УДК 004.056.5

СОВРЕМЕННЫЕ ПОДХОДЫ К ЗАЩИТЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ В УЧЕБНЫХ ЗАВЕДЕНИЯХ

Снитко Д.А.[1], Скиба И.Г. [2], Мигалевич С.А. [3]

[1]*Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь, laixdanik@gmail.com*
[2]*Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь, i.skiba@bsuir.by*
[3]*Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь, migalevich@bsuir.by*

Аннотация. Рассмотрены стратегии и меры, принимаемые университетом для обеспечения безопасности и конфиденциальности персональных данных в контексте растущих рисков обработки и хранения информации, включая применение методов обезличивания и современных технологий.

Ключевые слова. Безопасность информации, обезличивание данных, метод подмены, защита информационных ресурсов, безопасность данных.

Введение. Современные учебные заведения стремятся максимально эффективно использовать информационные технологии для улучшения образовательного процесса, управления и взаимодействия с участниками образовательной среды. Однако, с ростом объема персональных данных возрастают и риски, связанные с их обработкой и хранением. Белорусский государственный университет информатики и радиоэлектроники (БГУИР), будучи лидером в области технологий и образования, уделяет особое внимание безопасности персональных данных и применению методов обезличивания.

Защита персональных данных. Защита персональных данных обеспечивает уровень конфиденциальности, необходимый для создания доверительной образовательной среды. Студенты и сотрудники предоставляют свои персональные данные учебному заведению. Нарушение конфиденциальности может подорвать доверие и повлиять на общую атмосферу в университете. Персональные данные могут содержать финансовую и идентификационную информацию, которая может быть использована для мошенничества, кражи личности и других преступлений. Университет, сохраняя эти данные в безопасности, предотвращает потенциальные финансовые потери и защищает своих студентов и сотрудников от преступных действий. Студенты и преподаватели должны быть уверены в том, что их учебные и исследовательские достижения останутся конфиденциальными и не подвергнутся угрозе несанкционированного доступа. Принцип минимизации доступа играет значимую роль в обеспечении безопасности персональных данных в университете. Этот принцип предусматривает, что доступ к персональным данным имеет только минимальное количество сотрудников, необходимое для выполнения их профессиональных обязанностей. Даже разработчики, занимающиеся созданием и поддержкой информационных систем, не имеют прямого доступа к реальным персональным данным [1].

Закон о защите персональных данных. С 15 ноября 2021 года вступил в силу Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных». Данный правовой акт заложил основы правового регулирования вопросов защиты персональных данных, прав и свобод физических лиц при обработке их персональных данных. С учетом этого закона, организации и граждане обязаны строго соблюдать установленные нормы, гарантирующие конфиденциальность и безопасность личной информации. Принятие данного закона подчеркивает серьезное отношение Республики Беларусь к вопросам защиты персональных данных и соответствие международным стандартам в этой области. Он устанавливает принципы сбора, хранения и обработки данных, а также укрепляет права субъектов данных на контроль над своей информацией. Организации, осуществляющие обработку персональных данных, теперь обязаны принимать меры безопасности в соответствии с новым законодательством. Это включает в себя не только технические аспекты, такие как шифрование и управление доступом, но и организационные меры, например, проведение регулярных аудитов безопасности и обучение персонала в вопросах защиты данных [2].

Обезличивание персональных данных: Подход "подмены". Обезличивание персональных данных – это процесс обработки информации с целью удаления или изменения таких элементов, которые могут идентифицировать конкретное лицо. Цель обезличивания заключается в том, чтобы сохранить полезность данных для анализа, исследования или других целей, при этом обеспечивая анонимность индивида, к которому эти данные относятся. Обезличивание персональных данных в университете осуществляется с использованием метода "подмены". При работе с системой или в случае возникновения ошибок при заполнении данных в деканате, разработчики получают не реальные персональные данные, а их обезличенные аналоги [3].

Процедура обезличивания через "подмену" включает в себя следующие этапы:

Замена идентификаторов:

- Замена реальных имен на псевдонимы или случайные коды.
- Замена реальных номеров телефонов на фиктивные или обобщенные значения.

- Замена электронных адресов на анонимные или обобщенные адреса.

- Замена других уникальных идентификаторов случайными или обобщенными значениями.

Анонимизация:

- Удаление или замена конкретных данных, таких как адреса или имена, обобщенными значениями.

- Замена определенных частей информации значениями идентификатора другого человека или случайными данными.

Шифрование данных:

- Применение криптографических алгоритмов для защиты конфиденциальных данных.

- Шифрование данных в покое и в передаче.

Сокрытие дополнительных атрибутов:

- Обобщение дат, например, замена конкретных дней рождения на возрастные категории.

- Замена определенных частей информации данными другого человека или случайными значениями.

Обработка шума:

- Внесение случайных изменений в данные для того, чтобы затруднить восстановление оригинальной информации.

- Добавление небольших случайных отклонений к числовым значениям [4].

На рисунке 1 представлен алгоритм метода “подмены”.

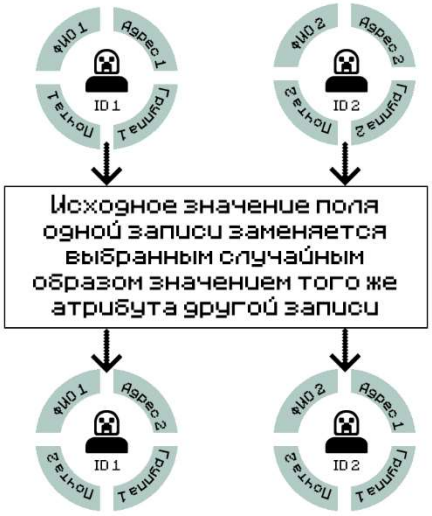

Рисунок 1 – Метод “подмены”

Преимущества подхода "подмены". Безопасность персональных данных: Реальные персональные данные остаются защищенными, так как разработчики имеют доступ только к обезличенным данным. Соответствие законодательству: Метод "подмены" соответствует требованиям законодательства о защите персональных данных, а также способствует повышению уровня доверия студентов и сотрудников к университету.

Способы защиты персональных данных:

Политика безопасности:

- Разработка строгой политики безопасности, включающей правила обработки, хранения и передачи персональных данных. Эта политика должна быть доступной всем сотрудникам и студентам и регулярно обновляться [5].

Обучение персонала и студентов:

- Проведение регулярных обучающих сессий по вопросам кибербезопасности для сотрудников и студентов. Обучение должно включать в себя правила создания безопасных паролей, распознавание фишинговых атак и другие аспекты информационной безопасности.

Управление доступом:

- Реализация систем управления доступом, определяющих уровни доступа для сотрудников, студентов и других пользователей. Ролевая модель может быть использована для предоставления минимально необходимых прав.

Шифрование данных:

- Применение шифрования данных на всех этапах их передачи и хранения. Это включает в себя использование SSL/TLS для защиты передачи данных через сеть и шифрование хранилищ данных.

Мониторинг и аудит безопасности:

- Внедрение систем мониторинга безопасности для обнаружения аномальной активности или попыток несанкционированного доступа. Регулярные аудиты безопасности помогут выявлять уязвимости и слабые места в системе.

Физическая безопасность:

- Обеспечение физической безопасности серверных комнат и центров обработки данных с использованием систем контроля доступа, видеонаблюдения и других физических мер безопасности.

Многомодальная аутентификация:

- Использование многомодальной аутентификации, такой как двухфакторная аутентификация (2FA) или биометрические данные, для повышения безопасности учетных записей пользователей.

Регулярные бэкапы и восстановление:

- Регулярное создание бэкапов всех важных данных и их тестирование на возможность восстановления. Это обеспечивает защиту от потери данных из-за случайного удаления, атак или технических сбоев.

Обновление программного обеспечения:

- Регулярное обновление операционных систем, прикладного программного обеспечения и антивирусных программ для устранения известных уязвимостей и обеспечения общей безопасности системы.

Соблюдение законодательства:

- Соблюдение всех применимых законов и нормативов в области защиты персональных данных о защите конфиденциальности.

Системы предотвращения утечек данных (*Data Loss Prevention, DLP*):

- Внедрение систем DLP для контроля и предотвращения утечек чувствительных данных, мониторинга их передачи внутри и за пределами университета [1].

Системы предотвращения утечек данных. Они представляют собой комплексный подход к обеспечению безопасности информации путем контроля, мониторинга и предотвращения утечек чувствительных данных из внутренних источников организации. Направлены на предотвращение непреднамеренного или злонамеренного раскрытия персональных данных. Основные аспекты систем DLP:

Идентификация и классификация данных:

- Системы DLP определяют чувствительные данные на основе их содержания, контекста и меток классификации.

Мониторинг сетевой активности:

- Системы следят за сетевой активностью, сканируя трафик и анализируя его в режиме реального времени. Они могут обнаруживать попытки передачи чувствительных данных через электронные письма, мессенджеры и другие каналы связи.

Контроль устройств и приложений:

- Системы DLP могут управлять доступом к устройствам и приложениям, ограничивая возможность копирования, вставки или передачи чувствительных данных через съемные носители, внешние диски, принтеры и другие устройства.

Шифрование и маскирование данных:

- Некоторые системы DLP предоставляют функционал шифрования или маскирования данных, что обеспечивает дополнительный уровень защиты в случае утечки или несанкционированного доступа.

Политики безопасности и управление правами доступа:

- Системы DLP позволяют настраивать политики безопасности в соответствии с требованиями учебного заведения. Это включает в себя управление правами доступа, определение критериев для срабатывания тревог и другие настройки.

Машинное обучение (Machine Learning) и аналитика:

- Использование технологий машинного обучения для выявления аномалий в поведении пользователей и сетевой активности. Это позволяет системе DLP адаптироваться к новым угрозам и сценариям утечек.

Интеграция с другими системами безопасности:

- Системы DLP могут интегрироваться с другими решениями безопасности, такими как системы управления угрозами (SIEM), антивирусные программы и системы контроля доступа [6].

Использование современных технологий в обеспечении безопасности. БГУИР активно внедряет современные технологии для обеспечения безопасности персональных данных. Криптографические методы шифрования применяются для защиты передаваемой информации между системами. Регулярные аудиты безопасности и мониторинг системы обнаружения инцидентов используются для выявления и предотвращения возможных угроз.

Обучение сотрудников и студентов в области безопасности данных. Создание безопасной информационной среды требует внимания к обучению сотрудников и студентов университета. Регулярные тренинги по вопросам безопасности данных и осведомление о возможных рисках помогают создать культуру ответственного отношения к обработке персональных данных.

Заключение. Вопросы защиты персональных данных и обезличивания играют важную роль в создании безопасной и информационной среды в учебных заведениях. Применение подхода "подмены" при обработке персональных данных позволяет балансировать необходимость использования информационных технологий с обязательством по обеспечению безопасности и конфиденциальности. Разработка и активное внедрение мер по защите персональных данных являются важным элементом стратегии университета, направленной на создание надежной и безопасной образовательной среды, где конфиденциальность каждого участника образовательного процесса является приоритетом.

Литература

1. Основные понятия и принципы защиты информации [Электронный ресурс] – Режим доступа: https://www.bsut.by/images/MainMenuFiles/Obrazovanie/Studentam/eumkd/et/euk_56_20/ch1/ch1_1/ch1_1_1.pdf

2. Закон Республики Беларусь “О защите персональных данных” [Электронный ресурс] – Режим доступа: https://etalonline.by/document/?regnum=h12100099&q_id=6232166

3. Обезличивание персональных данных [Электронный ресурс] – Режим доступа: https://data-sec.ru/personal-data/depersonalization/

4. Все, что вам нужно знать про обезличивание данных [Электронный ресурс] – Режим доступа: https://market.cnews.ru/articles/2023-09-03_vsechto_vam_nuzhno_znat_pro_obezlichivanie

5. Политика безопасности в отношении обработки персональных данных БГУИР [Электронный ресурс] – Режим доступа: https://www.bsuir.by/m/12_100229_1_157457.pdf

6. What is DLP? Data Loss Prevention [Электронный ресурс] – Режим доступа: https://www.netskope.com/security-defined/what-is-data-loss-prevention-dlp

MODERN APPROACHES TO PROTECTING INFORMATION RESOURCES IN EDUCATIONAL INSTITUTIONS

Snitko D.A. [1], Skiba I.G.[2], Migalevich S.A[3]

[1]*Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus, laixdanik@gmail.com*
[2]*Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus, i.skiba@bsuir.by*
[3]*Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus, migalevich@bsuir.by*

Abstract. The strategies and measures taken by the university to ensure the security and confidentiality of personal data in the context of the growing risks of processing and storing information, including the use of depersonalization methods and modern technologies, are considered.

Keywords. Information security, data depersonalization, substitution method, protection of information resources, data security.