ТЕХНИЧЕКИЕ НАУКИ
TECHNICAL SCIENCES

Научная статья

УДК 004.056

Кирилл Павлович Колпаков[1], Вячеслав Евгеньевич Новиков[2], Владимир Александрович Устюгов[3]

[1, 2, 3] Сыктывкарский государственный университет имени Питирима Сорокина, Сыктывкар, Россия

[1] zadose442094@yandex.ru,2 slivanov8787@gmail.com, 3 ustyugov@syktsu.ru

Информационная безопасность электронной образовательной среды вуза: риски и пути их преодоления

Аннотация. *Электронная информационно-образовательная среда (ЭИОС) является ключевым элементом современного университета, обеспечивающим реализацию образовательных программ, организацию учебного процесса и хранение данных студентов. Однако расширение использования цифровых технологий сопровождается ростом рисков, связанных с обеспечением информационной безопасности. В статье рассматриваются основные угрозы ЭИОС, классифицированные на технические, организационные и угрозы низкой осведомленности. Отдельное внимание уделено источникам рисков: уязвимостям программных платформ, пробелам нормативного регулирования, недостаточной цифровой грамотности участников образовательного процесса. На основе анализа предложены пути их преодоления, включающие внедрение современных средств защиты информации, разработку локальной нормативной базы вуза и формирование культуры информационной безопасности у студентов и преподавателей. Комплексное применение этих мер позволит снизить вероятность инцидентов, обеспечить устойчивость образовательной среды и повысить доверие к электронным сервисам университета.*

Ключевые слова: *информационная безопасность, электронная образовательная среда, вуз, риски, угрозы, защита данных, цифровая культура*

Для цитирования: Колпаков К. П., Новиков В. Е., Устюгов В. А. Информационная безопасность электронной образовательной среды вуза: риски и пути их преодоления // Молодежный научный вестник СГУ им. Питирима Сорокина. 2025. № 2. С. 7–15. URL: https://mnv.syktsu.ru/

Article

Kirill P. Kolpakov[1], Vladislav E. Novikov[2], Vladimir A. Ustyugov[3]
[1, 2, 3] Pitirim Sorokin Syktyvkar State University, Syktyvkar, Russia
[1] zadose442094@yandex.ru,[2] slivanov8787@gmail.com, [3] ustyugov@syktsu.ru

Information security of the university's electronic educational environment: risks and ways to overcome them

Abstract. *The electronic educational environment (EEE) is a key component of a modern university, providing the implementation of educational programs, the organization of the learning process, and the storage of students' data. However, the growing use of digital technologies is accompanied by an increase in risks related to information security. The article examines the main threats to the EEE, classified into technological, organizational, and awareness-related threats. Particular attention is paid to the sources of risks: vulnerabilities of software platforms, gaps in regulatory frameworks, and insufficient digital literacy of participants in the educational process. Based on the analysis, ways to overcome these risks are proposed, including the introduction of modern information security tools, the development of a university's local regulatory framework, and the formation of an information security culture among students and teachers. The comprehensive application of these measures will reduce the likelihood of incidents, ensure the resilience of the educational environment, and increase trust in the university's electronic services.*

Keywords: *information security, electronic educational environment, university, risks, threats, data protection, digital culture*

For citation: Kolpakov K. P., Novikov V. E., Ustyugov V. A. Information security of the university,s electronic educational environment: risks and ways to overcome them. *Molodezhnyj nauchnyj vestnik SGU im. Pitirima Sorokina* [Youth scientific bulletin Pitirim Sorokin Syktyvkar State University]. 2025. No 2. Pp. 7–15. URL: https://mnv.syktsu.ru/

Введение. С недавнего времени университетская электронная информационно-образовательная среда (ЭИОС), в состав которой входит система управления обучением — Learning Management System (LMS), является важнейшим вспомогательным элементом для реализации образовательных программ — через нее обеспечиваются доступ к учебным планам и рабочим программам дисциплин, проведение занятий и аттестации — как промежуточной в виде контрольных работ, так и итоговой в виде тестов, хранение результатов обучения и взаимодействие между участниками образовательного процесса. Требования к составу и

функциям ЭИОС закреплены в Постановлении Правительства РФ от 11.10.2023 № 1678, статье 16 Закона об Образовании в РФ, № 273-ФЗ от 29.12.2012: ЭИОС должна обеспечивать доступ к образовательным ресурсам, фиксацию результатов и иные сервисы, критичные для учебного процесса.

Одновременно с расширением спектра функций ЭИОС растут риски, связанные с соблюдением образовательной организацией правовых норм, установленных регулирующими органами. Нарушение ряда из них может повлечь серьезные последствия. Обработка персональных данных обучающихся и сотрудников в LMS, системах прокторинга (технологиях дистанционного контроля за процессом прохождения экзаменов и тестирований с применением видеонаблюдения и специализированного программного обеспечения) и облачных сервисах подчинена требованиям Федерального закона № 152-ФЗ «О персональных данных» и иных подзаконных нормативных актов, требующих законность и безопасность обработки информации, назначение ответственного и принятие организационно-технических мер защиты. Регулирующий орган регулярно публикует разъяснения и рекомендации по снижению рисков утечек и инцидентов (назначение ответственного, физический контроль доступа, локальные акты, взаимодействие с подрядными организациями) [1].

На уровне государственной стратегии актуальность защиты ЭИОС подтверждается Доктриной информационной безопасности РФ (Указ Президента РФ от 05.12.2016 № 646), где вузовский сегмент рассматривается как часть национального информационного пространства и, следовательно, требует устойчивой защиты [3].

Практика показывает, что профильные риски ЭИОС включают: уязвимости компонентов LMS (в т. ч. Moodle), ошибки интеграции в информационную сеть образовательной организации, недостаточный мониторинг действий пользователей, а также риски, связанные с прокторингом, а именно объемом собираемых данных (в т. ч. биометрия, обработка видео, управление поставщиками услуг прокторинга). Современные исследования наглядно указывают на необходимость системной оценки защищенности компонентов LMS вплоть до анализа программного кода, а также осознанного выбора и эксплуатации прокторинговых решений с приоритетом защиты данных [7].

В этой работе мы систематизируем риски ЭИОС вуза и предлагаем практико-ориентированный набор мер их преодоления на трех уровнях:

1) нормативно-организационном (политики, роли, локальные акты, проверка этапов обработки по 152-ФЗ),

2) техническом (контроль уязвимостей LMS, безопасная архитектура сети и журналирование каждого пользователя, взаимодействие с подрядными организациями),

3) профилактическом (формирование цифровой гигиены и культуры ИБ у студентов и профессорско-преподавательского состава, регламенты использования прокторинга).

Такой подход позволяет соотнести требования закона с реальной практикой эксплуатации ЭИОС, что в конечном счете позволит повысить качество и устойчивость образовательного процесса в целом.

Риски электронной образовательной среды вуза: классификация и источники. Электронная информационно-образовательная среда стала обязательным элементом университетской инфраструктуры — именно через нее организуются онлайн-занятия, в ней хранится информация о результатах обучения и обеспечивается взаимодействие студентов и преподавателей. Согласно требованиям Минобрнауки России, ЭИОС должна гарантировать доступ к учебным планам, рабочим программам дисциплин, расписанию, образовательным ресурсам и обеспечивать фиксацию результатов обучения [2]. Таким образом, сбои в ее работе или недостаточная защищенность становятся не только риском кратковременного прекращения доступа ко всем материалам, хранящимся в ЭИОС, но и прямым фактором, влияющим на качество образовательного процесса [2; 4].

Анализ современного состояния ЭИОС в российских вузах показывает, что риски можно условно разделить на три основные группы: технические, организационные и риски, связанные с низкой осведомленностью участников образовательного процесса [6].

1. Технические риски. К техническим рискам относятся уязвимости программных платформ управления обучением (например, Moodle, Blackboard), перебои в работе серверов, недостаточная защищенность каналов связи. В последние годы фиксировались инциденты, когда сбои LMS приводили к срыву экзаменационных сессий и задержке выдачи результатов. Утечки персональных данных студентов и преподавателей также становятся заметной проблемой: Роскомнадзор регулярно сообщает о росте числа нарушений, связанных с обработкой данных в образовательных организациях.

2. Организационные риски. К организационным рискам относятся пробелы в локальной нормативной базе вузов, несоответствие требованиям Федерального закона «О персональных данных» № 152-ФЗ, а также слабый контроль подрядчиков, предоставляющих облачные сервисы и системы прокторинга. Отсутствие четких регламентов обработки данных студентов создает угрозу не только для информационной безопасности, но и для репутации вуза. Кроме того, значительная часть университетов сталкивается с проблемой недостаточного финансирования ИТ-инфраструктуры, что напрямую отражается на возможности своевременного обновления средств защиты.

3. Риски, связанные с низкой осведомленностью участников образовательного процесса. Особую роль играет человеческий фактор — низкий уровень цифровой грамотности студентов и преподавателей, пренебрежение правилами безопасности (использование слабых паролей, хранение данных в открытом виде, общий доступ к аккаунтам). Эти риски могут проявляться в форме успешного фишинга в отношении студентов или преподавателей, несанкционированного доступа к учебным материалам или потери данных. Важно отметить, что формирование цифровой культуры вуза напрямую влияет на устойчивость ЭИОС к подобным угрозам.

Таким образом, источниками рисков выступают как технические сбои и уязвимости программного обеспечения, так и организационные недоработки и недостаточная цифровая культура участников образовательного процесса. Их совокупность делает электронную образовательную среду одной из наиболее уязвимых составляющих современного университета.

Пути преодоления рисков электронной образовательной среды вуза. Эффективная защита электронной образовательной среды вуза требует системного подхода, сочетающего технические, организационные и профилактические меры по повышению уровня осведомленности. Только при их комплексной реализации можно обеспечить устойчивую работу инфраструктуры и сохранить доверие участников образовательного процесса (см. табл.).

Таблица

Пути преодоления рисков ЭИОС

Меры	***Реализация***
1	*2*
Технические меры	– регулярное обновление платформ управления обучением и их компонентов, установка патчей безопасности;

Окончание табл.

1	*2*
Технические меры	– использование современных средств защиты информации: антивирусного ПО, межсетевых экранов, систем обнаружения вторжений; – резервное копирование образовательных данных и настройка механизмов восстановления в случае сбоев; – защита каналов связи при помощи специализированных протоколов с шифрованием данных, особенно при дистанционном доступе преподавателей и студентов; – внедрение систем централизованного мониторинга событий безопасности (SIEM), позволяющих выявлять инциденты безопасности в режиме реального времени [5]
Организационные меры	– разработка и утверждение локальных актов по обработке персональных данных и обеспечению ИБ ЭИОС в соответствии с требованиями 152-ФЗ; – назначение ответственного за информационную безопасность и проведение регулярных аудитов защищенности; – четкая регламентация работы с подрядчиками, предоставляющими облачные и прокторинговые сервисы, включая требования по безопасности и ответственность сторон; – формирование долгосрочной стратегии развития ИТ-инфраструктуры вуза, предусматривающей обновление оборудования и программных решений; – включение вопросов информационной безопасности в систему управления качеством образования и аккредитационные процедуры [5]
Профилактические	– проведение регулярных обучающих семинаров для студентов и преподавателей по вопросам защиты данных и правил работы в ЭИОС; – интеграция элементов цифровой гигиены в образовательные программы, включая дисциплины по основам информационной безопасности; – разработка инструкций и памяток по безопасному использованию LMS, систем прокторинга и облачных сервисов; – создание системы мотивации студентов к ответственному использованию образовательной среды (например, через участие в конкурсах и кибертренировках) [5]

Таким образом, устойчивое развитие электронной образовательной среды вуза возможно только при комплексном применении технических средств защиты, организационно-правовом регулировании каждого действия и педагогических подходов к повышению уровня осведомленности. Только комплексный подход

позволит снизить вероятность инцидентов, обеспечить соблюдение требований законодательства и сформировать у студентов и преподавателей ответственное отношение к вопросам информационной безопасности.

Заключение. Электронная информационно-образовательная среда сегодня является неотъемлемой частью функционирования современного университета. Она обеспечивает доступ к учебным материалам, взаимодействие преподавателей и студентов, хранение результатов обучения и организацию образовательного процесса.

Проведенный анализ показал, что наибольшие угрозы связаны с уязвимостями программных платформ и сетевой инфраструктуры, недостаточной проработкой локальной нормативной базы вузов и низкой цифровой грамотностью участников образовательного процесса. Эти риски напрямую отражаются на качестве образования, репутации учебного заведения и доверии студентов.

Пути их преодоления требуют комплексного подхода — внедрения современных сертифицированных средств защиты информации и механизмов мониторинга; разработки и соблюдения локальных актов, регламентирующих работу ЭИОС; повышения уровня осведомленности студентов и преподавателей. Только при сочетании технических, организационных и профилактических мер возможно устойчивое развитие университетской образовательной среды, соответствующее требованиям законодательства и вызовам современности.

Список источников

1. О персональных данных : федеральный закон от 27.07.2006 № 152-ФЗ (в ред. от 04.08.2023). Доступ из справ.-правовой системы «КонсультантПлюс», 2025.

2. Об утверждении порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения и дистанционных образовательных технологий : приказ Минобрнауки РФ от 05.04.2017 № 301. Доступ из справ.-правовой системы «КонсультантПлюс», 2025.

3. Доктрина информационной безопасности Российской Федерации, утв. Указом Президента РФ от 05.12.2016 № 646. Доступ из справ.-правовой системы «КонсультантПлюс», 2025.

4. Зуфарова А. С. Информационная безопасность в образовательном процессе // Молодой ученый. 2022. № 12 (406). С. 55–58.

5. Леонова И. И. Формирование культуры информационной безопасности студентов в условиях электронной образовательной среды // Образование и безопасность. 2021. № 4. С. 25–31.

6. Проталинский О. М., Ажмухамедов И. М. Информационная безопасность вуза // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. 2009. № 1. С. 18–23.

7. Роскомнадзор. Отчет о состоянии защиты персональных данных в образовательных организациях за 2022 год. URL: https://rkn.gov.ru (дата обращения: 09.09.2025).

References

1. *O personal'nyh dannyh : federal'nyj zakon ot 27.07.2006 № 152-FZ (v red. ot 04.08.2023)* [On Personal Data : federal Law of 27.07.2006 No 152-FZ (as amended on 04.08.2023)]. (In Russ.)

2. *Ob utverzhdenii poryadka primeneniya organizaciyami, osushchestvlyayushchimi obrazovatel'nuyu deyatel'nost', elektronnogo obucheniya i distancionnyh obrazovatel'nyh tekhnologij : prikaz Minobrnauki RF ot 05.04.2017 № 301* [On approval of the procedure for the use of e-learning and distance learning technologies by educational organizations : order of the Ministry of Education and Science of the Russian Federation of 05.04.2017 No 301]. (In Russ.)

3. *Doktrina informacionnoj bezopasnosti Rossijskoj Federacii, utv. Ukazom Prezidenta RF ot 05.12.2016 № 646* [Doctrine of Information Security of the Russian Federation, approved by the Decree of the President of the Russian Federation of 05.12.2016 No 646]. (In Russ.)

4. Zufarova A. S. Information security in the educational process. *Molodoy Ucheny* [Young scientist], 2022, no 12 (406), pp. 55–58. (In Russ.)

5. Leonova I. I. Formation of students' information security culture in the context of the electronic educational environment. *Obrazovanie i Bezopasnost* [Education and safety], 2021, no 4, pp. 25–31. (In Russ.)

6. Protalinskiy O. M., Azhmukhamedov I. M. Information security of institute of higher education. *Vestnik AGTU. Seriya: Upravlenie, Vychislitelnaya Tekhnika i Informatika* [ASTU Bulletin. Series: Management, Computer Engineering, and Informatics], 2009, no 1, pp. 18–23. (In Russ.)

7. *Roskomnadzor. Otchet o sostoyanii zashchity personal'nyh dannyh v obrazovatel'nyh organizaciyah za 2022 god* [Report on the state of personal data protection in educational organizations for 2022]. Available at: https://rkn.gov.ru (accessed 09.09.2025). (In Russ.)

Информация об авторах

Колпаков Кирилл Павлович, магистрант 2-го курса направления подготовки «Педагогическое образование». Профиль: «Искусственный интеллект и цифровая среда образовательной организации», СГУ им. Питирима Сорокина» (Россия, 167001, г. Сыктывкар, Октябрьский пр., д. 55)

Новиков Вячеслав Евгеньевич, студент 1-го курса бакалавриата по направлению подготовки «Информационная безопасность». Профиль: «Техническая защита безопасности», СГУ им. Питирима Сорокина» (Россия, 167001, г. Сыктывкар, Октябрьский пр., д. 55)

Устюгов Владимир Александрович, кандидат физико-математических наук, доцент, заведующий кафедрой информационной безопасности, СГУ им. Питирима Сорокина» (Россия, 167001, г. Сыктывкар, Октябрьский пр., д. 55)

Information about the authors

Kirill P. Kolpakov, a 2nd year Master's student, field of study "Pedagogical Education", profile "Artificial Intelligence and Digital Educational Environment of the Organization", Pitirim Sorokin Syktyvkar State University (55, Oktyabrsky ave., Syktyvkar, 167001, Russia)

Vyacheslav E. Novikov, a 1st year undergraduate student, field of study "Information Security", Pitirim Sorokin Syktyvkar State University (55, Oktyabrsky ave., Syktyvkar, 167001, Russia)

Vladimir A. Ustyugov, candidate of Physical and Mathematical Sciences, Associate Professor, Head of the Department of Information Security, Pitirim Sorokin Syktyvkar State University, Syktyvkar, Russia,

Вклад авторов

Колпаков К. П. — сбор и анализ материала, разработка структуры статьи, написание основного текста, формулировка выводов.

Новиков В. Е. — участие в сборе информации, анализ образовательных практик, подготовка справочных данных.

Устюгов В. А. — научное руководство, определение методологии, редактура текста.

Contribution of the authors

Kolpakov K. P. — collection and analysis of materials, development of the article structure, writing of the main text, formulation of conclusions.

Novikov V. E. — participation in data collection, analysis of educational practices, preparation of reference materials.

Ustyugov V. A. — scientific supervision, definition of methodology, text editing.

Поступила в редакцию: 20.09.2025
Одобрена после рецензирования: 01.11.2025
Принята к публикации: 10.11.2025