Столыпинский вестник

Научная статья

Original article

УДК 35

ОБЕСПЕЧЕНИЕ ЦИФРОВОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА В СОВРЕМЕННЫХ УСЛОВИЯХ

ENSURING DIGITAL SECURITY OF THE EDUCATIONAL PROCESS IN MODERN CONDITIONS

Кокорев Николай Михайлович, ФГБОУ ВО Сибирская пожарно-спасательная академия ГПС МЧС, Кафедра государственного и муниципального управления

Kokorev Nikolai Mikhailovich, Siberian Fire and Rescue Academy of the Ministry of Emergency Situations, Department of Public and Municipal Administration

Аннотация: В современном образовательном пространстве цифровые технологии играют ключевую роль, однако с этим возникают новые вызовы в области безопасности. Данная статья исследует актуальные проблемы цифровой безопасности в образовательном процессе и предлагает эффективные стратегии и меры для их решения.

Автор анализирует основные угрозы, с которыми сталкиваются учебные заведения в цифровой среде, такие как кибератаки, утечки персональной информации и мошенничество. В работе рассматриваются современные методы защиты, включая использование средств шифрования, внедрение многоуровневых систем аутентификации и обучение персонала в области кибербезопасности.

Особое внимание уделяется вопросам обеспечения безопасности онлайн-обучения, в том числе защите данных студентов и преподавателей в виртуальных средах. Автор призывает к формированию культуры безопасности, включая разработку политик и стандартов, адаптированных к уникальным требованиям образовательной среды.

Abstract: Digital technologies play a key role in the modern educational space, but with this new challenges arise in the field of security. This article explores the current problems of digital security in the educational process and suggests effective strategies and measures to solve them.

The author analyzes the main threats faced by educational institutions in the digital environment, such as cyber attacks, leaks of personal information and fraud. The paper examines modern security methods, including the use of encryption tools, the introduction of multi-level authentication systems and training of personnel in the field of cybersecurity.

Special attention is paid to the issues of ensuring the security of online learning, including the protection of students' and teachers' data in virtual environments. The author calls for the formation of a safety culture, including the development of policies and standards adapted to the unique requirements of the educational environment.

Ключевые слова: цифровая безопасность, обеспечение, образовательный процесс, виртуальная образовательная среда.

Keywords: digital security, provision, educational process, virtual educational environment.

Современное образование все более интегрируется с цифровыми технологиями, предоставляя учащимся и преподавателям уникальные возможности для обучения и обмена знаниями. Однако с этими выгодами возникают новые вызовы в области безопасности данных и цифровой инфраструктуры образовательных учреждений[4]. В настоящее время обеспечение цифровой безопасности в образовательном процессе становится критически важным аспектом, требующим всестороннего и системного подхода.

Образовательные учреждения становятся объектами интереса для киберпреступников, стремящихся получить доступ к чувствительной информации, такой как персональные данные студентов и преподавателей, результаты экзаменов и другие конфиденциальные сведения [2]. Мошеннические попытки манипулирования людьми через обман и обсуждение конфиденциальной информации стали распространенными. Использование различных цифровых платформ для обучения требует высокого уровня безопасности, чтобы предотвратить несанкционированный доступ, утечку данных и другие угрозы.

Недостаток осведомленности и навыков в области кибербезопасности среди преподавателей и студентов увеличивает риски успешных кибератак. Эффективные стратегии и меры для решения проблем цифровой безопасности в образовательном процессе включают в себя несколько важных аспектов. В первую очередь, необходимо внедрить современные системы шифрования для защиты хранимых данных. Использование мощных алгоритмов шифрования помогает предотвратить несанкционированный доступ к конфиденциальной информации.

Для поддержания высокого уровня безопасности следует регулярно проводить аудиты безопасности. Систематические проверки и аудиты позволяют выявлять уязвимости в инфраструктуре и оперативном обеспечении, что дает возможность своевременно предпринимать меры по их устранению. Важным шагом является внедрение многоуровневых систем аутентификации. Дополнительные слои аутентификации, такие как двухфакторная аутентификация, способствуют усилению защиты учетных записей от несанкционированного доступа [3].

Обучение персонала и студентов в области кибербезопасности играет ключевую роль в обеспечении безопасности. Регулярные обучающие мероприятия и тренинги по кибербезопасности способствуют повышению осведомленности и формированию культуры безопасности в учебном заведении.

Неотъемлемой частью безопасности является разработка и соблюдение политик безопасности. Создание четких стандартов и процедур в области цифровой безопасности, а также их строгое соблюдение, обеспечивают эффективное функционирование системы защиты [1]. Интеграция антивирусного и антифишингового программного обеспечения также играет важную роль в предотвращении вредоносных программ и фишинговых атак. С использованием современных средств обнаружения и блокировки можно существенно улучшить уровень безопасности в образовательном процессе.

Принятие этих стратегий и мер позволит учебным заведениям существенно повысить уровень цифровой безопасности в образовательном процессе, обеспечивая защиту данных и сохранение доверия участников образовательного процесса.

Учебные заведения, функционирующие в цифровой среде, подвергаются различным угрозам, которые могут серьезно повлиять на безопасность данных и процесс обучения. Кибератаки представляют собой постоянные или скоординированные атаки, направленные на перегрузку сетевой инфраструктуры учебного заведения, что может привести к временным сбоям в доступе к ресурсам. Вредоносное программное обеспечение может использоваться для несанкционированного доступа, кражи данных или разрушения информации.

Утечки персональной информации становятся проблемой из-за нарушений безопасности данных, которые могут привести к утечкам личных данных студентов, преподавателей и сотрудников, представляя серьезные последствия для конфиденциальности. Мошеннические фишинговые атаки, использующие электронные письма или веб-сайты, могут предоставить киберпреступникам доступ к личной информации и учетным данным [3].

Акты социальной инженерии, направленные на манипуляцию людьми с целью получения конфиденциальной информации, представляют собой значительные риски. Недостаточная безопасность онлайн-платформ и

виртуальных образовательных сред может привести к уязвимостям, используемым для несанкционированного доступа и атак.

Сбои в кибербезопасности при дистанционном обучении, такие как несанкционированный доступ к видеоконференциям и обмен нежелательным контентом, становятся более распространенными с ростом дистанционного обучения [5]. Неэффективная подготовка персонала и студентов в области кибербезопасности, вызванная отсутствием соответствующего обучения, может обострить риск успешных кибератак.

Общее понимание этих угроз позволяет учебным заведениям разработать и внедрить эффективные стратегии и меры по обеспечению цифровой безопасности и минимизации рисков.

Современные методы защиты в образовательном процессе включают в себя ряд технологий и стратегий для эффективного противостояния угрозам цифровой безопасности. Шифрование данных является важным аспектом обеспечения безопасности в образовательной среде. Это включает использование мощных алгоритмов шифрования для защиты хранящихся и передаваемых данных, в том числе личных данных студентов и результатов экзаменов. Многоуровневые системы аутентификации, такие как двухфакторная аутентификация (2FA) и многофакторная аутентификация (MFA), внедряются для усиления безопасности учетных записей. Эти системы добавляют дополнительные этапы аутентификации, такие как временные коды или биометрические данные, помимо обычного ввода пароля.

Обучение персонала и студентов в области кибербезопасности является неотъемлемой частью стратегии безопасности. Проведение обязательных обучающих программ с регулярным обновлением знаний в соответствии с последними трендами в области киберугроз способствует поддержанию высокого уровня безопасности [3]. Системы обнаружения и предотвращения инцидентов (IDS/IPS) мониторят сетевую активность для выявления аномалий и блокирования подозрительной активности.

Использование современных антивирусных программ и антималварных средств регулярно обновляется для предотвращения вредоносных атак и защиты от вирусов. Регулярные аудиты безопасности позволяют выявлять уязвимости и принимать меры по их устранению, а также обновлять системы и программное обеспечение для поддержания высокого уровня защиты [3].

Для защиты видеоконференций выбираются безопасные и защищенные платформы, и принимаются меры, такие как использование паролей, чтобы предотвратить несанкционированный доступ. Управление доступом осуществляется согласно принципу наименьших привилегий, что подразумевает ограничение доступа к данным и ресурсам только тем пользователям, которые действительно нуждаются в этом для выполнения своих задач.

Комбинированный подход, включающий в себя эти современные методы защиты, позволяет учебным заведениям эффективно управлять и минимизировать риски в сфере цифровой безопасности в современной образовательной среде.

Обеспечение безопасности онлайн-обучения является критически важным аспектом в современной цифровой среде. Для защиты данных студентов и преподавателей в виртуальных средах можно использовать определенные меры. Шифрование данных в онлайн-обучении играет ключевую роль в обеспечении безопасности и помогает предотвратить перехват и несанкционированный доступ к передаваемой информации [2]. Выбор безопасных платформ, включая виртуальные образовательные платформы и онлайн-инструменты с высоким уровнем безопасности, обеспечивает защиту от несанкционированного доступа и использование средств шифрования.

Многоуровневая аутентификация внедряется для учетных записей студентов и преподавателей, повышая уровень безопасности при входе в систему. Обучение участников обучения по вопросам кибербезопасности становится важным аспектом, чтобы они были осведомлены о рисках онлайн-обучения и знали, как предотвращать угрозы.

Управление доступом осуществляется с ограничением прав доступа согласно принципам наименьших привилегий, гарантируя, что каждый участник имеет доступ только к необходимой информации [4]. Регулярные аудиты безопасности виртуальных образовательных платформ и инфраструктуры проводятся для выявления уязвимостей и их своевременного устранения.

Защита от фишинга осуществляется через фильтрацию электронной почты с целью предотвращения доставки фишинговых сообщений. Разработка и соблюдение политик безопасности, включая четкие правила использования и хранения данных, являются важными шагами для обеспечения общей безопасности. Обеспечение конфиденциальности видеоконференций достигается через использование паролей и доступных настроек конфиденциальности.

Мониторинг и реагирование на подозрительную активность реализуются с помощью систем мониторинга событий, что обеспечивает быстрое обнаружение и эффективное реагирование на потенциальные угрозы.

Эффективное сочетание этих мер позволит учебным заведениям обеспечивать высокий уровень безопасности в онлайн-обучении и защищать данные как студентов, так и преподавателей в виртуальных средах.

Аспекты социальной инженерии в образовательной среде включают в себя различные манипулятивные сценарии, направленные на получение конфиденциальной информации [2]. Эти сценарии включают имитацию авторитетных лиц, использование психологических тактик, фишинговые атаки, манипуляции через социальные сети, а также маскировку под студентов или сотрудников.

Для борьбы с этими угрозами проводится обучение членов образовательного сообщества в распознавании фишинговых атак и других видов манипуляций. Сюда входит организация регулярных тренингов по кибербезопасности, поддержка психологического осведомления, имитации фишинговых атак для практики реакции на угрозы, обучение безопасности электронной почты и правилам проверки личности.

Создание среды доверия также является важным аспектом. Для этого необходимо формирование культуры доверия и открытости, где сотрудники и студенты могут свободно сообщать о подозрительной активности. Важно проводить информационные кампании, в том числе распространение информационных брошюр и постов, чтобы поднять уровень осведомленности об угрозах социальной инженерии.

Технологические средства, такие как антивирусные программы и системы фильтрации электронной почты, внедряются для дополнительной защиты от манипуляций. Постоянное обновление знаний осуществляется через регулярные обучающие курсы и информационные ресурсы, чтобы оставаться в курсе современных методов социальной инженерии.

Обучение членов образовательного сообщества не только распознавать манипуляции, но и развивать критическое мышление в онлайн-среде, является ключевым элементом создания устойчивой и безопасной цифровой образовательной среды.

Будущее цифровой безопасности в образовании возможно только с использованием искусственного интеллекта (ИИ) и машинного обучения для анализа данных и предсказания угроз. Блокчейн признается важным инструментом для обеспечения прозрачности в данных, особенно в хранении результатов экзаменов. Кибергигиена и аналитика поведения становятся фокусом, позволяя системам анализировать пользовательское поведение и предотвращать угрозы. Исследование квантовой криптографии направлено на обеспечение стойкости шифрования в условиях будущих квантовых компьютеров [3].

Киберстрахование выделяется как важный аспект для защиты от финансовых потерь при киберинцидентах. Интеграция умных технологий и интернета вещей (IoT) предполагает мониторинг безопасности физических пространств образовательных учреждений и улучшение управления доступом. Человеческий фактор приобретает значимость, с акцентом на обучение участников культуре безопасности и принципам социальной инженерии.

Развитие глобальных стандартов безопасности для образования стремится к унификации подходов и рекомендаций. Для совершенствования стратегий и технологий предлагается интегрировать обучение по кибербезопасности в учебные программы, стимулировать инновации через исследования, формировать междисциплинарные команды и активно внедрять облачные технологии с фокусом на безопасности данных.

Для обеспечения будущей безопасности в образовании также предлагается обновить законодательство, консолидировать ресурсы, адаптироваться к новым угрозам и создавать гибкие стратегии. Эти шаги призваны обеспечить комплексную систему защиты, охватывая технологии, обучение, стратегии и сотрудничество.

В целом, развитие цифровой безопасности в образовательной сфере представляет собой важное и актуальное направление в свете постоянного увеличения киберугроз и цифровых рисков. Развитие технологий, таких как искусственный интеллект, блокчейн, и интернет вещей, создает новые возможности для обеспечения безопасности данных и образовательных процессов. Однако, вместе с этим, угрозы также становятся более сложными и изощренными, требуя постоянного совершенствования стратегий и технологий.

Обучение студентов и персонала безопасности в цифровой среде должно стать неотъемлемой частью образовательных программ. Развитие культуры безопасности должно начинаться с первых этапов обучения и охватывать все уровни образования. Использование передовых технологий, таких как искусственный интеллект и блокчейн, для более эффективного выявления и предотвращения киберугроз. Развитие систем, способных адаптироваться к новым угрозам и предоставлять оперативные решения.

Формирование междисциплинарных команд и экосистемы кибербезопасности, объединяющих образовательные учреждения, бизнес-сектор, государственные органы и исследовательские центры. Совместные усилия могут привести к более эффективной защите от киберугроз.

Таким образом, цифровая безопасность в образовании требует комплексного и постоянного подхода. Совершенствование стратегий и технологий должно быть непрерывным процессом, направленным на обеспечение безопасности образовательной среды и защиты от киберугроз в будущем.

Литература

1. Адольф В.А и др. Цифровая трансформация образования: безопасность и пути ее обеспечения. // Проблемы современного образования. 2022. №5.
2. Ивашевский С.Л. и др. Особенности «цифрового образования» специалистов в сфере обеспечения экономической безопасности // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. №4 (60).
3. Казинец В.А. и др. Информационная безопасность как часть цифровой культуры выпускников педагогических университетов // Современное педагогическое образование. 2022. №5.
4. Левушкин А.Н. Защита информации при осуществлении предпринимательской деятельности в цифровую эпоху // Журнал прикладных исследований. 2022. №4.
5. Хамидуллин Р.С. и др. Политика кибербезопасности современного образования // Право и политика. 2023. №4.

References

1. Adolf V.A. et al. Digital transformation of education: security and ways to ensure it. // Problems of modern education. 2022. №5.
2. Ivashevsky S.L. et al. Features of the "digital education" of specialists in the field of economic security // Legal science and practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. 2022. №4 (60).
3. Kazinets V.A. et al. Information security as part of the digital culture of graduates of pedagogical universities // Modern pedagogical education. 2022. №5.
4. Levushkin A.N. Information protection in the implementation of entrepreneurial activity in the digital age // Journal of Applied Research. 2022. No.4.

5. Khamidullin R.S. et al. Cybersecurity policy of modern education // Law and politics. 2023. №4.

Для цитирования: Кокорев Н.М. Обеспечение цифровой безопасности образовательного процесса в современных условиях // Научный сетевой журнал «Столыпинский вестник» №/2024.