УДК 004 **Информационные технологии**

Польченко Максим Александрович, *магистрант,*
ДГТУ Ростов-на-Дону, РФ
E-mail: polchenkomax@rambler.ru

БЕЗОПАСНОСТЬ БАЗ ДАННЫХ

Аннотация: В связи с растущим значением данных в современных организациях крайне важно, чтобы они принимали меры по обеспечению безопасности своих баз данных. Безопасность баз данных относится к процессу защиты баз данных от несанкционированного доступа, использования, раскрытия или уничтожения. В этой статье будет обсуждаться организация безопасности баз данных, включая различные меры безопасности, которые организации могут внедрить для защиты своих баз данных.

Ключевые слова: безопасность, база данных, технические меры защиты информации, мер информационной безопасности.

Abstract: Due to the growing importance of data in modern organizations, it is imperative that they take steps to ensure the security of their databases. Database security refers to the process of protecting databases from unauthorized access, use, disclosure, or destruction. This article will discuss the organization of database security, including the various security measures that organizations can implement to secure their databases.

Key words: security, database, technical information security measures, information security measures.

Введение

Организация безопасности баз данных предполагает многогранный подход, который охватывает как технические, так и нетехнические меры.

Первым шагом в организации безопасности базы данных является определение рисков и угроз для базы данных. Это включает в себя анализ типа данных, хранящихся в базе данных, точек доступа к базе данных и потенциальных уязвимостей, которые могут быть использованы хакерами или злоумышленниками. Как только риски будут определены, организации смогут разработать план обеспечения безопасности, учитывающий каждый из этих рисков [1].

В современную цифровую эпоху информация является ценным товаром, который необходимо защищать от несанкционированного доступа, кражи и неправильного использования. В связи с растущей зависимостью от технологий и растущей угрозой кибератак частным лицам и организациям стало крайне важно внедрять технические меры защиты информации для защиты своих данных.

Технические меры защиты информации относятся к использованию технологических решений для защиты информации от несанкционированного доступа, модификации или уничтожения [2]. Эти меры используются для обеспечения конфиденциальности, целостности и доступности информации.

Одной из наиболее распространенных технических мер защиты информации является **шифрование**. Шифрование предполагает использование математических алгоритмов для преобразования обычных текстовых данных в нечитаемый формат, который может быть расшифрован только тем, у кого есть ключ или пароль для его расшифровки. Шифрование используется для защиты передаваемых данных, таких как электронная почта, и данных в состоянии покоя, таких как файлы, хранящиеся на жестком диске или облачном сервере [3].

Брандмауэры являются еще одной важной технической мерой защиты информации. Брандмауэр — это система сетевой безопасности, которая отслеживает и управляет входящим и исходящим трафиком на основе заранее определенных правил безопасности. Брандмауэры могут быть реализованы на различных уровнях, включая сеть, хост и приложение, для предотвращения несанкционированного доступа и блокирования вредоносного трафика.

Антивирусное программное обеспечение также является важнейшей технической мерой защиты информации. Антивирусное программное обеспечение предназначено для обнаружения и удаления вредоносных программ, таких как вирусы, черви и троянские программы, с компьютера или сети. Антивирусное программное обеспечение использует обнаружение на основе сигнатур, поведенческий анализ и машинное обучение для выявления и удаления вредоносного программного обеспечения [4].

В дополнение к шифрованию, брандмауэрам и антивирусному программному обеспечению существуют другие технические меры защиты информации, которые организации могут внедрить для защиты своих данных. К ним относятся системы обнаружения и предотвращения вторжений, информация о безопасности и системы управления событиями, двухфакторная аутентификация, контроль доступа, а также сканирование и оценка уязвимостей.

Системы обнаружения и предотвращения вторжений (IDLS) используются для мониторинга сетевого трафика, обнаружения и предотвращения несанкционированного доступа и атак. IDPS можно настроить для оповещения групп безопасности или выполнения автоматических действий по блокированию вредоносного трафика [1].

Системы информации о безопасности и управления событиями (SIEM) используются для сбора и анализа данных, связанных с безопасностью, из множества источников, таких как брандмауэры, системы обнаружения вторжений и антивирусное программное обеспечение. SIEM-системы предоставляют службам безопасности информацию о потенциальных угрозах в режиме реального времени и помогают им быстро реагировать на инциденты безопасности.

Двухфакторная аутентификация (2FA) - это мера безопасности, которая требует от пользователей предоставления двух форм идентификации для доступа к системе или приложению. Это может включать пароль и биометрический фактор, такой как отпечаток пальца или распознавание лица.

Средства контроля доступа используются для ограничения доступа к конфиденциальным данным и ресурсам на основе роли и разрешений пользователя. Средства контроля доступа могут быть реализованы на различных уровнях, включая физический, логический и административный.

Сканирование и оценка уязвимостей используются для выявления и устранения уязвимостей в сети и приложениях организации. Сканирование уязвимостей включает автоматическое сканирование сети или системы для выявления уязвимостей, в то время как оценка уязвимости включает ручное тестирование и анализ средств контроля безопасности.

Нетехнические меры обеспечивают уровень защиты на случай, если технические меры потерпят неудачу. Хотя брандмауэры и шифрование эффективны, они не являются надежными. Злоумышленники все еще могут находить уязвимости и использовать их. Нетехнические меры, такие как планы резервного копирования и восстановления, могут помочь организациям быстро восстановиться после нарушений безопасности. Планы аварийного восстановления могут помочь организациям восстановить данные и системы после атаки, в то время как планы резервного копирования могут гарантировать, что критически важные данные не будут потеряны [5].

Нетехнические меры могут помочь организациям соблюдать правовые и нормативные требования. Во многих отраслях, таких как здравоохранение и финансы, действуют строгие правила, касающиеся безопасности данных и конфиденциальности. Нетехнические меры, такие как контроль доступа, могут помочь организациям гарантировать, что только авторизованный персонал может получить доступ к конфиденциальным данным. Политика и процедуры также могут гарантировать, что организации соблюдают нормативные акты и избегают дорогостоящих штрафных санкций.

Существует множество эффективных нетехнических мер информационной безопасности, которые могут внедрить организации. Одним из наиболее важных является контроль доступа, который гарантирует, что только авторизованный персонал может получить доступ к конфиденциальным данным.

Это может быть достигнуто с помощью паролей, двухфакторной аутентификации или биометрической идентификации. Регулярная смена паролей и ограничения на совместное использование паролей также могут помочь предотвратить несанкционированный доступ [3].

Еще одной эффективной мерой являются программы обучения и повышения осведомленности сотрудников. Обучая сотрудников передовым методам обеспечения безопасности, организации могут свести к минимуму риск человеческой ошибки. Учебные программы могут охватывать такие темы, как фишинг, социальная инженерия и защита паролем. Регулярные кампании по повышению осведомленности о безопасности также могут помочь укрепить эту практику и создать культуру осведомленности о безопасности.

Заключение (выводы). Политика и процедуры также являются важными нетехническими мерами. Политики могут определять приемлемое использование ресурсов компании, политику паролей и процедуры обработки данных. Процедуры могут описывать, как данные должны храниться, передаваться и утилизироваться. Внедряя политику и процедуры, организации могут гарантировать, что сотрудники следуют лучшим практикам и соблюдают нормативные акты.

Библиографический список:

1. Александров, В.В. Информационное обеспечение интегрированных производственных комплексов / В.В. Александров, Ю.С. Вишняков, Л.М. Горская, и др.. - М.: Машиностроение, 2018. - 264 с.

2. Ассанж, Дж. Шифропанки. Свобода и будущее Интернета / Дж. Ассанж. - М.: Азбука, 2014. - 418 с.

3. Бабенко, Л. К. Параллельные алгоритмы для решения задач защиты информации / Л.К. Бабенко, Е.А. Ищукова, И.Д. Сидоров. - Москва: ИЛ, 2014. - 304 с.

4. Болотов, А. А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. - М.: КомКнига, 2014. - 306 с.

5. Голицына, О. Л. Базы данных / О.Л. Голицына, Н.В. Максимов, И.И. Попов. - М.: Форум, 2019. - 400 с.