

УДК 004.056:37

DOI: 10.34670/AR.2026.78.15.023

Выявление и преодоление проблем информационной безопасности в образовании

Алкесов Руслан Темботович

Кандидат социологических наук, доцент,
кафедра административного и уголовного права,
Майкопский государственный технологический университет,
385000, Российская Федерация, Майкоп, ул. Первомайская, 191;
e-mail: alkesov55@mail.ru

Аннотация

В статье автор рассматривает актуальные проблемы информационной безопасности в образовательной среде и предлагает пути их преодоления. Проанализированы ключевые угрозы, характерные для образовательных учреждений: кибератаки, фишинг, социальная инженерия, а также внутренние риски, обусловленные человеческим фактором. Особое внимание уделено типичным уязвимостям ИТ-инфраструктуры — недостаточной защите сетевых ресурсов, слабостям удалённого доступа, использованию устаревшего программного обеспечения. Предложен системный подход к обеспечению информационной безопасности, включающий комплекс мер — от регулярного обновления ПО и внедрения средств мониторинга до формирования культуры безопасности посредством обучения и тренингов. Подчёркнута необходимость баланса между защитой данных и сохранением доступности образовательных ресурсов, а также учёта нормативно-правовых требований. Результаты исследования могут быть полезны руководителям образовательных организаций, специалистам по информационной безопасности и администраторам ИТ-систем при разработке и совершенствовании политик защиты информации.

Для цитирования в научных исследованиях

Алкесов Р.Т. Выявление и преодоление проблем информационной безопасности в образовании // Вопросы российского и международного права. 2026. Том 16. № 7А. С. 203-207. DOI: 10.34670/AR.2026.78.15.023

Ключевые слова

Информационная безопасность, образование, киберугрозы, человеческий фактор, защита данных, цифровая грамотность, ИТ-инфраструктура, фишинг, политика информационной безопасности, киберустойчивость.

Введение

Развитие информационной безопасности в образовании – это непрерывный процесс, требующий постоянного совершенствования и адаптации к новым вызовам и угрозам. Только системный и стратегический подход, основанный на анализе текущего состояния, современных технологиях и лучших практиках, сможет обеспечить надежную защиту данных и создать безопасную образовательную среду для всех участников образовательного процесса.

Основная часть

Алкесов Р.Т. полагает, что «в современном образовательном пространстве информационная безопасность становится все более актуальной задачей, поскольку образовательные учреждения активно используют цифровые технологии для организации учебного процесса, хранения и обработки данных студентов, преподавателей и административного персонала. Однако, с ростом цифровизации возрастает и количество угроз, способных нанести значительный ущерб информационной инфраструктуре образовательных учреждений. Основными угрозами являются кибератаки, внутренние инциденты, технические сбои и человеческий фактор». [Алкесов, 2026, с.207]

Частые случаи нарушений безопасности в образовательных учреждениях свидетельствуют о том, что, несмотря на внедрение современных технологий защиты информации, многие организации сталкиваются с повторяющимися проблемами, которые ставят под угрозу конфиденциальность данных и стабильность работы систем. Одной из наиболее распространенных причин нарушений является человеческий фактор. Сотрудники и студенты зачастую не обладают достаточной осведомленностью о мерах информационной безопасности, что приводит к ошибкам, неправильному обращению с данными и игнорированию правил безопасности. Например, использование слабых паролей, их повторное применение на различных ресурсах или хранение паролей в открытом виде увеличивают риск несанкционированного доступа к системам.

Из-за низкой цифровой грамотности или элементарной неосторожности пользователи нередко передают свои учётные данные злоумышленникам: достаточно перейти по фишинговой ссылке или скачать вредоносное приложение, чтобы сеть учреждения оказалась под угрозой.

Угрозы изнутри – одна из самых непростых задач в защите информации в учебных заведениях. Далеко не каждый сотрудник или студент понимает, насколько важно беречь данные и следовать правилам. Порой информация утекает из-за случайной ошибки или намеренного действия пользователя. Если права доступа настроены небрежно, а за действиями внутри системы почти не следят, риск происшествий заметно растёт. Например, сотрудники, обладающие избыточными правами, могут случайно или намеренно удалить важные файлы или изменить настройки систем, что негативно сказывается на работе учреждения. Внутренние угрозы также связаны с использованием неподдерживаемого или устаревшего программного обеспечения, которое не получает своевременных обновлений и патчей, что делает системы уязвимыми для атак.

Еще одной частой причиной нарушений является недостаточная защита сетевой инфраструктуры. В образовательных учреждениях зачастую используются открытые или недостаточно защищенные Wi-Fi сети, что создает возможности для перехвата данных злоумышленниками. Отсутствие должной сегментации сети, неэффективные средства проверки подлинности пользователей и незашифрованный обмен данными существенно расширяют

поверхность атаки. Следствием этого становится риск перехвата конфиденциальной информации, получения злоумышленниками доступа к корпоративным ресурсам, кражи персональных данных, а также компрометации инфраструктуры через вредоносное ПО.

Проблема недостаточной защищённости удалённого и мобильного доступа остаётся одной из значимых в системе информационной безопасности образовательной среды. Активное использование личных устройств в рамках дистанционной работы и обучения сопряжено с повышенными рисками: отсутствие надлежащих средств защиты и своевременного обновления ПО на таких устройствах формирует уязвимости, которые могут быть использованы для проникновения в корпоративные информационные системы. Отсутствие многофакторной аутентификации, слабая защита VPN и отсутствие контроля за удалёнными подключениями увеличивают вероятность проникновения вредоносных программ и утечки данных.

Фишинговые атаки и социальная инженерия остаются одними из наиболее распространённых методов взлома систем. Одним из распространённых векторов атак выступают фишинговые письма, стилизованные под легитимную переписку с администрацией или контрагентами учреждения. Посредством таких сообщений злоумышленники стремятся получить доступ к персональным данным пользователей или обеспечить внедрение вредоносного ПО. Результатом успешных атак становится нарушение целостности учётных записей и проникновение в корпоративную инфраструктуру, сопряжённое с риском разглашения охраняемой информации.

В процессе внедрения систем информационной безопасности в образовательных учреждениях часто сталкиваются с рядом проблем и сложностей, которые затрудняют достижение поставленных целей и требуют особого внимания со стороны руководства и специалистов. Одной из основных проблем является недостаточная осведомлённость и культура безопасности среди сотрудников и студентов. Многие пользователи не осознают важности соблюдения правил информационной безопасности, что приводит к пренебрежению мерами защиты, использованию слабых паролей, переходу по сомнительным ссылкам и другим ошибкам, создающим уязвимости в системе. Отсутствие систематического обучения и регулярных тренингов способствует тому, что даже при наличии технических средств защиты, уровень человеческого фактора остается высоким риском для безопасности.

Ещё одной сложностью является недостаточное финансирование и ресурсы, выделяемые на обеспечение информационной безопасности. В условиях ограниченного бюджета образовательные учреждения зачастую вынуждены ограничиваться минимальными мерами, что снижает эффективность защиты данных. Недостаток средств мешает внедрению современных технологий, обновлению программного обеспечения, проведению регулярных аудитов и сертификаций, а также привлечению квалифицированных специалистов в области информационной безопасности. В результате, системы защиты могут устаревать, а уязвимости оставаться неустранёнными, что увеличивает риск успешных кибератак.

Особую проблему представляет недостаточная интеграция мер информационной безопасности в общую стратегию развития учреждения. В некоторых случаях вопросы защиты информации рассматриваются как отдельная функция, не связанная с основными бизнес-процессами и образовательной деятельностью. Это ведет к тому, что меры безопасности реализуются фрагментарно, без учета специфики образовательной среды и требований к доступности и удобству использования систем. Такой подход зачастую вызывает сопротивление со стороны сотрудников и студентов, которые воспринимают меры защиты как неудобство или ограничение их деятельности.

Скорость технологического развития и изменчивость киберугроз формируют комплекс

технических вызовов. Поддержание актуального уровня защищённости требует регулярной актуализации защитных механизмов и их адаптации к трансформирующимся угрозам. При этом значительная часть образовательных учреждений испытывает нехватку профильных специалистов и компетенций, что препятствует своевременному выявлению и нейтрализации уязвимостей. Отсутствие внутренней команды специалистов или высокая стоимость привлечения внешних экспертов создает дополнительные препятствия для поддержания системы безопасности на должном уровне.

В образовательной среде важна доступность информации для студентов и преподавателей, а чрезмерные ограничения могут привести к снижению эффективности учебного процесса. Слабость реализуемых мер защиты формирует потенциальные угрозы утечки конфиденциальной информации, что критически важно в контексте соблюдения законодательства о персональных данных. Обеспечение гармоничного сочетания требований безопасности и пользовательского удобства – сложный процесс, требующий персонализированных решений и систематического мониторинга.

Значительные сложности возникают при внедрении автоматизированных систем оценки уязвимостей и мониторинга безопасности. Эти системы требуют высокой квалификации специалистов для их настройки и интерпретации результатов. Нередко возникают ситуации, когда автоматические отчеты о слабых местах системы игнорируются или неправильно интерпретируются, что снижает эффективность профилактических мер. Кроме того, автоматизация может сталкиваться с техническими ограничениями инфраструктуры, несовместимостью программных решений и недостаточной интеграцией с существующими системами.

Обновление программного обеспечения: часто уязвимости появляются из-за устаревшего программного обеспечения. Поэтому важно регулярно обновлять все программные компоненты, включая операционные системы, приложения, библиотеки и фреймворки. Разработчики выпускают обновления, которые исправляют уязвимости в программном обеспечении, поэтому необходимо следить за обновлениями и устанавливать их вовремя. [Хромова, Петросян, 2023, с. 68]

Заключение

В целом, выявление и преодоление этих проблем требует системного подхода, комплексных решений и постоянного развития компетенций сотрудников. Необходимость инвестиций в обучение, технологическую модернизацию и создание внутренней культуры безопасности становится очевидной. Важно также учитывать специфику образовательной среды, балансировать между обеспечением защиты и сохранением доступности ресурсов, а также учитывать нормативные требования и современные угрозы. Только при условии комплексного и последовательного подхода можно преодолеть существующие сложности и создать устойчивую систему информационной безопасности, способную эффективно защищать данные и поддерживать доверие к образовательным учреждениям.

Библиография

1. Алкесов Р.Т. Проблемы защиты информации в образовательных организациях // Вопросы российского и международного права. 2026. Т. 16. № 3А. С. 163–168.
2. Хромова А.Р., Петросян Л.Е. Анализ уязвимостей в системах безопасности данных // Инженерный вестник Дона. 2023. № 6 (102). С. 67–76.

Identifying and Overcoming Information Security Problems in Education

Ruslan T. Alkesov

PhD in Sociology, Associate Professor,
Department of Administrative and Criminal Law,
Maykop State Technological University,
385000, 191, Pervomayskaya str., Maykop, Russian Federation;
e-mail: alkesov55@mail.ru

Abstract

In the article, the author examines current problems of information security in the educational environment and proposes ways to overcome them. The key threats characteristic of educational institutions are analyzed: cyberattacks, phishing, social engineering, as well as internal risks conditioned by the human factor. Particular attention is paid to typical vulnerabilities of IT infrastructure – insufficient protection of network resources, weaknesses in remote access, and the use of outdated software. A systemic approach to ensuring information security is proposed, including a set of measures – from regular software updates and the introduction of monitoring tools to the formation of a security culture through training and workshops. The necessity of a balance between data protection and maintaining the accessibility of educational resources, as well as taking into account regulatory and legal requirements, is emphasized. The results of the research can be useful to heads of educational organizations, information security specialists, and administrators of IT systems in developing and improving information protection policies.

For citation

Alkesov R.T. (2026) Vyyavlenie i preodolenie problem informatsionnoy bezopasnosti v obrazovanii [Identifying and Overcoming Information Security Problems in Education]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 16 (7A), pp. 203-207. DOI: 10.34670/AR.2026.78.15.023

Keywords

Information security, education, cyber threats, human factor, data protection, digital literacy, IT infrastructure, phishing, information security policy, cyber resilience.

References

1. Alkesov, R.T. (2026) Problemy zashchity informatsii v obrazovatel'nykh organizatsiyakh [Problems of Information Protection in Educational Organizations]. *Voprosy rossiyskogo i mezhdunarodnogo prava*, 16(3A), 163–168.
2. Khromova, A.R., & Petrosyan, L.E. (2023). Analiz uyazvimostey v sistemakh bezopasnosti dannykh [Analysis of Vulnerabilities in Data Security Systems]. *Inzhenemyy vestnik Dona*, (6(102)), 67–76.