ОСНОВНЫЕ УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ И СОВРЕМЕННЫЕ МЕТОДЫ ИХ ПРЕДОТВРАЩЕНИЯ

Равшонбек Рахимов Раззакбердиевич
Международный Азиатский Университет, магистрант 2 курса

Аннотация: *В статье рассматриваются основные угрозы кибербезопасности в образовательных учреждениях, включая фишинг, взлом учетных записей, утечку персональных данных, распространение вредоносного ПО и DDoS-атаки. Анализируются ключевые уязвимости, связанные с человеческим фактором, слабой защитой сетевой инфраструктуры и недостаточным контролем доступа. Подчёркивается, что комплексное сочетание технических и организационных мер существенно повышает уровень киберзащиты образовательных учреждений.*

Ключевые слова: *кибербезопасность, образовательные учреждения, фишинг, вредоносное ПО, DDoS-атаки, персональные данные, аутентификация, шифрование, IDS/IPS, сетевая безопасность, кибергигиена.*

Цифровизация образовательной среды усилила зависимость учебных учреждений от информационных систем, что повышает их уязвимость перед киберугрозами. Как отмечает У. Столлингс, образовательный сектор становится одной из наиболее атакуемых сфер. Учреждения сталкиваются с фишингом, взломом аккаунтов, утечкой персональных данных и DDoS-атаками. Исследования Р. Андерсона показывают, что человеческий фактор остаётся ключевой причиной инцидентов. М. Бишоп подчёркивает, что слабая кибергигиена и недостаточная аутентификация значительно увеличивают риски.

Необходимость многоуровневой защиты обоснована в работах Б. Шнайера и Ч. Пфлегера. Авторы отмечают эффективность современных методов предотвращения угроз: многофакторной аутентификации, шифрования данных, IDS/IPS-систем, сетевой сегментации и мониторинга на основе ИИ.

Комплексная реализация технических и организационных мер, как указывают Кауфман–Перлман–Спесинер, существенно повышает уровень киберзащиты образовательных учреждений.

Методология исследования. Методологическая основа данного исследования включает комплексный подход к изучению киберугроз и методов их предотвращения в образовательных учреждениях. В работе использованы следующие методы:

Аналитический метод. Проведён анализ научных публикаций по кибербезопасности, включая работы У. Столлингса, Р. Андерсона, М. Бишопа, Б. Шнайера и Ч. Пфлегера. Особое внимание уделено источникам, содержащим данные о современных киберугрозах и технических средствах защиты.

Сравнительный метод. Выполнено сопоставление традиционных и современных методов обеспечения кибербезопасности, включая многофакторную аутентификацию, криптографические алгоритмы (AES, RSA), IDS/IPS-системы и решения на основе искусственного интеллекта.

Структурно-функциональный анализ. Проведено изучение структуры цифровой инфраструктуры образовательных учреждений и выделены ключевые компоненты, уязвимые к фишингу, утечкам данных и взлому учетных записей.

Метод экспертной оценки. Основные выводы сформированы с опорой на аналитические заключения ведущих специалистов в области кибербезопасности и данные международных стандартов (ISO/IEC 27001).

Современные образовательные учреждения всё больше зависят от цифровой инфраструктуры, что приводит к росту киберугроз. По данным У. Столлингса, учебные организации являются частыми целями фишинговых нападений, взломов учетных записей, распространения вредоносного ПО и DDoS-атак. Эти угрозы нарушают конфиденциальность, целостность и доступность данных, а также могут привести к остановке учебного процесса.

Значительная часть киберинцидентов связана с человеческим фактором. Как указывает Р. Андерсон, низкий уровень кибергигиены и недостаточные навыки пользователей создают дополнительные уязвимости. М. Бишоп подчёркивает, что слабые пароли и отсутствие многофакторной аутентификации значительно повышают риск компрометации учебных систем.

Современные методы защиты включают сочетание технических и организационных мер. К ключевым техническим инструментам относятся многофакторная аутентификация (MFA), шифрование данных с использованием алгоритмов AES и RSA, применение IDS/IPS-систем для выявления вторжений, а также использование искусственного интеллекта для анализа аномальной активности. Эффективность данных подходов подробно обоснована в работах Кауфмана, Перлман и Спесинера. Кроме того, Ч. Пфлегер подчёркивает важность защиты данных в образовательных системах посредством криптографических технологий.

Организационные меры включают обучение сотрудников и студентов основам кибергигиены, разработку и внедрение внутренней политики информационной безопасности, регулярные аудиты и тестирование на устойчивость к фишинговым атакам. Как отмечает Б. Шнайер, технические решения эффективны только в сочетании с грамотной и системной организацией процессов безопасности.

В целом, наиболее результативным подходом к обеспечению кибербезопасности образовательных учреждений является комплексное применение технических (MFA, шифрование, сетевой мониторинг) и организационных (обучение, регламенты, аудит) мер. Такая интеграция позволяет значительно снизить риск кибератак и повысить устойчивость образовательной инфраструктуры.

Проведённый анализ показывает, что образовательные учреждения становятся одной из наиболее уязвимых сфер в контексте современных киберугроз. Основные риски связаны с фишингом, взломом учетных записей, распространением вредоносного ПО и DDoS-атаками, что подтверждается исследованиями ведущих специалистов в области кибербезопасности. Значительная часть инцидентов обусловлена человеческим фактором и недостаточным уровнем цифровой грамотности пользователей.

Эффективное обеспечение киберзащиты возможно только при комплексном подходе, который сочетает технические и организационные меры. К наиболее результативным техническим инструментам относятся многофакторная аутентификация, криптографические методы защиты данных, IDS/IPS-системы и мониторинг аномальной активности с использованием технологий искусственного интеллекта. Организационные меры включают обучение сотрудников и студентов кибергигиене, разработку политики информационной безопасности и регулярные аудиты.

Обобщённые выводы показывают, что устойчивость образовательных учреждений к кибератакам существенно возрастает при интеграции многоуровневых защитных механизмов и системного управления кибербезопасностью. Такой подход позволяет минимизировать риски, обеспечить стабильность учебного процесса и защитить персональные данные всех участников образовательной среды.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Андерсон Р. Инженерия безопасности. – М.: Вильямс, 2020. – 1248 с.
2. Бишоп М. Компьютерная безопасность: искусство и наука. – М.: Диалектика, 2018. – 1296 с.
3. Кауфман К., Перлман Р., Спесинер М. Сетевая безопасность: частные коммуникации в публичной среде. – М.: Лаборатория знаний, 2016. – 752 с.
4. Менезес А., ван Ооршот П., Ванстоун С. Прикладная криптография. Справочник. – М.: Техносфера, 2019. – 810 с.
5. Пфлегер Ч., Пфлегер С. Безопасность в вычислительной технике. – СПб.: Питер, 2019. – 832 с.
6. Столлингс У. Основы сетевой безопасности: приложения и стандарты. – М.: Вильямс, 2020. – 504 с.
7. Шнайер Б. Прикладная криптография: протоколы, алгоритмы и исходный код на С. – М.: Вильямс, 2015. – 784 с.
8. ISO/IEC 27001:2022. Information Security Management Systems. – Geneva: ISO, 2022.
9. Закон Республики Узбекистан «Об информатизации». – Ташкент: Адолат, 2003 (в ред. 2021 г.).

10. Закон Республики Узбекистан «О персональных данных». – Ташкент: Народное слово, 2019.