# INFORMATION SECURITY IN THE DIGITAL EDUCATIONAL ENVIRONMENT

**Shavkat Mamirovich Ibragimov**
Fergana State University, Associate Professor of the Department of Information Technologies.
shavkat70@bk.ru +998 90 530 18 04 http://orcid.org/0000-0001-7812-1898
**Jasminabonu Kuvonchbek qizi Mashrabova**
Fergana State University Student of the program Philology and Language Teaching (English Language)
jasminamashrabova@gmail.com

***Abstract:*** This article examines the problems of ensuring information security in the digital educational environment under the conditions of active digitalization of the education system. The main threats to information security arising from the use of electronic educational platforms, cloud technologies, and distance learning formats are analyzed. Special attention is paid to the protection of personal data of students and teachers, issues of cybersecurity in educational institutions, as well as the development of digital literacy among participants in the educational process. The article reveals the key principles and mechanisms for ensuring information security, considers the regulatory and legal foundations of information protection, and modern technological solutions in this field. The methodological basis of the research consists of system analysis, comparative-analytical methods, and the generalization of domestic and foreign studies. The obtained results indicate that an effective information security system is a necessary condition for the sustainable functioning of the modern digital educational environment.

***Keywords:*** information security, digital educational environment, cybersecurity, personal data protection, digitalization of education, distance learning, digital literacy, educational technologies.

## ВВЕДЕНИЕ

Современный этап развития общества характеризуется стремительной цифровой трансформацией практически всех сфер человеческой деятельности, включая систему образования. Активное внедрение информационно-коммуникационных технологий, электронных образовательных платформ, облачных сервисов и систем дистанционного обучения формирует качественно новую цифровую образовательную среду, обеспечивающую расширение доступа к образовательным ресурсам и повышение гибкости образовательного процесса.

Особенно интенсивно процессы цифровизации образования проявились в период пандемии COVID-19, когда образовательные учреждения были вынуждены в кратчайшие сроки перейти на дистанционные формы обучения. Данный переход продемонстрировал как значительный потенциал цифровых технологий, так и серьёзные проблемы, связанные с обеспечением информационной безопасности образовательного пространства.

Цифровая образовательная среда представляет собой сложную информационную экосистему, включающую обучающихся, преподавателей, администрации образовательных учреждений, электронные платформы, базы данных, облачные сервисы и сетевые коммуникации. Функционирование такой среды сопровождается постоянным обменом значительными объёмами информации, включая персональные данные, учебные материалы, результаты оценивания и иные конфиденциальные сведения. Вследствие этого вопросы защиты информации и обеспечения кибербезопасности приобретают особую

актуальность. Актуальность исследования определяется рядом факторов. Во-первых, наблюдается устойчивый рост числа кибератак на образовательные организации, сопровождающихся утечками персональных данных и нарушением работы информационных систем. Во-вторых, широкое распространение дистанционного обучения существенно увеличивает риски несанкционированного доступа к образовательным ресурсам. В-третьих, недостаточный уровень цифровой грамотности отдельных участников образовательного процесса создаёт дополнительные угрозы информационной безопасности.

Целью настоящей статьи является комплексный анализ проблем информационной безопасности в цифровой образовательной среде, рассмотрение основных угроз, механизмов защиты информации и перспектив развития безопасной цифровой образовательной инфраструктуры.

Для достижения поставленной цели решаются следующие задачи: изучить теоретические основы информационной безопасности в образовании; проанализировать основные угрозы цифровой образовательной среды; рассмотреть нормативно-правовые основы защиты информации; исследовать современные методы обеспечения кибербезопасности образовательных организаций; определить роль цифровой грамотности в обеспечении информационной безопасности; выявить перспективные направления развития систем защиты информации в образовании.

Методологическую основу исследования составляют системный подход, сравнительно-аналитический метод, анализ научной литературы и нормативных документов, а также метод обобщения результатов современных исследований в области информационной безопасности.

**Теоретические основы информационной безопасности в образовании**

Информационная безопасность представляет собой состояние защищённости информационной среды от внутренних и внешних угроз, обеспечивающее сохранность, целостность, конфиденциальность и доступность информации. В контексте цифровой образовательной среды информационная безопасность приобретает комплексный характер, охватывая технические, организационные, правовые и педагогические аспекты.

Теоретической основой современной концепции информационной безопасности является модель CIA (Confidentiality, Integrity, Availability), включающая три ключевых принципа: конфиденциальность информации, её целостность и доступность. В образовательной среде данные принципы имеют особое значение, поскольку образовательные организации одновременно обеспечивают открытый доступ к учебным ресурсам и обязаны защищать персональные данные участников образовательного процесса.

Существенное влияние на развитие подходов к обеспечению информационной безопасности оказала концепция кибербезопасности, рассматривающая цифровую инфраструктуру как объект комплексной защиты от технических и социальных угроз. Современные исследования показывают, что человеческий фактор остаётся одной из основных причин нарушений информационной безопасности, что особенно актуально для образовательной среды с большим количеством пользователей различного уровня цифровой подготовки.

В условиях цифровизации образования особое значение приобретает концепция цифровой грамотности, включающая навыки безопасного использования информационных технологий, критического анализа цифровой

информации и ответственного поведения в сети Интернет. Формирование данных компетенций рассматривается как неотъемлемый элемент современной образовательной политики.

**Основные угрозы информационной безопасности в цифровой образовательной среде**

Современная цифровая образовательная среда подвержена широкому спектру угроз информационной безопасности. Наиболее распространёнными являются кибератаки, направленные на получение несанкционированного доступа к информационным системам образовательных организаций.

Одной из наиболее серьёзных угроз выступают утечки персональных данных обучающихся и преподавателей. Электронные образовательные платформы аккумулируют значительные объёмы конфиденциальной информации, включая персональные сведения, результаты обучения, контактные данные и финансовую информацию. Недостаточный уровень защиты таких данных может привести к их незаконному распространению и использованию.

Серьёзную опасность представляют фишинговые атаки, направленные на получение логинов, паролей и иной конфиденциальной информации пользователей образовательных систем. Практика показывает, что обучающиеся и преподаватели нередко становятся жертвами социальной инженерии вследствие недостаточной осведомлённости о принципах безопасного поведения в цифровой среде.

Распространённой угрозой являются вредоносные программные средства, включая вирусы, программы-вымогатели и шпионское программное обеспечение. Попадание вредоносного кода в информационную инфраструктуру образовательной организации может привести к блокировке доступа к учебным

ресурсам, утрате данных и нарушению образовательного процесса. Дополнительную проблему создаёт использование незащищённых сетевых соединений и личных устройств участников образовательного процесса. В условиях дистанционного обучения обучающиеся и преподаватели часто подключаются к образовательным платформам через публичные сети Wi-Fi и используют устройства с недостаточным уровнем защиты, что существенно увеличивает вероятность компрометации данных.

Особого внимания заслуживают психологические и социальные угрозы цифровой среды, включая кибербуллинг, распространение деструктивного контента и манипулятивное воздействие через социальные сети. Для несовершеннолетних пользователей данные угрозы могут иметь серьёзные последствия как для психологического состояния, так и для образовательной деятельности.

**Нормативно-правовые основы обеспечения информационной безопасности**

Обеспечение информационной безопасности в цифровой образовательной среде основывается на комплексе международных и национальных нормативно-правовых актов. Основу правового регулирования составляют законы о защите персональных данных, информационных технологиях и кибербезопасности.

В большинстве государств образовательные организации обязаны обеспечивать защиту персональных данных обучающихся и сотрудников в соответствии с действующим законодательством. Это предполагает внедрение организационных и технических мер защиты информации, ограничение доступа к конфиденциальным сведениям и соблюдение принципов обработки персональных данных. Важную роль играют международные стандарты информационной безопасности, включая стандарты серии ISO/IEC 27000,

определяющие требования к системам управления информационной безопасностью. Использование данных стандартов позволяет образовательным организациям формировать комплексный подход к защите информационной инфраструктуры.

Современные нормативные документы также предусматривают необходимость формирования безопасной цифровой образовательной среды, включающей механизмы фильтрации контента, защиты несовершеннолетних пользователей и предотвращения распространения противоправной информации.

**Методы и технологии обеспечения информационной безопасности**

Современные образовательные организации используют комплекс организационных и технических методов обеспечения информационной безопасности. Одним из базовых механизмов является система аутентификации и авторизации пользователей, обеспечивающая разграничение прав доступа к информационным ресурсам.

Широкое распространение получили технологии многофакторной аутентификации, существенно повышающие уровень защищённости пользовательских аккаунтов. Дополнительным средством защиты выступает шифрование данных, обеспечивающее конфиденциальность информации при её хранении и передаче через сети связи.

Важную роль играют системы резервного копирования данных, позволяющие минимизировать последствия кибератак и технических сбоев. Регулярное создание резервных копий учебных материалов и баз данных обеспечивает устойчивость образовательного процесса даже в условиях информационных инцидентов. Современные системы мониторинга и обнаружения угроз позволяют оперативно выявлять подозрительную активность

в информационной инфраструктуре образовательной организации. Использование технологий искусственного интеллекта и машинного обучения способствует автоматическому анализу сетевого трафика и выявлению потенциальных угроз.

Существенное значение имеют организационные меры безопасности: разработка внутренних регламентов, проведение инструктажей, ограничение доступа к критически важным системам и регулярное повышение квалификации сотрудников в области кибербезопасности.

**Цифровая грамотность как фактор информационной безопасности**

Одним из ключевых условий обеспечения информационной безопасности в цифровой образовательной среде является высокий уровень цифровой грамотности участников образовательного процесса. Современные исследования показывают, что значительная часть инцидентов информационной безопасности связана с ошибками пользователей.

Формирование цифровой грамотности предполагает развитие у обучающихся и преподавателей навыков безопасной работы с информацией, критического мышления, способности распознавать угрозы и соблюдать правила цифровой гигиены. Особое значение приобретают навыки создания надёжных паролей, защиты персональных данных и безопасного использования сетевых сервисов.

В образовательных организациях всё более активно внедряются программы цифровой безопасности, направленные на повышение осведомлённости пользователей о современных киберугрозах. Практика показывает, что регулярное проведение обучающих мероприятий способствует значительному снижению числа инцидентов, связанных с человеческим фактором.

**Проблемы и перспективы развития информационной безопасности в образовании**

Несмотря на активное развитие технологий защиты информации, обеспечение информационной безопасности в цифровой образовательной среде остаётся сложной задачей. Одной из основных проблем является недостаточное финансирование систем кибербезопасности в образовательных организациях, особенно в учреждениях среднего и высшего образования.

Серьёзную проблему представляет быстрое изменение характера киберугроз. Развитие технологий искусственного интеллекта, автоматизированных атак и методов социальной инженерии требует постоянного обновления систем защиты и повышения квалификации специалистов.

Дополнительные трудности связаны с необходимостью соблюдения баланса между открытостью образовательной среды и требованиями безопасности. Избыточные ограничения могут негативно влиять на доступность образовательных ресурсов и эффективность учебного процесса.

Перспективными направлениями развития информационной безопасности являются внедрение интеллектуальных систем обнаружения угроз, использование технологий блокчейн для защиты образовательных данных, развитие биометрических методов аутентификации и создание единых национальных платформ безопасного цифрового образования.

## ЗАКЛЮЧЕНИЕ

Проведённый анализ позволяет сделать вывод о том, что информационная безопасность является одним из ключевых условий эффективного функционирования современной цифровой образовательной среды. Стремительное развитие цифровых технологий и расширение дистанционных

форм обучения существенно повышают значимость защиты информации и кибербезопасности образовательных организаций.

Современные угрозы информационной безопасности имеют комплексный характер и требуют сочетания технических, организационных, правовых и педагогических мер защиты. Особое значение приобретает формирование цифровой грамотности обучающихся и преподавателей как важнейшего элемента безопасного поведения в цифровой среде.

Эффективная система информационной безопасности должна рассматриваться не только как технический механизм защиты данных, но и как важный компонент современной образовательной политики, обеспечивающий устойчивость, доступность и качество цифрового образования.

Таким образом, дальнейшее развитие цифровой образовательной среды невозможно без комплексного совершенствования механизмов информационной безопасности, внедрения современных технологий защиты информации и формирования культуры ответственного использования цифровых технологий.

## СПИСОК ЛИТЕРАТУРЫ

1. Беляев А.Н. Информационная безопасность образовательной организации. - М.: Юрайт, 2021. - 214 с.
2. Баранова Е.К., Лапина О.А. Цифровая образовательная среда: проблемы и перспективы развития // Высшее образование в России. - 2020. - № 8–9. - С. 45–53.
3. Castells M. The Rise of the Network Society. - Oxford: Blackwell Publishers, 2010. - 597 p.
4. ISO/IEC 27001:2022 Information Security Management Systems - Requirements.

5. Kaspersky Lab. Cyberthreats in Education Report. - 2022.

6. Кузнецов П.С. Кибербезопасность в условиях цифровизации образования // Информатика и образование. - 2021. - № 6. - С. 15–22.

7. OECD. Digital Education Outlook 2021: Pushing the Frontiers with Artificial Intelligence, Blockchain and Robots. - Paris: OECD Publishing, 2021.

8. Schwab K. The Fourth Industrial Revolution. - Geneva: World Economic Forum, 2016. - 172 p.

9. Солдатова Г.У., Рассказова Е.И. Цифровая компетентность подростков и безопасность в Интернете // Психологическая наука и образование. - 2019. - Т. 24, № 5. - С. 28–38.

10. UNESCO. Guidance on Digital Learning and Data Protection. - Paris: UNESCO, 2021.

11. Шарифьянов Ф.М. Защита персональных данных в образовательной среде // Педагогическое образование в России. - 2022. - № 3. - С. 97–104.

12. Sweller J. Cognitive Load Theory and Educational Technology // Educational Technology Research and Development. - 2020. - Vol. 68. - P. 1–16.