СВЕДЕНИЯ ОБ АВТОРАХ
Принадлежность к организации

Курамагомедова Зулейха Магомедовна, кандидат филологических наук, доцент, кафедра экономики и управления, Московский автомобильно-дорожный государственный технический университет, Махачкалинский филиал, Махачкала, Россия; e-mail: zuzuchekk@mail.ru

Курбанова Ольга Владимировна, кандидат филологических наук, доцент, кафедра русского языка, Дагестанский государственный технический университет, Махачкала, Россия; e-mail: olgavlad1967@yandex.ru

Принята в печать 22.04.2025 г.

INFORMATION ABOUT THE AUTHORS
Affiliations

Zuleikha M. Kuramagomedova, Ph. D. (Philology), assistant professor, the chair of Economics and Management, Moscow Automobile and Road State Technical University, Makhachkala Branch, Makhachkala, Russia; e-mail: zuzuchekk@mail.ru

Olga V. Kurbanova, Ph. D. (Philology), assistant professor, the chair of the Russian, Dagestan State Technical University, Makhachkala, Russia; e-mail: olgavlad1967@yandex.ru

Received 22.04.2025.

Педагогические науки / Pedagogical Science
Оригинальная статья / Original Paper
УДК 378.017
DOI: 10.31161/1995-0659-2025-19-2-59-62

Обеспечение информационной безопасности в условиях цифровизации системы образования

© 2025 Магомедов Ш. А., Билалов М. К.
Дагестанский государственный педагогический университет им. Р. Гамзатова, Махачкала, Россия; e-mail: sh-mag@mail.ru, bilalov@mail.ru

РЕЗЮМЕ. Цель. Выявить имеющиеся комплексные подходы к обеспечению информационной безопасности в условиях цифровизации системы образования. **Методы**. Анализ и обобщение существующего опыта по информационной безопасности, изучение взаимосвязей между угрозами и методами защиты. **Результат.** Создание культуры безопасности в организациях, где каждый понимает свою роль в защите информации. Формирование культуры безопасности требует времени и усилий, но это инвестиция, которая оправдает себя в виде снижения рисков и повышения общей защищенности организации. Необходимо чувствовать свою ответственность за безопасность информации и понимать, как его действия влияют на общую защиту. **Вывод.** Информационная безопасность – это не только технические решения, но и комплексный процесс, включающий людей, процессы и технологии. В условиях быстрого развития цифровых технологий важно постоянно адаптироваться к новым угрозам и вызовам.

Ключевые слова: общество, цифровизация, безопасность, угрозы, защита, личная и корпоративная информация.

Формат цитирования: Магомедов Ш. А., Билалов М. К. Обеспечение информационной безопасности в условиях цифровизации системы образования // Известия Дагестанского государственного педагогического университета. Психолого-педагогические науки. 2025. Т. 19. № 2. С. 59-62. DOI: 10.31161/1995-0659-2025-19-2-59-62

Ensuring Information Security in the Context of Digitalization of the Education System

© 2025 Shamil A. Magomedov, Magomed K. Bilalov,
Gamzatov Dagestan State Pedagogical University, Makhachkala, Russia; e-mail: sh-mag@mail.ru, bilalov@mail.ru

ABSTRACT. Aim. To identify the existing comprehensive approaches to ensuring information security in the context of digitalization of modern society. **Methods.** Analysis and generalization of existing information security experience, study of the interrelationships between threats and protection methods. **Result.** Creating a culture of security in organizations where everyone understands their role in protecting information. Building a safety culture takes time and effort, but it is an investment that will pay off in the form of reducing risks and increasing the overall security of the organization. It is necessary to feel responsible for the security of information and understand how his actions affect the overall protection. **Conclusion.** Information security is not only technical solutions, but also a complex process involving people, processes and technologies. In the context of the rapid development of digital technologies, it is important to constantly adapt to new threats and challenges.

Keywords: society, digitalization, security, threats, protection, personal and corporate information.

For citation: Magomedov Sh. A., Bilalov M. K. Ensuring Information Security in the Context of Digitalization of the Education System. Dagestan State Pedagogical University. Journal. Psychological and Pedagogical Sciences. 2025. Vol. 19. No. 2. Pp. 59-62. DOI: 10.31161/1995-0659-2025-19-2-59-62 (in Russian)

Введение

Быстрое развитие цифровых технологий создает не только новые возможности, но и новые угрозы. Кибербезопасность становится важной частью стратегии как для общества в целом, так и для системы образования. Обеспечение информационной безопасности направленно на предохранения личных данных, на противодействие несанкционированного доступа, а также повреждение или утечки конфиденциальной информации. С развитием технологий (например, облачных вычислений, Интернета вещей и искусственного интеллекта) увеличиваются и риски, связанные с информационной безопасностью в том числе и в системе образования. Поэтому важно постоянно адаптировать стратегии защиты и быть в курсе новых угроз. Информационная безопасность – это не только техническая задача, но и важный аспект управления рисками для организаций всех размеров.

Целью статьи является необходимость раскрытия существующих комплексных подходов в обеспечении информационной безопасности в условиях цифровизации системы образования.

Методы: анализ и обобщение существующего опыта по информационной безопасности, изучение взаимосвязей между угрозами и методами защиты.

Обсуждение и результаты

В новых существующих реалиях цифровизации системы образования происходят общественно-политические, социально-экономические и культурно-просветительские трансформации, которые в свою очередь влияют на производственные отношения в том или ином обществе. В такой ситуации коммуникации становятся основными ресурсами, а взаимодействие между людьми, организациями и государствами осуществляется преимущественно через цифровые каналы, требующие надежности и безопасности [4, с. 769].

Одним из ключевых методов защиты конфиденциальной информации является шифрование. Шифрование данных включает в себя процесс преобразования информации в нечитабельный формат и основывается на специальном алгоритме. Алгоритмы шифрования – это методы, используемые для защиты информации путем преобразования данных в неразборчивую форму. Существует несколько типов алгоритмов шифрования, которые можно разделить на две основные категории: симметричные и асимметричные. Шифрование играет ключевую роль в обеспечении конфиденциальности и целостности информации в современном цифровом мире. Также используется гибридное шифрование, где применяется комбинация симметричного и асимметричного шифрования для повышения безопасности и производительности.

Вопросы конфиденциальности и безопасности данных становятся важными в системе образования, так как объем собираемой информации растет. Поэтому возникает необходимость разработки комплекса мер и практик, направленных на защиту данных от несанкционированного доступа, использования, раскрытия, разрушения или изменения [2, с. 51].

Алгоритмы шифрования широко применяются в различных областях таких, как защита данных на дисках и в облачных хранилищах, безопасная передача данных

по сети (например, HTTPS), цифровые подписи и аутентификация, которые включают:

1. Доступность, гарантия того, что данные и системы доступны пользователям тогда, когда они нужны, что включает в себя защиту от атак типа «отказ в обслуживании» (DDoS) и обеспечение резервного копирования данных.

2. Аудит и мониторинг, регулярная проверка систем и процессов для выявления уязвимостей и обеспечения соблюдения политик безопасности.

3. Обучение пользователей основам безопасности информации, чтобы они могли распознавать угрозы, такие как фишинг или вредоносное программное обеспечение.

4. Политики безопасности, где разработка и внедрение четких политик безопасности, которые определяют правила обработки и защиты информации.

Киберугрозы представляют собой разнообразные риски, которые могут повредить информационные системы, данные и сети. Существуют программы, которые внедряются в другие файлы и могут повреждать или уничтожать данные. Также представляют угрозу самостоятельно распространяющиеся программы, которые используют сети для копирования себя на другие устройства. К вредоносным программам относятся программы, маскирующиеся под легитимное программное обеспечение, которые открывают доступ к системе [1, с. 190].

Соблюдение политики безопасности информации системы образования включает в себя основной набор правил и процедур, направленных на защиту конфиденциальности, целостности и доступности информации. Важно применять шифрование для защиты конфиденциальной информации как при хранении, так и при ее передаче по каналам связи. При этом возникает необходимость в обеспечении защиты физических ресурсов, таких как серверы и рабочие станции, от несанкционированного доступа, регулярно создавать резервные копии данных и разрабатывать планы восстановления после сбоев или утечек данных. Периодически пересматривать и обновлять политику безопасности информации в соответствии с постоянными технологическими новшествами [5, с. 9].

Внедрение систем мониторинга для отслеживания активности в сети и на серверах, обслуживающих систему образования. Данные системы включают в себя анализ логов для выявления подозрительных действий или аномалий, а также регулярное обновление программного обеспечения и применение специализированных патчей, способствующих минимизации возникающих рисков при обновлениях различных приложений. При этом создание и тестирование планов действий на случай инцидентов безопасности обеспечивают готовность команды к быстрой реакции на угрозы и минимизации ущерба [3, с. 134].

Регулярное обновление информации о новых угрозах и методах защиты представляет собой важный аспект обеспечения безопасности информационных систем. Знания о киберугрозах охватывают широкий спектр тем и аспектов, связанных с безопасностью информационных систем. Данные знания позволяют использовать решения для мониторинга угроз (Threat Intelligence Platforms), которые собирают и анализируют данные о новых уязвимостях и атаках. Поэтому возникает необходимость регулярного пересмотра и обновления внутренней политики безопасности на основе новых угроз и методов защиты. Это поможет адаптировать защитные меры к текущей ситуации.

Вывод

Поддержание актуальности знаний о киберугрозах – это непрерывный процесс, который требует внимания и ресурсов, но он критически важен для защиты от потенциальных рисков. Угрозы могут исходить от устройства IoT, часто имеют слабую защиту, что делает их уязвимыми для атак и применяют их для создания ботнетов или доступа к образовательным сетям. Использование уязвимостей в программном обеспечении для выполнения произвольного кода или получения несанкционированного доступа к системам, обеспечивающим защиту данных образовательных организаций. Все атаки, направленные на взлом шифрования данных, имеют своей целью получение доступа к защищенной информации.

Таким образом, каждый из этих типов угроз требует специфических методов защиты и реагирования для минимизации рисков и защиты информации как в обществе в целом, так и в системе образования.

Литература

1. Иванько А. Ф. Информационная безопасность вчера и сегодня // Молодой ученый. 2017. № 51. С. 185-192.
2. Пилецкая А. В. Искусственный интеллект и безопасность в современных возможностях // Молодой ученый. 2020. № 20 (310). С. 50-52.
3. Громов Ю. Ю. Информационная безопасность и защита информации: Учебное пособие. Ст. Оскол: ТНТ, 2017. 384 с.
4. Ковалев А. А. Роль информационных технологий в обеспечении безопасности государства // Молодой ученый. 2016. № 21 (125). С. 767-771.
5. Корнев Л. В. Обеспечение информационной безопасности в условиях цифровизации // Молодой ученый. 2022. № 12 (407). С. 7-11.

References

1. Ivanko A. F. *Informacionnaya bezopasnost' vchera i segodnya* [Information security yesterday and today]. Young scientist. 2017. No. 51 (185). (In Russian)
2. Piletskaya A. V. *Iskusstvennyj intellekt i bezopasnost' v sovremennykh vozmozhnostyakh* [Artificial intelligence and security in modern capabilities]. Young scientist. 2020. No. 20 (310). Pp. 50-52. (In Russian)
3. Gromov Yu. Yu. *Informacionnaya bezopasnost' i zashchita informacii: Uchebnoe posobie* [Information security and information protection: A textbook]. St. Oskol: TNT, 2017. 384 p. (In Russian)
4. Kovalev A. A. *Rol' informacionnykh tekhnologij v obespechenii bezopasnosti gosudarstva* [The role of information technology in ensuring state security]. Young scientist. 2016. № 21 (125). Pp. 767-771. (In Russian)
5. Kornev L. V. *Obespechenie informacionnoj bezopasnosti v usloviyakh cifrovizacii* [Ensuring information security in the context of digitalization]. Young scientist. 2022. No. 12 (407). Pp. 7-11. (In Russian)

СВЕДЕНИЯ ОБ АВТОРАХ
Принадлежность к организации

Магомедов Шамиль Абдулмажидович, кандидат педагогических наук, доцент, кафедра теории и методики профессионального образования, Дагестанский государственный педагогический университет им. Р. Гамзатова, Махачкала, Россия; e-mail: sh-mag@mail.ru

Билалов Магомед Курбандибирович, кандидат педагогических наук, доцент, кафедра педагогики, Дагестанский государственный педагогический университет им. Р. Гамзатова, Махачкала, Россия; e-mail: bilalov@mail.ru

INFORMATION ABOUT THE AUTHORS
Affiliations

Shamil A. Magomedov, Ph. D. (Pedagogy), assistant professor, the chair of Theory and Methods of Professional Education, Gamzatov Dagestan State Pedagogical University, Makhachkala, Russia; e-mail: sh-mag@mail.ru

Magomed K. Bilalov, Ph. D. (Pedagogy), assistant professor, the chair of Pedagogy, Gamzatov Dagestan State Pedagogical University, Makhachkala, Russia; e-mail: bilalov@mail.ru

Принята в печать 20.03.2025 г.

Received 20.03.2025.