A critical deficit in understanding digital footprint among future teachers was revealed (38% correct understanding), blurring of boundaries between personal and professional online space (68%), and a significant gap between high intensity of digital tool usage and low cybersecurity competencies. A structural classification of teacher’s digital footprint components was developed.

Keywords: teacher’s digital footprint; information security; digital shadow; personal data; cyber threats in education; digital literacy; teacher training

For citation. Gerasimova, O. Y. (2026). Digital footprint risks and cybersecurity for future teachers. *Russian Journal of Education and Psychology*, 17(1-2), 190–209. <https://doi.org/10.12731/2658-4034-2026-17-1-877>

Введение

Процессы цифровизации коренным образом трансформировали образовательную среду, сделав неотъемлемой частью педагогической практики электронные журналы, системы управления обучением (LMS), облачные сервисы и мессенджеры. Эта трансформация привела к формированию принципиально нового образовательного пространства – цифрового образования, которое представляет собой «процесс взаимодействия между обучающими и обучающимися при движении от цели к результату в цифровой образовательной среде, основными средствами которой являются цифровые технологии, цифровые инструменты и цифровые следы как результаты учебной и профессиональной деятельности в цифровом формате» [1, с. 26].

Неизбежным следствием этого процесса стало формирование обширного цифрового следа каждого участника образовательных отношений. Под цифровым следом понимаются «те данные, которые оставляет пользователь при использовании конкретной информационной системы или, в более общем случае, сети Интернет» [7]. Согласно проекту «Университет 20.35», цифровой след в образовании – это «уникальный набор представленных в электронной форме данных о зафиксированных действиях, а также процессных, контекстных и иных обстоятельствах деятельности пользователя, групп пользователей или работы информационно-коммуникационных систем»» [12].

Проблематика цифрового следа привлекает внимание исследователей уже более полутора десятилетий. Американский маркетолог Тони Фиш писал о возможных опасностях цифровых следов еще в 2007 году [20]. Анализ электронного следа, по мнению Фиша, позволит выяснить, что, как и почему покупают интернет-пользователи. И не всегда эта информация может использоваться строго по исследовательскому назначению. В 2017 году венгерская исследовательница Каталин Фехер писала в своей статье о личных онлайн-стратегиях. В ней она упоминала о том, что пользователи, находясь в Интернете, оставляют очень много цифровых следов. Пользователь может о них и не помнить, но цифровые устройства сохраняют в памяти очень многие из его действий, и последствия при этом могут быть непредсказуемыми.

Фехер также подчеркивала, что «универсальные шаблоны персональных онлайн-стратегий подчинены в основном осознанным решениям, в результате чего пользователи сохраняют 70% контроль над своими цифровыми следами. Однако оставшиеся 30% действий в интернете пользователи совершают неосознанно, и это приводит к непредвиденным последствиям от кражи личных данных до похищения идентичности» [18]. Кража личных данных является одним из этапов, ведущих к краже идентичности, когда злоумышленник начинает использовать украденную информацию для совершения мошеннических действий от имени жертвы.

Особенность цифрового следа педагога заключается в его принципиальной комплексности и многосубъектности. В отличие от цифрового следа обычного пользователя, который формируется преимущественно в результате личных действий, след учителя включает информацию о третьих лицах – учениках и их родителях, коллегах, администрации школы. Более того, значительная часть этого следа создается не по собственной инициативе педагога, а в силу профессиональных обязанностей и требований образовательной системы.

Именно эта специфика превращает цифровизацию образования в палку о двух концах: наряду с очевидными преимуществами она создает новые, ранее неизвестные угрозы. Профессиональная деятельность педагога, документированная в цифровом формате, становится объектом повышенного интереса киберпреступников, что выходит далеко за рамки традиционных педагогических проблем. «При этом широкое применение информационных технологий в повседневной жизни стало не только толчком к открытию новых позитивных возможностей, но и фактором формирования нового вида преступности – киберпреступности» [10].

Актуальность исследования определяется несколькими ключевыми факторами.

Во-первых, педагог занимает уникальное положение в цифровом пространстве, которое делает его особо привлекательной мишенью для киберпреступников. С одной стороны, он обладает доступом к особо ценным данным – информации о несовершеннолетних и их се-

мьях, что представляет повышенный интерес для злоумышленников. С другой стороны, система образования требует от педагога активного цифрового присутствия через использование электронных журналов, образовательных платформ, служебных мессенджеров, но при этом не обеспечивает его адекватными компетенциями для обеспечения информационной безопасности в цифровой среде. Между тем, на сегодняшний день Российская Федерация постоянно лидирует в анти-рейтингах, связанных с кражей информации. Так, например, в 2024 г., по данным аналитиков «Positive Technologies», наша страна заняла первое место в мире по количеству объявлений о незаконной продаже баз данных организаций в Даркнете [13]. В 2023 г., согласно исследованию Росконгресса Россия заняла второе место в мире по количеству взломанных аккаунтов [11]. Компрометация педагога может иметь каскадные последствия для всей образовательной организации и ее воспитанников.

Во-вторых, наблюдается кардинальная трансформация самих киберугроз, направленных против работников образования. Если ранее доминировал примитивный массовый фишинг, который относительно легко идентифицировался, то современные методы социальной инженерии характеризуются высокой степенью персонализации и правдоподобности. Использование искусственного интеллекта для создания дипфейков и таргетированных атак, основанных на анализе профессиональной информации педагога, кардинально повышает их эффективность против образовательных работников.

В-третьих, в научной литературе и образовательной практике обнаруживается существенная лакуна в изучении проблем цифровой безопасности педагога. Несмотря на активное обсуждение цифровой грамотности, акцент традиционно делается на освоении базовых пользовательских навыков и образовательных платформ. Между тем вопросы осознанного управления профессиональным цифровым следом, анализа специфических для педагога рисков и противодействия современным методам кражи данных остаются недостаточно изученными и проработанными.

Цель исследования заключается в комплексном двухаспектном анализе проблемы цифровой безопасности современного педагога:

Теоретический аспект исследования направлен на систематизацию структуры цифрового следа педагогических работников и классификацию сопутствующих рисков, связанных с несанкционированным доступом к их персональным данным.

Эмпирический аспект – оценка готовности будущих педагогов к управлению своим цифровым следом и обеспечению информационной безопасности в профессиональной деятельности.

Интеграция теоретических и эмпирических результатов позволит определить приоритетные направления для разработки превентивных мер и модернизации программ подготовки будущих учителей в области информационной безопасности.

Правовой контекст исследования требует четкого определения границ защиты информации в педагогической деятельности. Российское законодательство (ст. 3 ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных») определяет персональные данные как «любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)». По сути, это любые сведения, позволяющие идентифицировать конкретного человека [3, с. 39], включая «фамилию, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы» и иную информацию личного характера.

Согласно действующему законодательству, организации, особенно государственного сектора, обязаны обеспечивать техническую защиту данных от несанкционированного доступа [15, с. 10]. Однако современные реалии демонстрируют, что существующие средства защиты информации зачастую оказываются неэффективными, что приводит к росту количества электронных краж персональных данных [6, с. 16].

В образовательном контексте под правовую защиту попадает обширный массив профессиональной информации педагога: от базовых паспортных данных до специфических сведений о месте работы, контактной информации из родительских чатов, фотографий с учебных и внеучебных мероприятий, а также служебной переписки. Эта многоплановость и объем защищаемых данных делают педагога особенно уязвимой категорией пользователей в цифровой среде.

Именно эта широкая интерпретация законодательства делает педагога особенно уязвимой фигурой в цифровом пространстве. Его цифровой след представляет собой сложную систему взаимосвязанных данных, включающую личную информацию, профессиональные сведения, данные об учениках и родителях, служебную переписку и методические материалы. В отличие от обычного пользователя, педагог вынужден размещать эти данные на множестве платформ не по личной инициативе, а в силу профессиональной необходимости, зачастую не имея возможности контролировать их безопасность. Это делает учителя привлекательной мишенью для киберпреступников, а компрометацию его данных – источником серьезных рисков для всей образовательной экосистемы.

Выявленная специфика цифрового следа педагога и многоплановость связанных с ним угроз обосновывают необходимость междисциплинарного исследовательского подхода, объединяющего теоретический анализ с эмпирической диагностикой готовности педагогического сообщества к решению данной проблемы.

Материалы и методы

Исследование носит комплексный характер и включает как теоретический анализ проблемы, так и эмпирическую оценку ее актуальности в педагогическом сообществе. Методология работы построена на сочетании теоретических и эмпирических методов.

На теоретическом уровне применялся анализ научной литературы по проблемам цифровизации образования и кибербезопасности, а также изучение нормативно-правовой базы, регулирующей оборот персональных данных (ФЗ № 152-ФЗ). Это позволило сформировать концептуальную рамку исследования и определить ключевые понятия.

Эмпирическая часть работы была реализована посредством метода анкетирования. Был разработан авторский опросник, направленный на изучение следующих аспектов:

- уровень осведомленности педагогов о понятии «цифровой след» и связанных с ним рисках;
- частота и цели использования цифровых инструментов в профессиональной деятельности;

- личный опыт столкновения с угрозами в цифровой среде (фишинг, кибербуллинг, утечка данных);
- оценка педагогами собственной цифровой грамотности и готовности к защите своих данных.

Выборку исследования составили 150 студентов 4 курсов педагогических направлений Набережночелнинского государственного педагогического университета. Выбор студентов 4 курса обусловлен тем, что они уже имеют опыт педагогической практики и готовятся к профессиональной деятельности. Сбор данных проводился в дистанционном формате с использованием сервиса Яндекс Формы в сентябре-октябре 2024 года.

Для обработки и анализа полученных эмпирических данных использовались методы математической статистики, включая описательную статистику для анализа распределения ответов и выявления ключевых тенденций.

Сочетание теоретического анализа и эмпирических данных позволило обеспечить комплексный подход к изучению проблемы и достоверность полученных выводов.

Результаты и обсуждения

Анализ профессиональной деятельности современного учителя показал, что его цифровой след является многокомпонентной и многоуровневой системой. В отличие от цифрового следа рядового интернет-пользователя, он формируется не только в результате личной активности, но и в значительной степени под влиянием профессиональных обязанностей.

В контексте профессиональной деятельности педагога оставляемые им цифровые данные принято классифицировать на активные и пассивные следы. Понимание этого различия является ключевым для оценки потенциальных рисков.

Активный цифровой след формируется в результате осознанных и целенаправленных действий пользователя. В случае педагога это могут быть публикации в профессиональных блогах, размещение методических материалов в социальных сетях, создание аккаунта в си-

стеме управления обучением (LMS) или участие в онлайн-форумах. Пользователь имеет возможность контролировать этот след, делая его общедоступным или закрытым. Закрытые цифровые следы «доступны только определенному кругу лиц (в пределах инфокоммуникационной сети организации, информация о посетителях веб-сайта, расположенная на конкретном сервере, и т. д.)» [5, с. 80].

Однако гораздо большую угрозу представляет пассивный цифровой след, который накапливается произвольно. Сюда относится история посещения веб-сайтов при поиске материалов к уроку, поисковые запросы, а также техническая информация об устройстве, с которого педагог работает. Например, поисковый запрос «методы пропаганды в Третьем рейхе» для подготовки к уроку истории может быть представлен как «учитель интересуется нацистской идеологией», или учитель биологии, изучающий материалы по половому воспитанию, оставляет в сети поисковые запросы, которые, будучи вырванными из контекста, могут выглядеть компрометирующе. На сегодняшний день есть много способов, посредством которых злоумышленники могут получить доступ к личной информации. Этот неконтролируемый сбор данных формирует так называемую «цифровую тень».

Речь идет о «цифровой тени», которая в отличие «от цифрового следа, создается автоматически, без согласия на то самой личности и является представителем человека в цифровом пространстве. Формируется она так же, как и цифровой след... Разница между ними в том, что цифровой след можно контролировать и изменять, а цифровую тень – нет» [4, с. 121]. Следовательно, это открытая и непреднамеренно оставленная информация, включающая «маршруты передвижений, покупки, видеозаписи камер наблюдений и т. д.».

Именно «цифровая тень» создает основные уязвимости для педагога, поскольку она предоставляет неконтролируемый доступ к персональной информации, открывая возможность для манипулирования и внешнего контроля. При этом с точки зрения объема «цифровая тень» уже превосходит «цифровой след», и «тенденция роста количества собираемой информации пугает» [14], делая проблему защиты персональных данных в образовательной среде особенно острой.

Терминологическая сложность в данной области исследований усугубляется отсутствием общепризнанных дефиниций. До сих пор понятие «цифровая идентичность» не определено. Чтобы его сформулировать нужно серьезное исследование сущности этого феномена [13]. Это создает дополнительные сложности при изучении проблематики цифрового следа педагога и разработке системы мер его защиты.

Важно отметить, что вся деятельность педагога в цифровой среде – как осознанная (цифровой след), так и непроизвольная (цифровая тень) – в совокупности приводит к созданию его детализированного «цифрового профиля», или «цифрового двойника». Это уже не просто набор разрозненных данных, а целостная виртуальная модель личности. «Развитие методов сбора, очистки и структурирования гетерогенных данных предоставляет возможность быстрого поиска информации о человеке в разных источниках и ее объединение для комплексного анализа» [2, с. 10].

Сущность этого явления раскрывает В. Н. Назаров, подчеркивая, что «облачное бытие» цифрового двойника «можно считать эквивалентом иррациональных глубин человеческой персоны... за моделью цифрового двойника стоит пользователь личного информационного пространства, который в некоем «симулятивно-творческом порыве» к информационной коммуникации создает своего «героя» информационного двойника, «сердцем» которого является персональная модель, построенная на массиве больших данных (Big Data) сумме информации, которую персона когда-либо поставила цифровому миру» [9, с. 142]. В условиях зарождающейся цифровой экономики в Российской Федерации, которая предполагает повсеместное использование big data, как и во всем мире остро стоит проблема контроля над формированием цифровой идентичности гражданина [8].

Таким образом, на основе профессиональной и личной онлайн-активности педагога формируется его цифровой аватар, который существует независимо и может быть проанализирован, спрогнозирован и, что самое опасное, использован третьими лицами без ведома и контроля самого человека. Персонализация информации ведет к тому, что крупные цифровые платформы окружают своего пользователя информационным «пузырем» [19], внутри которого демонстрируется отретушированная информационная картина мира. Это создает дополнительные риски для

педагогов, поскольку искаженное восприятие цифровой реальности может снижать их способность адекватно оценивать угрозы и принимать обоснованные решения в области информационной безопасности.

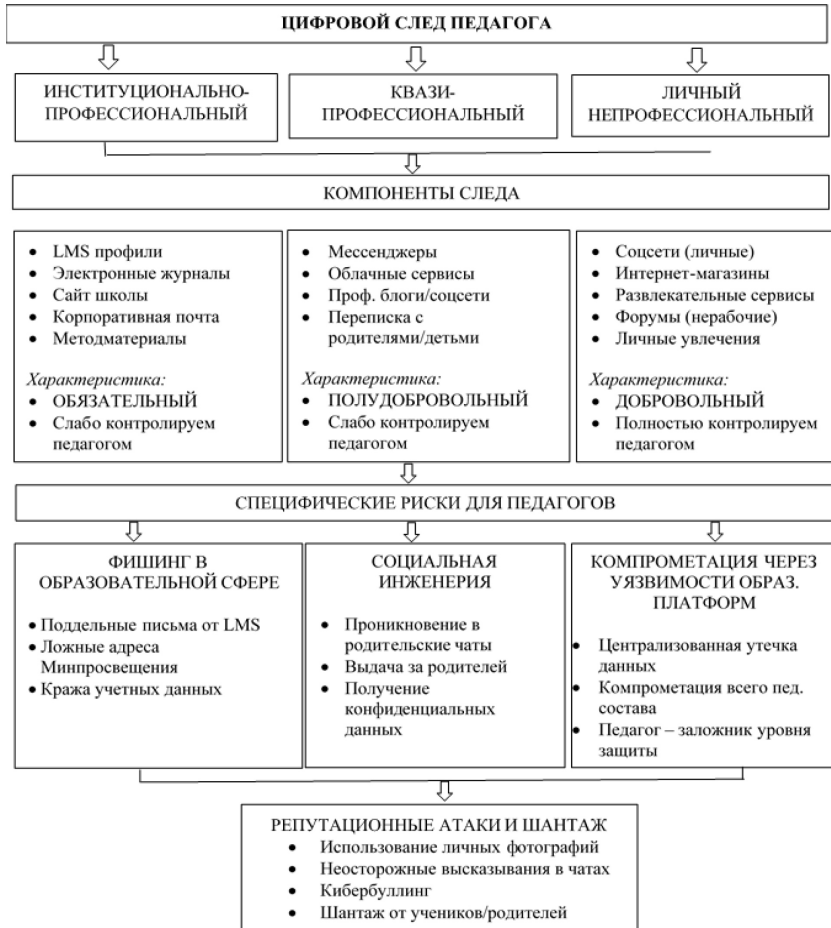


Рис. 1. Структура и классификация компонентов цифрового следа педагога

Fig. 1. Structure and classification of components of a teacher's digital footprint

Для того чтобы предметно проанализировать структуру этого сложного цифрового конструкта и оценить связанные с ним риски, необходимо декомпозировать его на составные части. На основе проведенного

анализа нами разработана структурная модель, включающая классификацию компонентов цифрового следа педагога, представленная на рисунке 1.

Для подтверждения актуальности выявленных теоретическим путем рисков и оценки готовности будущих педагогов к их минимизации было проведено эмпирическое исследование. Полученные данные позволяют соотнести теоретические концепты с реальным состоянием проблемы в педагогическом сообществе. Анализ результатов выявил следующие ключевые тенденции, представленные в табл. 1

Таблица 1.

Ключевые тенденции в области цифровой безопасности будущих педагогов**Table 1. Key Trends in Digital Security for Future Educators**

Ключевая тенденция	Количественные показатели	Качественная интерпретация
1. Дефицит комплексного понимания цифрового следа	38% - корректное понимание	Большинство будущих педагогов не рассматривают «цифровую тень» как часть своего цифрового следа, что создает слепую зону в оценке рисков
	47% - частичное понимание	
	15% - неверное понимание	
2. Размыwanie границ между личным и профессиональным цифровым пространством	96% - используют цифровые инструменты ежедневно	Смешение личного и профессионального цифрового пространства создает дополнительные риски утечки данных и снижает возможность контроля над собственным цифровым следом
	85% - применяют их как для личных, так и для профессиональных целей	
3. Высокая частота столкновения с угрозами при низкой эффективности противодействия	64% - сталкивались с угрозами в цифровой среде	Значительное число будущих педагогов уже имеет негативный опыт в цифровой среде, но недостаточно эффективно противодействует угрозам, что свидетельствует о нехватке практических навыков защиты
	41% - своевременно распознали угрозу	
4. Разрыв между общей цифровой грамотностью и специфическими навыками защиты	74% - самооценка общей цифровой грамотности	Существенный разрыв между навыками использования цифровых инструментов и компетенциями в области их безопасного применения указывает на дисбаланс в структуре цифровой грамотности будущих педагогов
	52% - самооценка готовности к защите персональных данных	
	41% - самооценка противодействия социальной инженерии	

Осведомленность о рисках, связанных с цифровым следом, также оказалась недостаточной. Большинство студентов (73%) смогли назвать не более двух потенциальных угроз, в основном ограничиваясь общими формулировками вроде «взлом аккаунта» или «кража личных данных». Более специфические риски, такие как репутационные атаки или таргетированный фишинг с использованием профессиональной информации, упоминались менее чем 20% опрошенных.

Результаты опроса показали высокую вовлеченность будущих педагогов в цифровую среду. 96% респондентов используют цифровые инструменты ежедневно, при этом 85% применяют их как для личных, так и для учебно-профессиональных целей. Наиболее популярными инструментами оказались:

- мессенджеры (WhatsApp, Telegram) – 98%;
- социальные сети – 92%;
- облачные хранилища (Google Drive, Yandex.Disk) – 89%;
- образовательные платформы (LMS университета) – 78%.

Тревожным фактором является то, что лишь 32% опрошенных четко разграничивают личные и профессиональные аккаунты в социальных сетях и мессенджерах. Подавляющее большинство (68%) используют единые учетные записи для всех сфер деятельности, что эмпирически подтверждает выявленную в теоретической части проблему размывания границ между личным и профессиональным цифровым пространством.

Критическую озабоченность вызывает тот факт, что 73% будущих педагогов не включают «цифровую тень» в структуру своего цифрового следа, формируя серьезную слепую зону при оценке потенциальных рисков. Данная проблема усугубляется феноменом, описанным в исследованиях Я. Каррьер-Суоллоу и В. Хаксара [17], которые выявили так называемый «парадокс конфиденциальности». Суть парадокса заключается в том, что при опросах люди декларируют высокую ценность конфиденциальности, однако на практике добровольно передают личные данные в обмен на минимальные удобства или символическую компенсацию. Типичным примером служит предоставление геолокационных данных в обмен на информацию о прогнозе погоды через сервисные приложения (Sinoptic, GisMeteo и др.).

Соглашаясь на установку приложения, пользователь фактически дает согласие не только на его функционирование, но и на комплексное цифровое отслеживание: определение текущего местоположения, построение маршрутов перемещения, что позволяет разработчикам аккумулировать детализированную информацию о пользователях, включая их распорядок дня, маршрут путешествий и социальную активность. Данный парадокс представляет особую опасность для педагогов, поскольку они систематически используют идентичные устройства и приложения как для личных, так и для профессиональных задач, неосознанно и бесконтролируемо расширяя свой цифровой след.

Эмпирическое исследование выявило критическую статистику: 64% респондентов лично сталкивались с различными формами цифровых угроз. Структура выявленных угроз распределилась следующим образом:

- фишинговые атаки (письма или сообщения) – 53%;
- попытки несанкционированного доступа к аккаунтам – 37%;
- неконтролируемое распространение персональной информации – 25%;
- случаи кибербуллинга – 18%.

Особую тревогу вызывает низкая эффективность противодействия угрозам: только 41% пострадавших смогли своевременно идентифицировать опасность и реализовать превентивные меры защиты. Остальные участники либо обнаруживали компрометацию постфактум, либо узнавали о нарушении безопасности от третьих лиц, что свидетельствует о критическом дефиците практических навыков цифровой самозащиты.

Анализ самооценки респондентов показал заметный разрыв между общей цифровой грамотностью и специфическими навыками защиты данных. По 10-балльной шкале средняя оценка собственной общей цифровой грамотности составила 7,4 балла, что свидетельствует о достаточно высокой уверенности будущих педагогов в своих базовых навыках работы с цифровыми инструментами.

Однако средняя оценка готовности к защите персональных данных оказалась значительно ниже – 5,2 балла. Это указывает на осознание студентами своих ограничений в области информационной безопасности. Особенно низко (в среднем 4,1 балла) была оценена готовность

противостоять современным методам социальной инженерии и таргетированным атакам.

Показательно, что 73% опрошенных выразили заинтересованность в получении дополнительных знаний и навыков по защите своего цифрового следа. При этом 68% считают, что данная тематика недостаточного освещена в рамках их профессиональной подготовки.

Сопоставление теоретических положений с результатами эмпирического исследования демонстрирует наличие системной проблемы. Выявленные в ходе анализа профессиональной деятельности педагога риски, связанные с цифровым следом, не только подтверждаются эмпирически, но и усугубляются недостаточной осведомленностью будущих учителей о данных угрозах. Особенно тревожным представляется разрыв между высокой интенсивностью использования цифровых инструментов и низким уровнем компетенций в области защиты персональных данных.

Полученные эмпирические данные убедительно подтверждают выводы теоретического анализа о наличии существенного пробела в подготовке будущих педагогов к обеспечению безопасности своего цифрового следа. Результаты свидетельствуют о необходимости усиления образовательных программ компонентами, направленными на формирование компетенций в области информационной безопасности с учетом специфики педагогической деятельности.

Заключение

Исследование позволило получить комплексное представление о проблеме цифровой безопасности современного педагога.

Установлено, что цифровой след педагога уникален из-за своей много субъектности и принудительного характера формирования. Разработана структурная классификация его компонентов (личные данные, профессиональные, данные об учениках и родителях, техническая информация). Выявлено, что наибольшую опасность представляет «цифровая тень» – неконтролируемая часть данных, создающая основу для таргетированных атак.

Обнаружен критический дефицит понимания своего цифрового следа у будущих педагогов (лишь 38% понимают его корректно). Выявлен разрыв между высоким уровнем использования цифровых инструментов и низки-

ми компетенциями в кибербезопасности. Установлено, что 68% будущих педагогов смешивают личные и профессиональные аккаунты, а 64% сталкивались с киберутрозами при низкой эффективности противодействия.

Научная новизна заключается в разработке концепции цифрового следа педагога как многосубъектной системы, включающей неконтролируемую «цифровую тень», и создании структурной классификации его компонентов. Получены новые данные о критическом разрыве между цифровой активностью будущих педагогов и их компетенциями в области кибербезопасности.

Практическая значимость состоит в создании основы для модернизации подготовки педагогических кадров в области цифровой безопасности. Результаты могут использоваться при разработке методических рекомендаций, образовательных программ и превентивных мер защиты в образовательной среде.

Выводы и рекомендации:

1. Модернизация подготовки педагогов предполагает необходимость дополнения образовательных программ специализированными модулями по цифровой безопасности.

2. Непрерывное образование требует разработки целенаправленных программ повышения квалификации для действующих педагогов в области информационной безопасности.

3. Организационно-технические меры должны включать формирование культуры информационной безопасности в образовательных организациях на системном уровне.

4. Нормативная база нуждается в создании специализированных стандартов по защите цифрового следа в сфере образования с учетом специфики педагогической деятельности.

Проблема защиты цифрового следа педагога требует системного решения, объединяющего усилия научного сообщества, органов управления образованием и самих педагогов.

Список литературы

1. Вайндорф-Сысоева, М. Е., & Субочева, М. Л. (2018). «Цифровое образование» как системообразующая категория: подходы к определению. *Вестник Московского государственного областного университета. Серия: Педагогика*, (3),

- с. 25–36. <https://doi.org/10.18384/2310-7219-2018-3-25-36>. EDN: <https://elibrary.ru/YLRDRB>
2. Гайдаш, О. В. (2020). Феномен цифрового следа в современном обществе. *Вестник магистратуры*, (6), с. 10–12. EDN: <https://elibrary.ru/OEACVB>
3. Григонис, В. П. (2022). Конституционные поправки, принятые в 2020 году, как фактор, повышающий безопасность государства. *Право. Безопасность. Чрезвычайные ситуации*, (3), с. 39–44. EDN: <https://elibrary.ru/KEWNXE>
4. Дорохина, Р. В., & Лаврёнов, С. В. (2021). Этические проблемы цифровизации в системе образования. *Век глобализации*, (2), с. 118–123. EDN: <https://elibrary.ru/WHXMNL>
5. Зайцева, С. А., & Смирнов, В. А. (2021). Аксиологический подход к понятию цифрового следа. *Ноосферные исследования*, (3), с. 79–87. <https://doi.org/10.46724/NOOS.2021.3.79-87>. EDN: <https://elibrary.ru/LZGMVY>
6. Кайнов, В. И. (2024). Историко-правовые аспекты становления института административной юстиции в России. *Право. Безопасность. Чрезвычайные ситуации*, (3), с. 16–22. <https://doi.org/10.61260/2074-1626-2024-3-16-22>. EDN: <https://elibrary.ru/QSNZTR>
7. Касперский. *Что такое цифровой след? Как защитить его от злоумышленников*. URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-a-digital-footprint>
8. Кондаков, А. М., & Костылева, А. А. (2019). Цифровая идентичность, цифровая самоидентификация, цифровой профиль: постановка проблемы. *Вестник Российского университета дружбы народов. Серия: Информатизация образования*, (3), с. 207–218. <https://doi.org/10.22363/2312-8631-2019-16-3-207-218>. EDN: <https://elibrary.ru/JFIWJJ>
9. Назаров, В. Н. (2020). Цифровой двойник как субъект информационной этики. *Этическая мысль*, (1), с. 142–154. <https://doi.org/10.21146/2074-4870-2020-20-1-142-154>. EDN: <https://elibrary.ru/ZONAYB>
10. Никуленко, А. В., Бозиев, Т. О., Милюков, С. Ф. и др. *Уголовное право. Общая часть: учебник*. Санкт-Петербург: Издательство РГПУ им. А. И. Герцена. 424 с. URL: <https://www.iprbookshop.ru/137279.html>
11. РИА Новости. *В 2023 г., согласно исследованию Росконгресса, Россия заняла второе место в мире по количеству взломанных аккаунтов*. URL: <https://ria.ru/20240731/rossija-1963062182.html>
12. Ромащенко, А. Р. (2024). Цифровой след обучения как способ фиксации вторичных учебных текстов в результате смыслового чтения учащимися средней школы. *Russian Journal of Education and Psychology*, 15(3), с. 157–179. <https://doi.org/10.12731/2658-4034-2024-15-3-583>. EDN: <https://elibrary.ru/AEEZFH>
13. *Россия стала лидером по количеству слитых данных*. URL: https://www.rbc.ru/technology_and_media/30/07/2024/66a894cc9a79470efe2b8e2d

14. CNews. *Человечество накрыла цифровая тень*. URL: http://www.cnews.ru/news/top/chelovechestvo_nakryla_tsifrovaya_ten
15. Шевченко, К. В. (2023). Государство как социальный институт. *Аграрное и земельное право*, (7), с. 10–12. https://doi.org/10.47643/1815-1329_2023_7_10. EDN: <https://elibrary.ru/QCQZWQ>
16. Шнейдер, Л. Б., & Сыманюк, В. В. (2017). Пользователь в информационной среде: цифровая идентичность сегодня. *Психологические исследования*, 10(52), с. 7. <https://doi.org/10.54359/ps.v10i52.392>. EDN: <https://elibrary.ru/ZIPADX>
17. Carrière-Suollow, Yan, & Haksar, Vikram. (2019). *The Economics and Implications of Data: An Integrated Perspective*. International Monetary Fund. Сентябрь. 46 с.
18. Feher, K. (2021). Digital Identity and the Online Self: Footprint Strategies – An Exploratory and Comparative Research Study. *Journal of Information Science*, 47(2), pp. 192–205. <https://doi.org/10.1177/0165551519879702>. EDN: <https://elibrary.ru/ULISRF>
19. Pariser, E. (2011). *The Filter Bubble: What the Internet Is Hiding from You*. New York: Penguin Press. 294 с.
20. Tony, F. (2009). *My Digital Footprint: A Two-Sided Digital Business Model Where Your Privacy Will Be Someone Else's Business!* Futuretext. URL: <https://www.amazon.co.uk/My-Digital-Footprint-Two-sided-Business/dp/0955606985>

References

1. Vaindorf-Sysoeva, M. E., & Subocheva, M. L. (2018). “Digital education” as a system-forming category: Approaches to definition. *Bulletin of the Moscow State Regional University. Series: Pedagogy*, (3), 25–36. <https://doi.org/10.18384/2310-7219-2018-3-25-36>. EDN: <https://elibrary.ru/YLRDRB>
2. Gaidash, O. V. (2020). The phenomenon of the digital footprint in modern society. *Bulletin of Magistracy*, (6), 10–12. EDN: <https://elibrary.ru/OEACVB>
3. Grigonis, V. P. (2022). Constitutional amendments adopted in 2020 as a factor enhancing state security. *Law. Security. Emergency Situations*, (3), 39–44. EDN: <https://elibrary.ru/KEWNXE>
4. Dorokhina, R. V., & Lavryonov, S. V. (2021). Ethical issues of digitalization in the education system. *Age of Globalization*, (2), 118–123. EDN: <https://elibrary.ru/WHXMNL>
5. Zaitseva, S. A., & Smirnov, V. A. (2021). Axiological approach to the concept of digital footprint. *Noospheric Research*, (3), 79–87. <https://doi.org/10.46724/NOOS.2021.3.79-87>. EDN: <https://elibrary.ru/LZGMVY>
6. Kainov, V. I. (2024). Historical and legal aspects of the formation of the institute of administrative justice in Russia. *Law. Security. Emergency Situations*, (3), 16–22. <https://doi.org/10.61260/2074-1626-2024-3-16-22>. EDN: <https://elibrary.ru/QSNZTR>

7. Kaspersky. *What is a digital footprint? How to protect it from attackers*. Retrieved from <https://www.kaspersky.ru/resource-center/definitions/what-is-a-digital-footprint>
8. Kondakov, A. M., & Kostyleva, A. A. (2019). Digital identity, digital self-identification, digital profile: Problem statement. *Bulletin of the Peoples' Friendship University of Russia. Series: Informatization of Education*, (3), 207–218. <https://doi.org/10.22363/2312-8631-2019-16-3-207-218>. EDN: <https://elibrary.ru/JFIWJJ>
9. Nazarov, V. N. (2020). Digital twin as a subject of information ethics. *Ethical Thought*, (1), 142–154. <https://doi.org/10.21146/2074-4870-2020-20-1-142-154>. EDN: <https://elibrary.ru/ZONAYB>
10. Nikulenko, A. V., Boziev, T. O., Milyukov, S. F., et al. (n.d.). *Criminal law. General part: Textbook*. Saint Petersburg: Publishing House of the Herzen State Pedagogical University of Russia. 424 p. Retrieved from <https://www.iprbookshop.ru/137279.html>
11. RIA Novosti. (2023). *In 2023, according to a Roscongress study, Russia ranked second in the world in the number of hacked accounts*. Retrieved from <https://ria.ru/20240731/rossija-1963062182.html>
12. Romashchenko, A. R. (2024). Digital learning footprint as a way to record secondary educational texts resulting from meaningful reading by secondary school students. *Russian Journal of Education and Psychology*, 15(3), 157–179. <https://doi.org/10.12731/2658-4034-2024-15-3-583>. EDN: <https://elibrary.ru/AEEZFH>
13. RBC. (2024). *Russia became the leader in the amount of leaked data*. Retrieved from https://www.rbc.ru/technology_and_media/30/07/2024/66a894cc9a79470efe2b8e2d
14. CNews. (20xx). *Humanity is covered by a digital shadow*. Retrieved from http://www.cnews.ru/news/top/chelovechestvo_nakryla_tsifrovaya_ten
15. Shevchenko, K. V. (2023). The state as a social institution. *Agrarian and Land Law*, (7), 10–12. https://doi.org/10.47643/1815-1329_2023_7_10. EDN: <https://elibrary.ru/QCQZWQ>
16. Shneider, L. B., & Symanyuk, V. V. (2017). User in the information environment: Digital identity today. *Psychological Research*, 10(52), 7. <https://doi.org/10.54359/ps.v10i52.392>. EDN: <https://elibrary.ru/ZIPADX>
17. Carrière Suollow, Y., & Haksar, V. (2019). *The economics and implications of data: An integrated perspective*. International Monetary Fund. September. 46 p.
18. Feher, K. (2021). Digital identity and the online self: Footprint strategies – An exploratory and comparative research study. *Journal of Information Science*, 47(2), 192–205. <https://doi.org/10.1177/0165551519879702>. EDN: <https://elibrary.ru/ULISRF>
19. Pariser, E. (2011). *The filter bubble: What the internet is hiding from you*. New York: Penguin Press. 294 p.
20. Tony, F. (2009). *My digital footprint: A two-sided digital business model where your privacy will be someone else's business!* Futuretext. Retrieved from <https://www.amazon.co.uk/My-Digital-Footprint-Two-sided-Business/dp/0955606985>

ДАННЫЕ ОБ АВТОРЕ

Герасимова Ольга Юрьевна, кандидат педагогических наук, доцент, доцент кафедры информатики и вычислительной математики
Набережночелнинский государственный педагогический университет
ул. Низаметдинова, 28, г. Набережные Челны, 423806, Российская Федерация
gerola1970@mail.ru

DATA ABOUT THE AUTHOR

Olga Y. Gerasimova, Ph.D. in Education, Associate Professor, Department of Computer Science and Computational Mathematics
Naberezhnye Chelny State Pedagogical University
28, Nizametdinov Str., Naberezhnye Chelny, 423806, Russian Federation
gerola1970@mail.ru
SPIN-code: 6130-9350
ORCID: <https://orcid.org/0000-0002-9934-2750>

Поступила 26.09.2025

После рецензирования 05.10.2025

Принята 11.10.2025

Received 26.09.2025

Revised 05.10.2025

Accepted 11.10.2025