УДК 621.762.4

Необходимость защиты информации в образовательном учреждении

Бабицкая Э. С., студент
Белорусский национальный технический университет,
г. Минск, Республика Беларусь
Научный руководитель: к. т. н., доцент Евтухова Т. Е.

Аннотация.

В статье рассматривается необходимость защиты информационной системы в образовательном учреждении, понятие информационная безопасность, а также предложены методы и шаги для защиты информации в данных учреждениях.

Информационная безопасность образовательного учреждения представляет собой комплекс мер направленных на реализацию защиты персональных данных и информационного пространства от несанкционированных вмешательств, хищения информации и изменения конфигурации системы со стороны третьих лиц и защиты учащихся от любых видов пропаганды, рекламы, запрещенной законом информации [1].

Информационная безопасность в образовательной среде в соответствии с законодательством предусматривает защиту сведений и данных, относящихся к следующим группам:

– персональные данные и сведения, которые имеют отношения к учащимся, преподавательскому составу, персоналу организации, оцифрованные архивные документы;

– обучающие программы, базы данных, библиотеки, другая структурированная информация, применяемая для обеспечения учебного процесса;

– защищенная законом интеллектуальная собственность.

Создание безопасной среды в образовательном учреждении – это ключевой аспект, к которому должно быть уделено должное внимание. В свете быстрого развития информационных технологий и доступа к интернету, необходимо понимать, что образовательные учреждения могут стать объектами атаки хакеров или злоумышленников,

которые могут украсть или уничтожить конфиденциальную информацию. Также нанести вред оборудованию или заразить систему вредоносными программами могут и сами учащиеся сознательно или ненамеренно. Это сделает образовательную среду уязвимой и подверженной потенциальным рискам.

Поэтому необходимо создать систему защиты информации в образовательном учреждении.

Следующие шаги могут помочь в защите информации в образовательном учреждении [2]:

1. Разработка политики безопасности информации (документ, определяющий правила и процедуры, которые используются для защиты информации и предотвращения утечек).

2. Аудит безопасности, включающий в себя проверку на наличие уязвимостей в системах защиты информации (поможет определить проблемы, которые могут статья уязвимыми для хакеров).

3. Обучение персонала по вопросам безопасности информации (обучение учащихся и сотрудников, которые имеют доступ к информации, по вопросам создания паролей).

4. Использование средств защиты информации – использование антивирусных программ, обновленного программного обеспечения, защиту паролей и других мер безопасности.

5. Резервное копирование информации (должно проводиться регулярно и находится в безопасном месте).

6. Мониторинг доступа к информации (поможет определить места, где данные могут быть нарушены.

7. Сотрудничество с внешними участниками, такими как IT-компании, может помочь в обеспечении безопасности информации.

Важно, чтобы все аспекты безопасности были учтены, так как нарушение безопасности информационных систем может иметь серьезные последствия для образовательной среды и всех ее участников. В конечном итоге это может привести к большим материальным и репутационным ущербам.

Один из наиболее важных моментов – является обучение пользователей безопасному использованию информационных технологий. Преподаватели и учащиеся должны быть осведомлены о потенциальных угрозах и должны уметь действовать в соответствии с правилами безопасности.

Важно проводить обучение на регулярной основе, поскольку технологии постоянно изменяются и возникают новые угрозы.

Другие аспекты безопасности информации включают в себя защиту от вирусов и злоумышленных программ, контроль доступа и аутентификацию, защиту сетевых соединений и безопасную утилизацию устаревшего оборудования. Кроме этого, важно обеспечить резервное копирование данных, чтобы в случае потери данных их можно было восстановить [3].

В целом, безопасная информационная среда в образовательном учреждении является неотъемлемой частью образования. Необходимость защиты информации должна быть признана и преподавателями, и учащимися. Разработка эффективной системы безопасности информации и обучение правилам безопасности являются главными инструментами в обеспечении безопасности и сохранении репутации образовательного учреждения.

В заключение, защита информации в образовательном учреждении – важная задача, которую необходимо решать всем вместе. Необходимо использовать комплексную стратегию, используя все возможные средства защиты информации, чтобы обеспечить безопасность конфиденциальных данных.

Список использованных источников

1. Информационная безопасность в образовательной организации – угрозы и их решение [Электронный ресурс] // www.smart-soft.ru. – Режим доступа: https://www.smart-soft.ru/blog/informatsionnaja_bezopasnost_v_obrazovateljnoj_organizatsii/. – Дата доступа: 14.03.2023.

2. Обеспечение защиты информации в образовательных организациях [Электронный ресурс] // moluch.ru. – Режим доступа: https://moluch.ru/archive/454/100167/. – Дата доступа: 14.03.2023.

3. Информационная безопасность общеобразовательного учреждения [Электронный ресурс] // elar.uspu.ru. – Режим доступа: http://elar.uspu.ru/bitstream/uspu/17031/2/Byjmov2.pdf. – Дата доступа: 14.03.2023.