18. ПРОБЛЕМЫ И ПРИНЦИПЫ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В УЧРЕЖДЕНИЯХ ВЫСШЕГО ОБРАЗОВАНИЯ

Гаврилюк М.Ю., студент гр.172302

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Федосенко В.А. – канд. техн. наук, доцент кафедры ЭИ

Аннотация: в современном обществе защита информации является одним из наиболее важных и актуальных вопросов. Для учреждений высшего образования, хранящих большое количество конфиденциальной информации о студентах, персонале, исследованиях и прочих данных, она является обязательным требованием. В статье рассмотрены проблемы и принципы системы защиты информации в учреждениях высшего образования и выделены наиболее важные аспекты безопасности данных, которые могут помочь учреждениям высшего образования повысить уровень информационной безопасности.

Ключевые слова: защита, информация, безопасность, учреждения высшего образования,

Современный университет – это кладезь разнообразной информации, требующей защиты. Речь идет о:

- персональных данных студентов, преподавателей, администрации и других категорий пользователей;
- разработанных университетом образовательных материалах, доступ к которым должен быть либо ограничен, либо контролируемым, т.к. они представляют собой интеллектуальную собственность;
- сведениях, составляющих коммерческую тайну университета и позволяющих ему опережать другие ВУЗы в области предоставления более качественного образования и образовательных программ, а также более прогрессивных методов обучения;
- приобретенных университетом программном обеспечении или лицензиях, кража которых может ухудшить положение учебного заведения в конкурентной борьбе либо повлечь за собой наступление уголовной или административной ответственности.

Несоблюдение требований информационной безопасности может привести к множеству проблем, таких как утечка конфиденциальной информации, взломы систем, повреждение репутации университета и нарушение законодательства, а также финансовые потери. Кроме того, высшие учебные заведения могут стать целью для киберпреступников и шпионов, которые могут использовать полученную информацию для своих целей, поэтому университеты должны уделять большое внимание вопросам информационной безопасности и разрабатывать эффективные системы защиты данных.

К наиболее распространённым проблемам системы защиты информации в учреждениях высшего образования относятся:

1. Уязвимые сети и системы. Многие университеты имеют устаревшие или неэффективные системы защиты, которые не могут предотвратить взломы или атаки хакеров. Уязвимости в сетях и системах учреждений высшего образования могут быть связаны с устаревшими системами защиты, недостаточной конфигурацией сетей, неправильным управлением доступом, недостаточной защитой от вредоносных программ, недостаточным мониторингом и др.
2. Низкая осведомленность о безопасности информации. Часто сотрудники и студенты не понимают важность безопасности информации и не принимают меры для защиты конфиденциальных данных.
3. Несоответствие законодательству. В некоторых случаях учреждения высшего образования не соблюдают требования законодательства по защите конфиденциальной информации, что может привести к нарушению конфиденциальности и потере доверия со стороны студентов и общества.
4. Недостаточная обученность персонала. Многие сотрудники учреждений высшего образования не имеют необходимых навыков и знаний по защите информации, что может привести к ошибкам и уязвимостям.
5. Недостаточное обновление программного обеспечения: Отсутствие своевременного обновления программного обеспечения на компьютерах и серверах может привести к уязвимостям в системах безопасности. Вирусы и другие типы вредоносных программ могут использовать эти уязвимости для получения доступа к конфиденциальной информации.

Атаки на внутренние сети могут быть одной из самых серьезных угроз для безопасности информации в учреждениях высшего образования. Они могут осуществляться различными способами, включая использование вредоносных программ, проникновение в уязвимые узлы сети, подбор паролей или фишинговые атаки на пользователей.

Для улучшения системы защиты информации в учреждениях высшего образования необходимо принять ряд мер, направленных на повышение осведомленности о безопасности информации и обучение персонала и студентов правилам безопасного обращения с конфиденциальными данными. Также необходимо внедрение современных систем защиты и обновление старых, а также соблюдение законодательства о защите информации и контроль доступа к конфиденциальной информации.

Необходимо установить и поддерживать обновленные и эффективные системы защиты, которые смогут предотвратить взломы или атаки хакеров. Важно также настроить правильную конфигурацию сетей, управление доступом и мониторинг системы.

Учреждениям высшего образования следует проводить регулярные аудиты безопасности для выявления уязвимостей и рисков, связанных с конфиденциальной информацией. Защита от вредоносных программ. Необходимо установить эффективное антивирусное программное обеспечение на всех компьютерах и серверах, чтобы предотвратить атаки вредоносных программ.

Чтобы защитить информацию в учреждениях высшего образования, необходимо проводить регулярное обучение персонала по принципам безопасности информации, которое должно быть обязательным и регулярным и охватывать как основные принципы безопасности, так и специфические политики и процедуры, применяемые в конкретном учреждении. Обучение должно включать в себя следующие вопросы: знакомство с основными понятиями информационной безопасности, такими как угрозы информационной безопасности, уязвимости и атаки; понимание типов угроз, которые могут быть использованы для атаки на системы, таких как фишинг, атаки на пароли, сброс паролей, вредоносные программы, сетевые атаки и т.д.; использование сильных паролей и меры по защите паролей, такие как двухфакторная аутентификация и др.

Использование программного обеспечения для управления информационной безопасностью может помочь университетам контролировать доступ к конфиденциальным данным, регулировать уровень доступа пользователей и мониторить угрозы безопасности.

Учреждения высшего образования также должны регулярно проводить аудит информационной безопасности, чтобы обнаруживать уязвимости в системе и принимать меры по их устранению.

Чтобы предотвратить атаки на внутренние сети, учреждения высшего образования должны принимать ряд мер по безопасности информации. Данные меры могут включать в себя:

1. Регулярное обновление программного обеспечения и обеспечение его безопасности: учреждения высшего образования должны регулярно обновлять и обеспечивать безопасность программного обеспечения на своих серверах и компьютерах. Это может помочь предотвратить уязвимости и атаки на внутренние сети.
2. Использование брандмауэров и антивирусного программного обеспечения: установка брандмауэров и антивирусного программного обеспечения на серверах и компьютерах может помочь предотвратить атаки на внутренние сети.
3. Ограничение доступа к чувствительной информации: учреждения высшего образования должны ограничивать доступ к чувствительной информации только тем пользователям, которые имеют на это полномочия. Это может помочь предотвратить случайный доступ к конфиденциальной информации.
4. Мониторинг сети: ВУЗы должны мониторить свои сети на предмет любой необычной активности. Это может помочь выявить атаки на внутренние сети в ранней стадии и принять меры по их предотвращению.
5. Обучение сотрудников: учреждения высшего образования должны обучать своих сотрудников правилам безопасности информации и как избегать фишинговых атак. Это может помочь сотрудникам узнать о возможных угрозах и принять меры по предотвращению атак на внутренние сети.
6. Формирование морально-этических норм толерантного поведения в информационных системах и адекватного ограничения от посещений агрессивных информационных пространств.

В целом, улучшение системы защиты информации в учреждениях высшего образования является необходимым шагом для защиты конфиденциальных данных, поддержания репутации и доверия со стороны студентов и общества. Однако, необходимо отметить, что безопасность информации является постоянной работой, и учреждения высшего образования должны регулярно обновлять свои меры по безопасности, чтобы обеспечить защиту от новых и современных угроз.

Список использованных источников:

1. Проталинский, О. М. Информационная безопасность ВУЗа/ Ажмухамедов, А. М.// Вестник АГТУ. Сер. Управление, вычислительная техника и информатика. – 2009. -№1. – С.18-23. - ISSN 2072-9502.

2. Труфанов, А. И. Политика информационной безопасности вуза как предмет исследования [Электронный ресурс]/ Труфанов, А. И. // Проблемы Земной цивилизации. – Вып. 9. – Иркутск: ИрГТУ, 2004. – Режим доступа: library.istu.edu/civ/default.htm.