Иглинская Инна Геннадьевна
магистр, преподаватель
Петракова Анастасия Владимировна
бакалавр, преподаватель

Старооскольский филиал ФГАОУ ВО «Белгородский государственный национальный исследовательский университет»
г. Старый Оскол, Белгородская область

КИБЕРБЕЗОПАСНОСТЬ В ЦИФРОВОМ ОБРАЗОВАНИИ: ЗАЩИТА ДАННЫХ СТУДЕНТОВ И ПРЕПОДАВАТЕЛЕЙ

Аннотация*: в условиях стремительного перехода к цифровым форматам обучения кибербезопасность становится одной из ключевых задач образовательных учреждений. В статье рассматриваются основные угрозы, с которыми сталкиваются участники образовательного процесса, включая утечки личной информации, кибератаки и мошенничество. Особое внимание уделяется методам защиты данных, таким как шифрование, многофакторная аутентификация и обучение пользователей основам кибербезопасности. Обсуждаются законодательные аспекты и стандарты, регулирующие защиту персональных данных в образовательной среде. В заключении работа подчеркивает важность создания культуры кибербезопасности в образовательных учреждениях, что способствует не только защите информации, но и повышению доверия со стороны студентов и преподавателей к цифровым образовательным платформам.*

Ключевые слова*: кибербезопасность, цифровое образование, защита данных, личная информация, утечки данных, кибератаки, мошенничество, шифрование, многофакторная аутентификация, обучение кибербезопасности, персональные данные, законодательные аспекты, стандарты безопасности, культура кибербезопасности, доверие пользователей, образовательные учреждения, цифровые платформы, риски киберугроз.*

В современном мире цифровое образование становится неотъемлемой частью учебного процесса, открывая новые горизонты для студентов и преподавателей. Однако с ростом популярности онлайн-курсов и образовательных платформ возникает и множество вызовов, связанных с кибербезопасностью. Защита данных студентов и преподавателей становится приоритетной задачей для образовательных учреждений, поскольку утечки личной информации и кибератаки могут иметь серьезные последствия как для отдельных пользователей, так и для всей образовательной системы.

С каждым годом количество киберугроз увеличивается, и с ними растет необходимость в эффективных мерах по обеспечению безопасности данных. Неправильное обращение с личной информацией может привести к мошенничеству, утечкам конфиденциальных данных и нарушению доверия между учебными заведениями и их пользователями. В этой статье мы рассмотрим основные аспекты кибербезопасности в цифровом образовании, проанализируем существующие угрозы и предложим рекомендации по защите данных студентов и преподавателей. Обеспечение кибербезопасности не только защищает личную информацию, но и способствует созданию безопасной образовательной среды, где каждый может сосредоточиться на получении знаний без страха за свою безопасность.

Актуальность проблемы кибербезопасности в цифровом образовании

С переходом образовательных учреждений на онлайн-форматы обучения, особенно в условиях пандемии COVID-19, кибербезопасность стала одной из ключевых проблем. Учебные заведения все чаще используют платформы для дистанционного обучения, что увеличивает риски кибератак. Студенты и преподаватели становятся мишенями для хакеров, стремящихся получить доступ к личной информации, финансовым данным и интеллектуальной собственности [1, с. 32–37].

Основные угрозы кибербезопасности в образовательной среде

Фишинг – это один из самых распространенных методов кибератак, при котором злоумышленники пытаются обманом заставить пользователей раскрыть свои личные данные. В образовательной среде фишинговые атаки могут быть направлены на студентов и преподавателей через электронную почту или

сообщения в социальных сетях. Злоумышленники могут маскироваться под официальные источники, предлагая ссылки на «важные» документы или «обновления» системы.

Образовательные платформы и системы управления обучением (LMS) могут содержать уязвимости, которые хакеры могут использовать для несанкционированного доступа к данным. Регулярные обновления программного обеспечения и патчи безопасности являются необходимыми мерами для защиты от таких угроз.

Несанкционированный доступ к личной информации студентов и преподавателей может происходить как из-за внешних атак, так и из-за внутренних угроз – например, недобросовестных сотрудников. Это подчеркивает важность контроля доступа и мониторинга действий пользователей в системах.

Рекомендации по обеспечению кибербезопасности

Одним из самых эффективных способов борьбы с киберугрозами является обучение студентов и преподавателей основам кибербезопасности. Программы обучения должны включать информацию о том, как распознавать фишинг-атаки, создавать надежные пароли и защищать свои устройства [2, с. 134–136].

Внедрение многофакторной аутентификации (MFA) значительно повышает уровень безопасности аккаунтов пользователей. Даже если злоумышленник получит доступ к паролю, ему потребуется дополнительный фактор аутентификации, чтобы войти в систему [3, с. 120–122].

Образовательные учреждения должны проводить регулярные аудиты безопасности своих информационных систем. Это поможет выявить потенциальные уязвимости и своевременно их устранить.

Шифрование данных, как в процессе их передачи, так и в состоянии покоя, является важным шагом для защиты конфиденциальной информации. Это затрудняет доступ злоумышленников к данным даже в случае их утечки.

Кибербезопасность в цифровом образовании – это не просто техническая задача, а комплексная проблема, требующая внимания со стороны всех участников образовательного процесса. Защита данных студентов и преподавателей

должна стать приоритетом для учебных заведений, чтобы создать безопасную и доверительную образовательную среду. Обучение пользователей, внедрение современных технологий защиты и регулярный мониторинг систем – ключевые элементы успешной стратегии кибербезопасности в образовательной сфере.

В условиях стремительного развития цифровых технологий и перехода на онлайн-форматы обучения кибербезопасность становится неотъемлемой частью образовательной среды. Защита данных студентов и преподавателей – это не только вопрос технической безопасности, но и важный аспект доверия к образовательным учреждениям. Эффективная стратегия кибербезопасности должна включать в себя обучение пользователей, внедрение многофакторной аутентификации, регулярные аудиты безопасности и шифрование данных.

Только совместными усилиями образовательных учреждений, преподавателей и студентов можно создать безопасную цифровую среду, способствующую эффективному обучению и развитию. Важно помнить, что киберугрозы продолжают эволюционировать, и поэтому необходимо постоянно адаптироваться и обновлять подходы к защите информации. В конечном итоге, безопасное образовательное пространство – это залог успешного обучения и формирования будущих специалистов, готовых к вызовам цифрового мира.

Список литературы

1. Гладков А.Н. Визуализация киберугроз как аспект формирования компетенций в области информационной безопасности / А.Н. Гладков, С.Н. Горячев, Н.С. Кобяков // Защита информации. Инсайд. – 2023. – №1. – С. 32–37. EDN CDIPBX

2. Кузьмина О.В. Информационно-технологическая безопасность обучающихся / О.В. Кузьмина // BI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики: материалы IX Междунар. науч.-практ. конф. (Екатеринбург, 2 дек. 2021 г.). – Екатеринбург, 2021. – С. 134–136.

3. Чучкалова И.Ю. Информационная безопасность в условиях трансформации общества / И.Ю. Чучкалова // BI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики: материалы IX Междунар. науч.-практ. конф. (Екатеринбург, 2 дек. 2021 г.). – Екатеринбург, 2021. – С. 120–122.