НАУЧНЫЙ ЖУРНАЛ
НАУКА И МИРОВОЗЗРЕНИЕ

УДК-004

КИБЕРУГРОЗЫ В ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ: ЗАЩИТА ДАННЫХ СТУДЕНТОВ И ПРЕПОДАВАТЕЛЕЙ

Эркаева Наргуль
Преподаватель, Международного университета нефти и газа имени Ягшыгелди Какаева
г. Ашхабад Туркменистан

Нурыллаев Акмухаммет
Студент, Международного университета нефти и газа имени Ягшыгелди Какаева
г. Ашхабад Туркменистан

Ораздурдыева Менгли
Студент, Международного университета нефти и газа имени Ягшыгелди Какаева
г. Ашхабад Туркменистан

Оденепесова Аразгуль
Студент, Международного университета нефти и газа имени Ягшыгелди Какаева
г. Ашхабад Туркменистан

Аннотация

С развитием цифровых технологий образовательные учреждения все чаще сталкиваются с киберугрозами, угрожающими безопасности данных студентов и преподавателей. Внедрение онлайн-платформ, электронных дневников, облачных хранилищ и дистанционного обучения создаёт дополнительные риски утечки информации, кражи учетных записей и атак вредоносного программного обеспечения. В статье анализируются ключевые киберугрозы, которым подвержены образовательные учреждения, рассматриваются методы защиты данных и предлагаются эффективные стратегии повышения цифровой безопасности в учебных заведениях.

Ключевые слова: кибербезопасность, образовательные учреждения, защита данных, фишинг, учетные записи, вредоносное ПО, цифровые угрозы

1. Введение

В современном мире образовательные учреждения активно используют цифровые технологии для оптимизации учебного процесса, управления документами и коммуникации между студентами и преподавателями.

Онлайн-платформы, электронные дневники, системы управления обучением (LMS) и облачные сервисы обеспечивают удобный доступ к учебным материалам, однако делают учреждения уязвимыми перед киберугрозами.

Одной из главных проблем является недостаточная защищенность персональных данных, что делает их мишенью для злоумышленников. Утечка информации о студентах и преподавателях может привести к мошенничеству, краже личности и другим видам киберпреступлений. Кроме того, образовательные системы часто становятся жертвами атак программ-вымогателей, которые блокируют доступ к данным и требуют выкуп за их восстановление.

Фишинговые атаки представляют ещё одну значительную угрозу. Преступники рассылают поддельные письма и создают ложные сайты, вынуждая пользователей раскрывать конфиденциальную информацию. Недостаточная цифровая грамотность студентов и сотрудников повышает вероятность успешного обмана и компрометации учетных данных.

Кроме атак на персональные данные, образовательные учреждения подвергаются DDoS-атакам, направленным на перегрузку серверов и выведение из строя онлайн-платформ. Такие атаки могут нарушить работу электронных дневников, систем управления обучением и даже официальных сайтов университетов и школ.

Таким образом, обеспечение кибербезопасности в образовательных учреждениях является приоритетной задачей. Для защиты данных студентов и преподавателей необходимо внедрять современные технологии киберзащиты, обучать пользователей основам цифровой безопасности и разрабатывать комплексные стратегии предотвращения угроз.

2. Основные киберугрозы в образовательных учреждениях

2.1. Фишинг и компрометация учетных записей

Фишинг остаётся одним из наиболее распространённых методов кибератак на образовательные учреждения. Хакеры создают поддельные письма, выдавая их за официальную рассылку от администрации университета, технической поддержки или образовательных платформ. В таких письмах содержатся ссылки на фальшивые сайты, имитирующие интерфейс входа в систему.

После ввода логина и пароля данные автоматически попадают в руки злоумышленников, которые могут использовать их для доступа к образовательным ресурсам, электронным дневникам и личной информации студентов. В результате преступники могут изменять оценки, похищать личные данные или распространять вредоносное ПО от имени жертвы.

Фишинг также активно распространяется через социальные сети и мессенджеры. Злоумышленники могут отправлять сообщения от имени преподавателей или однокурсников с просьбой пройти по ссылке или загрузить документ. Неосведомленные пользователи часто становятся жертвами подобных атак.

Особую опасность представляют целенаправленные фишинговые атаки (спирфишинг), направленные на руководителей учебных заведений и системных администраторов. Если преступники получают доступ к аккаунтам с расширенными правами, они могут изменить базы данных, удалить важные документы или заблокировать работу целых систем.

Для защиты от фишинговых атак образовательные учреждения должны применять двухфакторную аутентификацию, использовать фильтры для обнаружения подозрительных писем и регулярно обучать студентов и преподавателей методам распознавания фишинговых атак.

2.2. Вредоносное ПО и программы-вымогатели

Программы-вымогатели представляют серьёзную угрозу для образовательных учреждений. Они проникают в систему через заражённые вложения в письмах, вредоносные сайты или внешние носители и шифруют файлы, требуя выкуп за их разблокировку. В случае отказа от оплаты учебное заведение может потерять доступ к важным данным.

Образовательные учреждения часто становятся мишенью таких атак из-за слабой защиты и устаревшего программного обеспечения. В 2020 году хакерские группировки атаковали несколько университетов, заблокировав серверы и парализовав учебный процесс.

Вредоносное ПО может также включать кейлоггеры, шпионские программы и бэкдоры, позволяющие хакерам отслеживать активность пользователей и получать удаленный доступ к системам. Если вирус попадает в сеть университета, он может распространяться на все подключенные устройства.

Для защиты от подобных атак необходимо регулярно обновлять программное обеспечение, использовать антивирусные программы и ограничивать права доступа к критически важным системам. Также важно проводить резервное копирование данных, чтобы в случае атаки можно было восстановить информацию без выплаты выкупа.

3. Методы защиты данных студентов и преподавателей

3.1. Политики информационной безопасности

Одним из ключевых элементов защиты образовательных учреждений является внедрение строгих политик информационной безопасности.

Такие политики должны включать правила использования паролей, процедуры резервного копирования данных и ограничения доступа к конфиденциальной информации.

Администрация вузов и школ должна контролировать использование служебных устройств и сетей, исключая возможность подключения посторонних USB-накопителей и неизвестных программ. Доступ к данным должен быть ограничен по принципу минимально необходимого уровня.

Также важно разрабатывать и регулярно обновлять инструкции по реагированию на инциденты, чтобы в случае атаки сотрудники знали, как действовать и минимизировать ущерб.

3.2. Обучение основам кибербезопасности

Один из самых эффективных методов защиты данных — обучение студентов и преподавателей основам информационной безопасности. Регулярные тренинги, лекции и интерактивные курсы помогают повысить уровень осведомлённости пользователей о потенциальных угрозах.

Студенты и сотрудники должны уметь распознавать фишинговые атаки, правильно настраивать пароли и использовать антивирусное ПО. Практические занятия с моделированием киберугроз помогут лучше усвоить принципы защиты.

Образовательные учреждения могут сотрудничать с экспертами по кибербезопасности, проводить тестирование на уязвимости и разрабатывать учебные программы по цифровой безопасности.

4. Технические меры защиты данных

Современные образовательные учреждения должны применять комплексные технические меры защиты данных, чтобы минимизировать риски кибератак и утечек информации. Одним из ключевых инструментов является использование антивирусного программного обеспечения и систем обнаружения вторжений (IDS/IPS), которые позволяют блокировать вредоносные программы и подозрительные сетевые активности.

Брандмауэры и системы контроля доступа также играют важную роль в предотвращении несанкционированного проникновения в сети образовательных учреждений. Настройка безопасных Wi-Fi-сетей, шифрование данных и ограничение привилегий пользователей помогают снизить вероятность атак злоумышленников.

Внедрение систем мониторинга безопасности (SIEM – Security Information and Event Management) позволяет выявлять аномальные действия в реальном времени и оперативно реагировать на возможные угрозы.

Такие системы помогают администраторам анализировать журналы событий, отслеживать попытки несанкционированного доступа и предотвращать атаки до их реализации.

Важным элементом является также регулярное резервное копирование данных. Хранение резервных копий в зашифрованном виде на независимых серверах позволяет быстро восстановить информацию в случае кибератаки, программного сбоя или утраты данных.

5. Правовые и этические аспекты защиты данных

Образовательные учреждения обязаны соблюдать нормативно-правовые акты, регламентирующие защиту персональных данных. В разных странах действуют свои законы: например, **GDPR (Общий регламент по защите данных) в Европе**, **Федеральный закон "О персональных данных" в России**, **FERPA (Закон о правах на образование и конфиденциальность семей) в США**. Эти акты определяют правила хранения, обработки и передачи персональной информации студентов и преподавателей.

Помимо законодательных требований, важную роль играют **этические принципы** защиты данных. Образовательные учреждения должны обеспечивать прозрачность в обработке информации, уведомлять студентов о сборе и использовании их данных, а также предоставлять возможность управления персональными сведениями.

Ответственность за кибербезопасность лежит не только на администраторах системы, но и на самих пользователях. Недопустимо передавать учетные данные третьим лицам, использовать слабые пароли и игнорировать предупреждения о возможных угрозах. **Формирование киберэтики среди студентов и преподавателей** способствует повышению уровня цифровой грамотности и снижает риски неосторожного обращения с конфиденциальными сведениями.

Также стоит учитывать **вопросы цифрового суверенитета**. Некоторые образовательные учреждения работают с иностранными облачными сервисами, что может повлечь за собой риски утечки данных за пределы страны. Важно выбирать платформы, соответствующие национальным требованиям безопасности, и обеспечивать защиту данных на локальных серверах.

6. Заключение

Киберугрозы представляют серьёзную опасность для образовательных учреждений, требуя комплексных мер по защите данных. Внедрение современных технологий безопасности, обучение основам кибербезопасности и разработка строгих политик защиты данных помогут минимизировать риски.

Использование многофакторной аутентификации, фильтрация подозрительных писем, регулярное обновление ПО и резервное копирование данных являются ключевыми мерами защиты.

Образовательные учреждения должны активно работать над созданием безопасной цифровой среды, обучая студентов и преподавателей эффективным методам защиты личных данных. Только комплексный подход обеспечит надежную киберзащиту учебных заведений.

Литература

1. Андерсон Р. **"Безопасность компьютерных систем. Принципы и практика"**. – М.: БИНОМ, 2022.
2. Сингх С. **"Код. Тайная история взломов и шифров"**. – СПб.: Питер, 2021.
3. Уильямс М. **"Киберугрозы и информационная безопасность"**. – Лондон: Oxford University Press, 2020.
4. Национальный институт стандартов и технологий США (NIST). **"Критерии безопасности информационных систем"**. – 2023.
5. OWASP Foundation. **"Руководство по защите веб-приложений от атак"**. – 2023.