"Крипто БД" – сертифицированная система предотвращения утечек информации из СУБД

Денис Суховей, *директор по развитию бизнеса компании "Аладдин"*


Фото: Аладдин

Защита конфиденциальности информации в СУБД является одной из основных задач для многих компаний и государственных организаций. Система "Крипто БД" позволяет осуществлять выборочное динамическое шифрование информации, хранящейся в таблицах базы данных.

"Крипто БД" является наложенным средством защиты информации и не затрагивает штатные механизмы обработки информации в СУБД. При этом обеспечиваются дополнительный контроль доступа к защищенным данным, а также регистрация всех операций с ними, независимо от уровня привилегий пользователей СУБД.

Система реализует шифрование таблиц и/или столбцов базы данных, двухфакторную аутентификацию, необратимое удаление данных, централизованный мониторинг и аудит, разграничение доступа на основе ролевой модели.

Сценарий 1. Защита информации в СУБД при взломе

При атаках на информационные системы злоумышленники стремятся получить управление над функциями и параметрами информационной системы и СУБД, системными журналами, чтобы похитить или скомпрометировать информацию.

Система "Крипто БД" предотвращает эти угрозы, защищая информацию в СУБД с помощью устойчивого к криптоанализу шифрования, исключающего компрометацию в разумные сроки (ГОСТ 28147-89, ГОСТ 34.12–2015).

Сценарий 2. Защита от действий администратора СУБД

Администратор СУБД – это привилегированная, но не контролируемая роль, которая часто является слабым звеном в защите данных. "Крипто БД" обеспечивает защиту от действий администратора СУБД: администратор не имеет ключей шифрования, все попытки доступа фиксируются, реализован принцип разделения полномочий и ответственности. Но при этом администратор может выполнять свои обязанности без ограничений.

Сценарий 3. Разграничение доступа к защищаемой информации

Разграничение доступа к данным часто реализуется неоптимальным образом: на уровне сервера приложений, через пользовательский веб-интерфейс, без усиленной аутентификации. Эти методы легко обходятся манипуляцией запросами, оставляя данные в СУБД незащищенными.

Система "Крипто БД" обеспечивает надежное разграничение доступа: поддерживаются гибкая ключевая схема для удобного назначения доступа и расширенная ролевая модель для контроля доступа выделенным сотрудником безопасности.

Сценарий 4. Защита при размещении СУБД в облаке

Перенос информационной системы в облако сопряжен с рисками утечек, например через неконтролируемый и нефиксируемый физический доступ третьих лиц к серверам СУБД.

Использование системы "Крипто БД" для защиты информации в облаке снижает эти риски, ведь даже при прямом доступе к серверу злоумышленник получит лишь зашифрованные данные.

Сценарий 5. Защита резервных копий и архивов

Защита информации в архивах резервных копий является непростой задачей. Механизмы безопасности должны быть настроены таким образом, чтобы не нарушать процессы резервного копирования, а в случае кражи архивов обеспечить сохранение конфиденциальности данных. Восстановление информации при этом должно оставаться прозрачным, а хранение архивов – соответствовать нормативным требованиям, таким как 187-ФЗ и приказ № 21 ФСТЭК России.

За счет того, что "Крипто БД" защищает данные в таблицах СУБД шифрованием, данные в архивах по умолчанию защищены, что исключает угрозы потери конфиденциальности при краже их резервных копий.

Сценарий 6. Маскирование и деперсонализация информации

Для тестирования информационных систем или в целях проведения расследований часто требуется выполнять репликацию баз данных. При этом возникает задача защиты информации в реплицированных данных, которые тем не менее должны оставаться актуальными и соответствовать реальным объемам исходных данных.

Система "Крипто БД" решает эту проблему, реализуя гибкое динамическое маскирование. В результате после репликации реальные конфиденциальные данные не покидают СУБД.

Сценарий 7. Надежное уничтожение персональных данных

При выводе информационной системы из эксплуатации данные в СУБД должны быть надежно уничтожены без возможности восстановления. Эта же процедура требуется и при модернизации системы, изменении информационной модели и оптимизации структур данных в СУБД.

Система "Крипто БД" решает эту проблему, шифруя всю критичную информацию стойкими алгоритмами. При неавторизованном восстановлении данных злоумышленник получит лишь зашифрованный массив.

Сценарий 8. Независимый аудит доступа к информации

Эффективность расследования инцидентов зависит от актуальности и достоверности собираемых данных. Система "Крипто БД" позволяет собирать и обрабатывать информацию о доступе пользователей и администраторов к защищенным данным в СУБД, включая фиксацию событий доступа к защищаемой информации, передачу данных внешним системам (например, SIEM), защиту логирования от возможных злонамеренных действий со стороны администратора.

В заключение

"Крипто БД" сертифицирована ФСБ России как средство криптографической защиты информации классов КС1 и КС2, что позволяет использовать ее для защиты информации, не содержащей сведений, составляющих государственную тайну.

Решение включено в единый реестр отечественного ПО. ●