

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

Murtazaeva Rabiga Maksetgalievna.

Город Нукус - Политехнум № 2.

Специальный учитель науки

Annotatsiya: raqamli texnologiyalar va internetning keng tarqalishi bilan birga, ta'lim muassasalarida kiberhujumlar va ma'lumotlarni yo'qotish xavfi ortib bormoqda. Ta'lim jarayonida talabalar, o'qituvchilar va ma'muriyat o'rtasida axborot almashinuvi ko'payganligi sababli, kiberxavfsizlik masalalari dolzarblashmoqda. ta'lim jarayonida kiberxavfsizlikni ta'minlash nafaqat talabalar va o'qituvchilarni himoya qilish, balki ta'lim muassasalari obro'sini saqlab qolish uchun ham zarurdir.

Kalit so'zlar: kiberxavfsizlik, ta'lim jarayoni, xavfsizlik texnologiyalari, ma'lumotlarni himoya qilish, axborot almashinuvi, raqamli texnologiyalar, foydalanuvchilarni o'qitish.

Аннотация: наряду с цифровыми технологиями и широко распространенным в Интернете, риск потери кибергаз и данных в образовательных учреждениях растет. В ходе образования киберэкспозиция является срочной из-за увеличения обмена информацией между студентами, учителями и администрацией. Обеспечение киберзащита в образовательном процессе необходимо не только для защиты студентов и учителей, но и для поддержания репутации учебных заведений.

Ключевые слова: CyberKawness, образовательный процесс, технология безопасности, защита информации, цифровые технологии, пользователи.

Annotation: Along with digital technologies and the widespread of the Internet, the risk of loss of cyberways and data in educational institutions is growing. In the course of education, cyberexophenness is being urgent due to the increase in information exchange between students, teachers and administration. Ensuring

cybergavity in the educational process is necessary not only to protect students and teachers, but also to maintain the reputation of educational institutions.

Keywords: *Cyberkawness, educational process, security technology, information protection, Digital Technologies, users of users.*

Кибербезопасность — это важная область, которая фокусируется на защите компьютерных систем, сетей, программ и данных от различных угроз, включая вредоносные атаки, незаконный доступ, потерю информации и взломы систем. С распространением Интернета и распространением цифровых технологий кибербезопасность стала серьезной проблемой и требованием во всем мире. Каждая организация и физическое лицо должны принять эффективные меры кибербезопасности для защиты своих данных и систем. особенно важно для веб-приложений и мобильных приложений. Безопасность операционных систем: обеспечение защиты операционных систем, особенно Windows, Linux и macOS. Сюда входит защита вашей системы от вредоносных программ, троянов и руткитов. Мобильная безопасность: защита данных и защита от вредоносного ПО на мобильных устройствах, таких как смартфоны и планшеты. Мобильная безопасность также включает безопасность мобильных приложений. Облачная безопасность: защита данных и ресурсов, хранящихся в облачных системах (облачные вычисления). Важно обеспечить доступ к облачным сервисам и инфраструктуре и шифрование данных. В соответствии с 21-х историческим процессом цифровые образовательные процессы интегрированы с широкими онлайн-платформами, электронными ресурсами и цифровыми услугами. Наряду с созданием новых возможностей, этот процесс также вызывает серию проблем с киберражом. Защита личной информации, учебных материалов и образовательных платформ студентов и учителей становится важной проблемой. Не быть защищенным от таких рисков может привести к проблемам с украденными и другими вредными действиями. Обеспечение кибергифизма не только стабильной работы образовательных учреждений, но и для защиты информации о процессе образования студентов и

защиты от внешних угроз. Обеспечение кибербезопасности обеспечивает защиту данных обучающихся и сотрудников образовательных учреждений, защиту от повреждения и несанкционированного доступа. Ниже мы рассмотрим основные меры, которые следует предпринять для обеспечения кибербезопасности в образовательных учреждениях. 1. Профилактика несанкционированного доступа к системе: использование сильной аутентификации, надежной и использования двухэтапных технологий аутентификации является важным показателем для контроля доступа к дистанционным системам образовательных учреждений.

2. Бронирование информационных систем - это копирование и восстановление информационных систем: для создания регулярных резервных копий и регулярного хранения их для минимизации данных.

1. Защита личной информации: чтобы обеспечить конфиденциальность личных данных студентов, учителей и других сотрудников посредством криптографической защиты и безопасного хранения.

2. Защита онлайн -образовательных платформ: для улучшения удаленного доступа (ссылки) к платформам дистанционного обучения и учебных программ для использования временной аутентификации и идентификационных систем. Эти платформы должны быть защищены, и пользовательские данные должны быть достаточно безопасно сохранены.

3. Профессиональное развитие сотрудников и студентов граждан в учреждении: обучение и круглые столы, чтобы защитить их от фишинговых атак, защиты фишинговых атак и защита личного программного обеспечения и разговоров по защите круглой защиты.

4. Профилактика несанкционированного доступа к системе: использование сильной аутентификации, надежные пароли для управления удаленными системами учебных заведений и использование двухэтапных технологий аутентификации является важным показателем. Механизмы ограничений на доступ к инструментам и системам обучения в Узбекистане введены в Узбекистане для защиты личной информации, цен, финансовой информации

некоторых университетов и их систем. Например, при введении с помощью личного пароля и входа в систему можно будет войти в систему любым другим человеком для студента. Например, в связи с паролем для входа в электронную почту университета, код подтверждения понадобится SMS для телефона пользователя. Этот дополнительный этап позволяет пользователям обеспечивать защиту от несанкционированного доступа. Кансы или университеты должны регулярно копировать свои собственные учебные программы и цены в облаке или на локальном сервере. Например, если все важные данные теряются с использованием Google Drive или OneDrive, они смогут быстро восстановиться. Для защиты данных необходимо использовать технологии шифрования. Это касается не только персональных данных, но и всей информации, используемой в образовательном процессе. Зашифровав данные, посторонним лицам становится трудно прочитать или изменить их. Образовательные учреждения должны обучать учителей и студентов кибербезопасности. Пользователей можно информировать, проводя тренинги, семинары и мастер-классы по кибербезопасности. Это поможет им узнать о кибератаках, научит их безопасному использованию Интернета и поможет избежать ошибок. Образовательные учреждения должны использовать технологии безопасности. Кибератаки можно защитить с помощью таких инструментов, как антивирусное программное обеспечение, системы сетевой безопасности и безопасные облачные сервисы для хранения данных. Это также позволяет быстро реагировать на потенциальные угрозы посредством мониторинга сети. Каждое образовательное учреждение должно разработать собственную политику кибербезопасности. Эта политика определяет, как хранятся данные, как предоставляется доступ и что делать в случае кибератаки. Политика кибербезопасности должна быть ясной и понятной всем пользователям. Обеспечение кибербезопасности в образовательном процессе – вопрос не только технический, но и культурный. Учителя и учащиеся должны научиться безопасно пользоваться Интернетом и уделять внимание защите своей личной

информации. Обеспечивая кибербезопасность, образовательные учреждения могут защитить своих пользователей и успешно работать в цифровом мире.

Использованная литература

1. Alnajim, A.M.; Habib, S.; Islam, M.; Albelaihi, R.; Alabdulatif, A. Mitigating the Risks of Malware Attacks with Deep Learning Techniques. *Electronics* 2023, 12, 3166.
2. Sharma, R. (2021). Data Protection and Privacy in the Education Sector. *Cybersecurity Journal*, 12(3), 45-60.
3. Morrison, C. (2022). *Educational Technology and Cybersecurity*. Routledge.
4. National Institute of Standards and Technology (NIST). (2018). *Cybersecurity Framework*. Available at: <https://www.nist.gov>
5. <https://in-academy.uz/index.php/ejar/article/download/44224/28107/47539>