УДК004.056

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

Трофимов Р.А., студент гр. 110402-ИТСа-019, II курс
Научный руководитель: Губачев В.А., к.э.н., доцент
Южно-Российский государственный политехнический университет (НПИ)
имени М.И. Платова
г. Новочеркасск

История исследований баз данных насчитывает более тридцати лет, в течение которых была создана концепция реляционной системы баз данных, ставшая самым фундаментальным изменением стратегии организации. Как указывает А.М. Эльдарханов, в 1968 году была введена в эксплуатацию первая промышленная система управления базами данных- система IMS фирмы IBM - именно эта дата определена временем рождения [5].

В последнее десятилетие эволюция технологий привела к появлению более мощных систем, обеспечивающих защиту баз данных от неблагоприятных экономических последствий в форме потери сведений или их незаконного использования.

Очевидно, что сегодня организации должны обеспечить безопасность и конфиденциальность своей информации. Защита означает запрет незаконным пользователям доступа к базе данных и ее конфиденциальной информации, вне зависимости от характера доступа: преднамеренного или случайного [4]. Поэтому большинство фирм принимают во внимание возможность угроз в качестве мер для своих систем баз данных.

Система управления базами данных (СУБД) - это программноеобеспечение, позволяющее создавать базы данных и управлять ими. Иногда в научной литературе встречается и несколько иное определение: система управления базами данных (СУБД) - это программное обеспечение для хранения и извлечения данных пользователей с учетом соответствующих мер безопасности[3].

В последнее время развертывают системы или приложения, имеющие функции, службы и инструменты для обслуживания и управления данными - систему управления реляционными базами данных (РСУБД). Такие функции содержат возможности установить определенные привилегии для авторизации, чтобы сохранить законным (авторизованным) пользователям доступ к базе данных.

Как известно, в последние годы аппаратные возможности иповсеместное использование платформ Всемирной Паутины и информационных систем привели к принятию реляционных систем баз данных в качестве инфраструктуры хранилища данных. Огромные объемы

данных и информации стали главной проблемой безопасности, поскольку управление информацией стало децентрализованным. Именно конфиденциальность, целостность и доступность должны стать основой концепции безопасности реляционных баз данных. Эти факторы должны быть включены в прикладные процессы, чтобы гарантировать безопасность данных [1].

Воровство и мошенничество оказывают влияние на среду баз данных. Эти преступные действия чаще не являются внесением изменений в сами данные, однако, могут привести к снижению конфиденциальности и целостности закрытой информации субъекта. Нарушения безопасности, приводящие к потере конфиденциальности, могут привести к потере конкурентоспособности организации. Нарушение целостности означает, что данные повреждены и изменены. Многие организации стремятся к доступности 24/7. Потеря доступности означает, что система, или данные, или и то, и другое не могут быть доступны. Поэтому система управления реляционными базами данных направлена на снижение потерь, вызванных угрозами или ожидаемыми событиями.

К основным мерам обеспечения безопасности баз данных можно отнести следующие: контроль и управление доступом, аутентификация, резервное копирование, шифрование.

Контроль доступа к базе данных-это способ предоставления доступа к конфиденциальным данным компании только тем лицам (пользователям базы данных), которым разрешен доступ ктаким данным, и ограничения доступа посторонним лицам.

Контроль доступа - это метод безопасности, который регулирует, кто или что может просматривать или использовать ресурсы в вычислительной среде. Это фундаментальная концепция безопасности, которая сводит к минимуму риск для бизнеса или организации.

Целью контроля доступа является минимизация риска несанкционированного доступа к базам данных. Контроль доступа-это фундаментальный компонент программ обеспечения соответствия требованиям безопасности, который обеспечивает наличие технологий безопасности и политик контроля доступа для защиты конфиденциальной информации, такой как данные клиентов. Большинство организаций имеют инфраструктуру и процедуры, ограничивающие доступ к сетям, компьютерным системам, приложениям, файлам и конфиденциальным данным, таким как личная информация и интеллектуальная собственность.

Системы контроля доступа сложны и могут быть сложными для управления в динамических ИТ-средах, включающих локальные системы и облачные сервисы. После некоторых громких нарушений поставщики технологий перешли от систем единого входа (SSO) к единому управлению доступом, которое предлагает контроль доступа для локальных и облачных сред.

Управление доступом - это процесс, который интегрирован в ИТ-среду организации. Она может включать в себя системы управления идентификацией и доступом. Эти системы предоставляют программное обеспечение для контроля доступа, базу данных пользователей и инструменты управления политиками контроля доступа, аудита и принудительного применения.

Когда пользователь добавляется в систему управления доступом, системные администраторы используют автоматизированную систему подготовки для настройки разрешений на основе структур управления доступом, должностных обязанностей и рабочих процессов.Наилучшая практика наименьших привилегий ограничивает доступ только к тем ресурсам, которые требуются сотрудникам для выполнения их непосредственных должностных функций [3].

Контроль доступа включает в себя два основных компонента: аутентификацию и авторизацию.

Аутентификация - это процесс, который подтверждает личность пользователя и обеспечивает доступ к конфиденциальной информации.Традиционно это делается с помощью имени пользователя и пароля. Пользователь вводит свое имя пользователя, что позволяет системе подтвердить его личность. Эта система опирается на тот факт, что (надеюсь) только пользователь и сервер знают пароль.Процесс аутентификации веб-сайта работает путем сравнения учетных данных пользователя с данными в файле. Если совпадение найдено, процесс аутентификации завершен, и пользователь может быть «передвинут» в процесс авторизации.

Аутентификация паролем является наиболее распространенным способом подтверждения личности пользователя, однако, не относится к наиболее эффективному или безопасному методу. Есть еще типы аутентификации, которые являются более надежными для обеспечения защиты баз данных.

Например, биометрическая аутентификация, которая включает в себя любой метод, который требует биологических характеристик пользователя для проверки его личности. Сканирование отпечатков пальцев является наиболее известной формой биометрической аутентификации, но инструменты распознавания лиц становятся все более популярным выбором как для разработчиков, так и для пользователей.

Еще одним типом защиты баз данных является аутентификация по электронной почте, которая позволяет пользователям безопасно входить в любую учетную запись, используя только адрес электронной почты.

Аутентификация-это метод проверки личности человека, который получает доступ к вашей базе данных. Аутентификации недостаточно для защиты данных. Требуется дополнительный уровень безопасности-авторизация, которая определяет, должен ли пользователь получить доступ к данным или совершить транзакцию, которую он пытается совершить. Без аутентификации и авторизации нет никакой безопасности данных.

Любая компания, сотрудники которой подключаются к Интернету, таким образом, каждая компания сегодня нуждается в некотором уровне реализованного контроля доступа.

Защита данных предполагает наличие резервных копий, из которых можно выполнить их восстановление. Для большинства компаний и организаций резервное копирование данных относится к числу наиболее важных приоритетов в рамках обеспечения защиты базы данных. Около половины компаний работают со своими данными как со стратегическим активом. И ценность хранимых данных постоянно растет. Их используют для повышения качества обслуживания клиентов, поддержки текущей деятельности, исследований и разработок, учета, они задействованы в системах автоматизации, интернета вещей, искусственного интеллекта и др. Именно резервное копирование обеспечивает защиту баз данных от аппаратных сбоев, человеческих ошибок, вирусов и кибератак [4].

Заметным событием последних лет стала законодательная и нормативная конвергенция в области шифрования как ключевого инструментазащиты безопасности баз данных, неструктурированныхданных, облачных и прикладных данных. В некоторых странахтребование о развертывании шифрования установлено в правовых и нормативных стандартах; в других странах шифрование неявноодобряется как легкодоступное, стандартное для рынка решение,которое защищает бизнес от самых неблагоприятных правовых последствий нарушения конфиденциальности баз данных.

Хотя шифрование не является панацеей от всех угроз безопасности, оно является важным инструментом в борьбе с конкретными угрозами безопасности. В частности, быстрый рост электронного бизнеса стимулировал увеличение шифрования хранимых данных, таких как номера кредитных карт.

Основной принцип шифрования хранимых данных заключается в том, что они не должны мешать контролю доступа. Любой пользователь, имеющий привилегию доступа к данным в базе данных, не имеет ни больше, ни меньше привилегий в результате шифрования. Поэтому шифрование никогда не должно использоваться для решения проблем контроля доступа [1, 2].

Шифрование хранимых данных не должно мешать администрированию базы данных, поскольку в противном случае могут возникнуть более серьезные проблемы с безопасностью. Например, если при шифровании данных они коррумпируются, то создается проблема безопасности и сами данные становятся не поддающимися интерпретации, и, соответственно, их невозможно восстановить.

Процесс шифрования конфиденциальных данных требует высокой производительности системы, поскольку ему потребуется расшифровка этих данных. Поэтому важно обеспечить использование оптимизированных алгоритмов безопасности при кодировании баз данных.

Таким образом, к основным мерам обеспечения безопасности баз данных можно отнести контроль и управление доступом, аутентификация, резервное копирование, шифрование. Их применение усилит защиту информации и соответственно экономическое благополучие субъекта – правообладателя баз данных.

Список литературы:

1. Власова О.А. Защита и безопасность базы данных / Решетневские чтения. 2017. С. 317-321.
2. Полтавцева М.А. Безопасность баз данных: проблемы и перспективы / Программные продукты и системы. 2016. С. 15-19.
3. Петрянин Д.Л. Анализ систем защиты информации в базах данных / Труды международного симпозиума «Надежность и качество». 2013. С. 112-115.
4. Скакун В.В. Защита информации в базах данных и экспертных системах: пособие для студентов фак. радиофизики и комп. технологий / В. В. Скакун. Минск: БГУ. 2015. С. 78.
5. Эльдарханов А.М. Обзор моделей данных объектно-ориентированных СУБД / Труды Института системного программирования РАН. 2011. С. 205-208.