

УДК 004.056:378

<https://doi.org/10.33619/2414-2948/129/53>

ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ

©**Куват кызы К.**, ORCID: 0009-0000-1248-1081, Ошский технологический университет им. М. М. Адышева, г. Ош, Кыргызстан, kanysh.1993aa@gmail.com

©**Жумабек кызы М.**, ORCID: 0009-0004-0034-0045, Ошский технологический университет им. М. М. Адышева, г. Ош, Кыргызстан, meerim.minu@gmail.com

©**Анищенко Ю. В.**, ORCID: 0009-0005-4430-9047, SPIN-код: 7511-0543, канд. техн. наук, Ошский технологический университет им. М. М. Адышева, г. Ош, Кыргызстан, yulya.anishchenko.85@mail.ru

ISSUES OF PERSONAL DATA PROTECTION IN THE DIGITAL EDUCATIONAL ENVIRONMENT

©**Kuvat kyzy K.**, ORCID: 0009-0000-1248-1081, Osh Technological University named after M. Adyshev, Osh, Kyrgyzstan, kanysh.1993aa@gmail.com

©**Zhumabek kyzy M.**, ORCID: 0009-0004-0034-0045, Osh Technological University named after M. Adyshev, Osh, Kyrgyzstan, meerim.minu@gmail.com

©**Anishchenko Yu.**, ORCID: 0009-0005-4430-9047, SPIN-code: 7511-0543, Ph.D., Osh Technological University named after M. Adyshev, Osh, Kyrgyzstan, yulya.anishchenko.85@mail.ru

Аннотация. Рассматриваются проблемы защиты персональных данных в цифровой образовательной среде на примере использования электронных журналов, LMS-платформ, систем дистанционного обучения и облачных сервисов. Актуальность исследования обусловлена тем, что цифровизация образования сопровождается увеличением объема собираемых и обрабатываемых данных обучающихся, включая идентификационные сведения, контактную информацию, результаты обучения, данные о посещаемости и активности на образовательных платформах. Целью работы является анализ правовых, организационных, технических и поведенческих аспектов защиты персональных данных, а также оценка уровня осведомленности обучающихся о цифровых рисках. В исследовании использованы методы анализа нормативных, методических и научных документов, сравнительно-правового анализа, анкетирования, описательной статистики и процентного анализа. Эмпирическую основу составили результаты пилотного опроса 34 обучающихся 1 и 2 курсов направлений «Программная инженерия» и «Информационная безопасность». Результаты исследования позволили выявить основные проблемные зоны. Сделан вывод о необходимости комплексного подхода, сочетающего нормативное регулирование, технические меры защиты, организационные меры и систематическое повышение цифровой грамотности участников образовательного процесса.

Abstract. This study examines the problems of personal data protection in the digital educational environment through the examples of electronic journals, LMS platforms, distance learning systems, and cloud services. The relevance of the study is determined by the fact that the digitalization of education is accompanied by an increase in the volume of collected and processed student data, including identification information, contact details, learning outcomes, attendance records, and activity data on educational platforms. The aim of the study is to analyze the legal, organizational, technical, and behavioral aspects of personal data protection, as well as to assess

students' awareness of digital risks. The research employs methods including the analysis of regulatory, methodological, and scientific documents, comparative legal analysis, a questionnaire survey, descriptive statistics, and percentage analysis. The empirical basis of the study consists of the results of a pilot survey of 34 first- and second-year students majoring in Software Engineering and Information Security. The results demonstrate that the main problem areas are password reuse, insufficient awareness of the types of personal data collected by digital educational platforms, limited ability to recognize phishing threats, and uncertainty regarding the procedure for responding to suspected data leakage or account compromise. The study concludes that a comprehensive approach is required, combining a regulatory framework, technical protection measures, organizational measures, and the systematic improvement of digital literacy among participants in the educational process.

Ключевые слова: персональные данные, защита информации, цифровая образовательная среда, LMS-платформы, кибербезопасность, цифровая грамотность.

Keywords: personal data, information protection, digital educational environment, LMS platforms, cybersecurity, digital literacy.

Цифровизация образования сопровождается активным внедрением электронных журналов, LMS-платформ, систем дистанционного обучения, облачных сервисов и иных цифровых инструментов. Эти средства расширяют доступ к образованию, упрощают управление учебным процессом и обеспечивают оперативное взаимодействие между преподавателями, обучающимися и администрацией. Одновременно возрастает объем собираемых и обрабатываемых персональных данных, включая идентификационные сведения, контактные данные, результаты обучения, информацию о посещаемости и иные сведения, относящиеся к личности обучающихся и работников образовательной организации.

В Кыргызской Республике вопросы защиты персональных данных и цифровой безопасности приобрели особую актуальность в связи с развитием национального цифрового законодательства. Ранее правовые основы обработки персональных данных регулировались Законом КР «Об информации персонального характера», однако с 6 февраля 2026 г. данный закон утратил силу в связи с введением в действие Цифрового кодекса Кыргызской Республики. В настоящее время регулирование отношений в цифровой среде осуществляется с учетом положений Цифрового кодекса КР, а также требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства КР от 21 ноября 2017 г. №760 [1].

Дополнительное значение имеет Закон КР «О кибербезопасности Кыргызской Республики», определяющий правовые основы единой системы кибербезопасности и направленный на обеспечение цифровой устойчивости информационной инфраструктуры страны [2].

На международном уровне одним из ключевых ориентиров выступает Общий регламент Европейского союза по защите данных — GDPR, закрепляющий принципы законности, прозрачности, минимизации данных и ответственности оператора за их защиту [3].

В методическом плане важное значение имеют NIST Privacy Framework, ориентированный на управление рисками приватности на уровне организации, а также рекомендации UNESCO ИТЕ по защите персональных данных и приватности в онлайн-обучении [4, 5].

Актуальность проблемы подтверждается и современными исследованиями, в которых подчеркивается, что цифровая образовательная среда создает не только технические, но и организационные, правовые и поведенческие риски, связанные с обработкой данных обучающихся в LMS-платформах и онлайн-сервисах [6, 7, 10].

Несмотря на наличие нормативной и методической базы, в образовательной практике сохраняются проблемы, связанные с человеческим фактором: использованием одинаковых паролей для разных сервисов, слабой осведомленностью о фишинговых угрозах, передачей учетных данных третьим лицам и недостаточным пониманием порядка обработки персональных данных в цифровых образовательных сервисах. Особенно актуальной эта проблема становится в условиях онлайн-обучения, где обучающиеся, преподаватели и администрация ежедневно взаимодействуют с платформами, аккумулирующими значительные объемы учебной, идентификационной и поведенческой информации [5, 8, 9].

Цель исследования заключается в анализе проблем защиты персональных данных в цифровой образовательной среде и оценке уровня осведомленности обучающихся о связанных с этим рисках.

Материал и методы исследования

Исследование проводилось на базе образовательной программы Кибербезопасность и программная инженерия Ошского технологического университета им. М. М. Адышева, Кыргызская Республика. В пилотном анкетировании приняли участие 34 обучающихся 1 и 2 курсов направлений Программная инженерия и Информационная безопасность. Для сбора эмпирических данных использовался анонимный опрос, направленный на выявление уровня осведомленности респондентов по вопросам защиты персональных данных в цифровой образовательной среде.

Анкета включала 10 вопросов закрытого типа и была сгруппирована по нескольким тематическим блокам: частота использования цифровых образовательных платформ, практика использования паролей, применение двухфакторной аутентификации, опыт столкновения с подозрительными сообщениями и ссылками, способность распознавать признаки фишинга, знание принципов обработки персональных данных в LMS, ознакомленность с правилами безопасного использования цифровых сервисов, знание порядка действий при подозрении на утечку данных или взлом учетной записи, а также самооценка уровня знаний в области защиты персональных данных.

Обработка результатов осуществлялась с применением методов описательной статистики и процентного анализа. Теоретико-методологическую основу исследования составили нормативные, методические и научные источники по вопросам защиты персональных данных, кибербезопасности, цифрового образования и онлайн-обучения [1–12].

В работе применялись методы анализа нормативных и методических документов, сравнительно-правового анализа, анкетирования, систематизации научных источников, а также количественной обработки результатов опроса.

Результаты и обсуждение

Результаты пилотного опроса 34 обучающихся показали, что цифровые образовательные платформы активно используются в учебном процессе. Ежедневно ими пользуются 44,1% респондентов, ещё 38,2% используют такие платформы несколько раз в неделю. Таким образом, более 80% участников опроса регулярно взаимодействуют с цифровыми образовательными сервисами, что подтверждает актуальность вопросов защиты персональных данных в образовательной среде.

Одним из наиболее выраженных поведенческих рисков является повторное использование паролей. По результатам анкетирования, 52,9% респондентов указали, что используют один и тот же пароль для нескольких цифровых сервисов. Еще 29,4% делают это иногда. Следовательно, 82,3% обучающихся допускают повторное использование паролей хотя бы в отдельных случаях. Такая практика повышает риск компрометации учетных записей при утечке данных одного из используемых сервисов.

Использование двухфакторной аутентификации оказалось достаточно распространенным: 70,6% респондентов сообщили, что применяют данный механизм защиты. Вместе с тем 23,5% обучающихся не используют двухфакторную аутентификацию, а 5,9% указали, что не знают, что это такое. Это показывает, что, несмотря на наличие положительной практики у большинства участников, часть обучающихся по-прежнему не применяет дополнительные средства защиты учетных записей.

На вопрос о столкновении с подозрительными сообщениями, письмами или ссылками, связанными с учебными аккаунтами или образовательными платформами, 41,2% респондентов дали положительный ответ. При этом 44,1% сообщили, что не сталкивались с подобными ситуациями, а 14,7% затруднились ответить. Полученные данные показывают, что значительная часть обучающихся уже имела опыт взаимодействия с потенциально опасными цифровыми сообщениями.

Способность распознавать признаки фишинговых сообщений и поддельных ссылок нельзя признать достаточной. Только 38,2% респондентов указали, что уверенно распознают такие признаки. Еще 38,2% сообщили, что делают это частично, а 23,5% не умеют распознавать признаки фишинга. Следовательно, у большинства участников опроса навыки выявления фишинговых угроз сформированы неполностью.

Ограниченной остается и остается и осведомленность обучающихся о составе персональных данных, собираемых и обрабатываемых цифровыми образовательными платформами. Только 26,5% респондентов указали, что знают, какие данные о них обрабатываются. 47,1% выбрали вариант «частично», а 26,5% сообщили, что не знают этого. Это свидетельствует о том, что значительная часть обучающихся использует цифровые образовательные сервисы без полного понимания того, какие персональные данные собираются, хранятся и обрабатываются.

Отдельного внимания требует практика передачи учетных данных другим лицам. 14,7% респондентов сообщили, что передавали свой логин и пароль от образовательной платформы другому человеку, еще 8,8% указали, что делали это иногда. В совокупности 23,5% обучающихся допускали передачу учетных данных хотя бы в отдельных случаях. Такая практика противоречит базовым требованиям цифровой безопасности и создает риск несанкционированного доступа к учебной и персональной информации.

При этом 50% респондентов указали, что ознакомлены с правилами безопасного использования цифровых образовательных сервисов в учебном заведении. Еще 44,1% знакомы с такими правилами частично, и только 5,9% сообщили, что не ознакомлены с ними. Это означает, что формальное информирование обучающихся в определенной степени присутствует, однако оно не всегда переходит в устойчивые безопасные практики.

Проблемным является и порядок реагирования на инциденты. Только 38,2% обучающихся знают, куда обращаться в случае подозрения на утечку данных или взлом учебной учетной записи. 41,2% не знают порядка обращения, а 20,6% не уверены в своих действиях. При инцидентах информационной безопасности такой пользователь является существенным риском, поскольку своевременное уведомление ответственных лиц напрямую влияет на скорость локализации угрозы.

Самооценка уровня знаний по вопросам защиты персональных данных в цифровой среде также подтверждает необходимость дальнейшей работы в этом направлении. Большинство участников — 64,7% — оценили свой уровень как средний. Высокий уровень отметили 23,5%, низкий — 11,8%. Следовательно, обучающиеся в целом осознают наличие определенных знаний, однако эти знания не всегда являются достаточными для уверенного и безопасного поведения в цифровой образовательной среде.

Таблица

РЕЗУЛЬТАТЫ ПИЛОТНОГО ОПРОСА ОБУЧАЮЩИХСЯ

<i>Показатель</i>	<i>Доля респондентов, %</i>
Используют цифровые образовательные платформы ежедневно	44,1
Используют цифровые образовательные платформы несколько раз в неделю	38,2
Используют один и тот же пароль для нескольких цифровых сервисов	52,9
Иногда используют один и тот же пароль для нескольких цифровых сервисов	29,4
Используют двухфакторную аутентификацию	70,6
Не используют двухфакторную аутентификацию	23,5
Не знают, что такое двухфакторная аутентификация	5,9
Сталкивались с подозрительными сообщениями, письмами или ссылками	41,2
Уверенно распознают признаки фишинга	38,2
Частично распознают признаки фишинга	38,2
Знают, какие персональные данные собирают образовательные платформы	26,5
Частично, знают, какие персональные данные собирают образовательные платформы	47,1
Передавали логин и пароль другому человеку	14,7
Иногда передавали логин и пароль другому человеку	8,8
Ознакомлены с правилами безопасного использования цифровых образовательных сервисов	50
Частично ознакомлены с правилами безопасного использования цифровых образовательных сервисов	44,1
Знают, куда обращаться при подозрении на утечку данных или взлом аккаунта	38,2
Не знают, куда обращаться при подозрении на утечку данных или взлом аккаунта	41,2
Не уверены, куда обращаться при подозрении на утечку данных или взлом аккаунта	20,6
Оценивают свой уровень знаний как высокий	23,5
Оценивают свой уровень знаний как средний	64,7
Оценивают свой уровень знаний как низкий	11,8

Таблица содержит обобщенные результаты пилотного опроса по основным вопросам анкеты. Она позволяет оценить частоту использования цифровых образовательных платформ, распространенность отдельных практик цифровой безопасности, уровень осведомленности обучающихся о защите персональных данных и готовность респондентов к действиям при возможных инцидентах.

Для наглядного выделения наиболее значимых проблемных зон на Рисунке представлены основные поведенческие риски, выявленные по результатам пилотного опроса. В отличие от таблицы, рисунок отражает не все результаты анкетирования, а обобщенные показатели риска, сформированные на основе объединения близких по смыслу ответов.

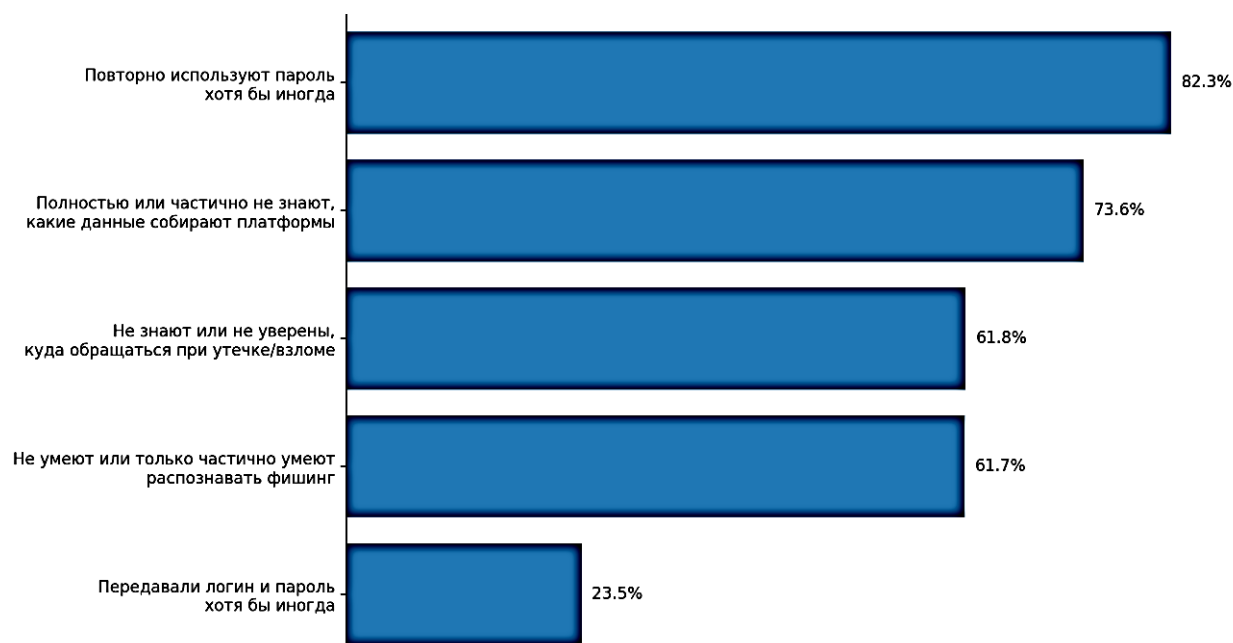


Рисунок. Основные поведенческие риски защиты персональных данных в цифровой образовательной среде

Как видно из Рисунка, наиболее выраженным поведенческим риском является повторное использование паролей: 82,3% респондентов указали, что используют один и тот же пароль для нескольких цифровых сервисов постоянно или хотя бы иногда. Существенной проблемой также является недостаточная осведомленность обучающихся о составе персональных данных, собираемых цифровыми образовательными платформами: 73,6% участников опроса либо не знают этого, либо владеют данной информацией лишь частично. Кроме того, значительная часть респондентов не обладает достаточными навыками противодействия цифровым угрозам. Так, 61,7% обучающихся не умеют распознавать признаки фишинга либо делают это только частично, а 61,8% не знают или не уверены, куда следует обращаться в случае подозрения на утечку данных или взлом учетной записи. Даже сравнительно распространенная, но значимая по последствиям практика передачи логина и пароля другим лицам была выявлена у 23,5% респондентов.

Полученные результаты показывают, что проблема защиты персональных данных в цифровой образовательной среде определяется не только техническими угрозами, но и поведенческими особенностями пользователей. Даже при наличии нормативных требований, технических средств защиты и международных методических подходов значительная часть рисков формируется на уровне повседневных пользовательских практик. Это согласуется с риск-ориентированным подходом, отраженным в NIST Privacy Framework, где защита персональных данных рассматривается как непрерывный процесс выявления, оценки и снижения рисков приватности [4].

Выявленные поведенческие риски также соотносятся с рекомендациями UNESCO ИТЕ по защите персональных данных в онлайн-обучении. В них подчеркивается необходимость обучения пользователей безопасной работе с цифровыми образовательными платформами, повышения прозрачности обработки данных и формирования ответственного отношения к цифровой приватности [5].

Для образовательных организаций это означает, что защита персональных данных не может ограничиваться только технической настройкой информационных систем. Сопоставление результатов опроса с современными исследованиями показывает, что

аналогичные проблемы характерны и для других систем высшего образования. В научной литературе отмечается, что образовательные платформы и онлайн-сервисы аккумулируют значительные объемы данных об обучающихся, при этом сами пользователи нередко недостаточно понимают, какие данные собираются, как они обрабатываются и кто может иметь к ним доступ [6, 7, 10].

Таким образом, результаты пилотного исследования подтверждают, что ключевыми уязвимым звеном является не только инфраструктура, но и недостаточно сформированная культура безопасного обращения с персональными данными. Повышение уровня защищенности требует сочетания правовых, организационных, технических и образовательных мер: регламентации доступа, информирования обучающихся о порядке обработки данных, внедрения двухфакторной аутентификации, регулярного обучения по вопросам фишинга и закрепления понятного порядка действий при подозрении на утечку данных или взлом учетной записи.

Выводы

Проведенное исследование показало, что защита персональных данных в цифровой образовательной среде требует комплексного подхода, сочетающего правовые, организационные, технические и образовательные меры. Использование LMS-платформ, электронных журналов, облачных сервисов и других цифровых инструментов расширяет возможности образовательного процесса, но одновременно повышает риски, связанные с обработкой персональных данных обучающихся.

Результаты пилотного опроса подтвердили, что значительная часть рисков связана не только с техническими уязвимостями, но и с поведением самих пользователей. Наиболее проблемными зонами являются повторное использование паролей, недостаточная осведомленность о составе собираемых персональных данных, неполная готовность к распознаванию фишинговых угроз и неуверенность обучающихся в порядке действий при возможной утечке данных или взломе учетной записи.

Следовательно, повышение уровня защиты персональных данных в образовательной организации должно включать регулярное информирование обучающихся, обучение безопасной работе с цифровыми сервисами, внедрение двухфакторной аутентификации, профилактику передачи учетных данных третьим лицам и разработку понятного алгоритма реагирования на инциденты. Перспективой дальнейшего исследования является расширение выборки и оценка эффективности конкретных мероприятий по повышению цифровой грамотности участников образовательного процесса.

Источники:

(1). Постановление Правительства Кыргызской Республики от 21 ноября 2017 г. № 760 «Об утверждении Требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных»: <https://www.gov.kg/ru/npa/s/679>

(2). Закон Кыргызской Республики от 17 июля 2024 г. №121 «О кибербезопасности Кыргызской Республики». <https://cert.gov.kg/ru/legislation/>

(3). 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, and Repealing Directive 95/46/EC (General Data Protection Regulation). <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

Список литературы:

1. Enterprise I. P. T. NIST privacy framework: a tool for improving privacy through enterprise risk management. 2020. <https://doi.org/10.6028/NIST.CSWP.01162020>
2. Huang R. H., Liu D. J., Zhu L. X., Chen H. Y., Yang J. F., Tlili A., Wang S. F. Personal data and privacy protection in online learning: Guidance for students, teachers and parents // Beijing: Smart Learning Institute of Beijing Normal University. 2020. P. 109.
3. Ulven J. B., Wangen G. A systematic review of cybersecurity risks in higher education // Future Internet. 2021. V. 13. №2. P. 39. <https://doi.org/10.3390/fi13020039>
4. Alier M., Casañ Guerrero M. J., Amo D., Severance C., Fonseca D. Privacy and e-learning: A pending task // Sustainability. 2021. V. 13. №16. P. 9206. <https://doi.org/10.3390/su13169206>
5. Jiang X., Goh T. T., Liu M. On students' willingness to use online learning: A privacy calculus theory approach // Frontiers in Psychology. 2022. V. 13. P. 880261. <https://doi.org/10.3389/fpsyg.2022.880261>
6. Majeed M., Ghani U., Meng W. Privacy concerns and online learning of postgraduate students through the lens of stimulus–organism–response model // Sustainability. 2022. V. 14. №18. P. 11604. <https://doi.org/10.3390/su141811604>
7. Dowell M. L., Greenhalgh S. P. Information flow solipsism in canvas: An exploration of student privacy awareness // The Internet and Higher Education. 2025. V. 65. P. 100989. <https://doi.org/10.1016/j.iheduc.2024.100989>
8. Фечина Л. А., Селезнева И. Г., Батурина Л. А., Воробьева Г. В., Сухова А. С. Защита персональных данных в системе образования // Право и государство: теория и практика. 2025. №5. С. 348-350. https://doi.org/10.47643/1815-1337_2025_5_348
9. Параскевов А. В., Каденцева А. А., Филоненко М. В. Защита персональных данных в информационных обучающих системах // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2016. №122. С. 1085-1098. <https://doi.org/10.21515/1990-4665-122-075>

References:

1. Enterprise, I. P. T. (2020). NIST privacy framework: a tool for improving privacy through enterprise risk management. <https://doi.org/10.6028/NIST.CSWP.01162020>.
2. Huang, R. H., Liu, D. J., Zhu, L. X., Chen, H. Y., Yang, J. F., Tlili, A., ... & Wang, S. F. (2020). Personal data and privacy protection in online learning: Guidance for students, teachers and parents. *Beijing: Smart Learning Institute of Beijing Normal University*, 109.
3. Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, 13(2), 39. <https://doi.org/10.3390/fi13020039>
4. Alier, M., Casañ Guerrero, M. J., Amo, D., Severance, C., & Fonseca, D. (2021). Privacy and e-learning: A pending task. *Sustainability*, 13(16), 9206. <https://doi.org/10.3390/su13169206>
5. Jiang, X., Goh, T. T., & Liu, M. (2022). On students' willingness to use online learning: A privacy calculus theory approach. *Frontiers in Psychology*, 13, 880261. <https://doi.org/10.3389/fpsyg.2022.880261>
6. Majeed, M., Ghani, U., & Meng, W. (2022). Privacy concerns and online learning of postgraduate students through the lens of stimulus–organism–response model. *Sustainability*, 14(18), 11604. <https://doi.org/10.3390/su141811604>
7. Dowell, M. L., & Greenhalgh, S. P. (2025). Information flow solipsism in canvas: An exploration of student privacy awareness. *The Internet and Higher Education*, 65, 100989. <https://doi.org/10.1016/j.iheduc.2024.100989>

8. Fechina, L. A., Selezneva, I. G., Baturina, L. A., Vorob'eva, G. V., & Sukhova, A. S. (2025). Zashchita personal'nykh dannykh v sisteme obrazovaniya. *Pravo i gosudarstvo: teoriya i praktika*, (5), 348-350. (in Russian). https://doi.org/10.47643/1815-1337_2025_5_348

9. Paraskevov, A. V., Kadentseva, A. A., & Filonenko, M. V. (2016). Zashchita personal'nykh dannykh v informatsionnykh obuchayushchikh sistemakh. *Politematicheskii setevoi elektronnyi nauchnyi zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta*, (122), 1085-1098. (in Russian). <https://doi.org/10.21515/1990-4665-122-075>

Поступила в редакцию
20.05.2026 г.

Принята к публикации
26.05.2026 г.

Ссылка для цитирования:

Куват кызы К., Жумабек кызы М., Анищенко Ю. В. Проблемы защиты персональных данных в цифровой образовательной среде // Бюллетень науки и практики. 2026. Т. 12. №8. С. 452-460. <https://doi.org/10.33619/2414-2948/129/53>

Cite as (APA):

Kuvat kyzy, K., Zhumabek kyzy, M., & Anishchenko, Yu. (2026). Issues of Personal Data Protection in the Digital Educational Environment. *Bulletin of Science and Practice*, 12(8), 452-460. (in Russian). <https://doi.org/10.33619/2414-2948/129/53>