

Реальные угрозы использования зарубежных платформ СУБД



text: Денис Суховой, руководитель департамента развития технологий компании «Аладдин Р.Д.»

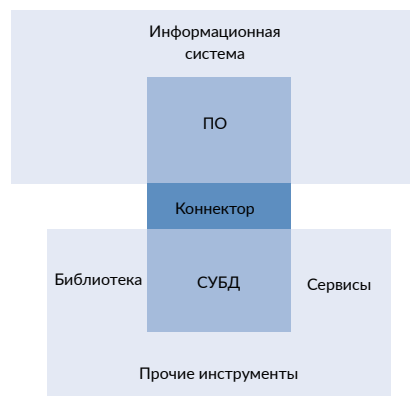


text: Анна Горшкова, продакт маркетинг менеджер компании «Аладдин Р.Д.»

Развитие крупных информационных систем (ИС) в России длительное время шло в неразрывной связке с Oracle и MS SQL. Другие СУБД не имели такого широкого распространения.

ИС в том виде, в котором они сейчас существуют, формировались долго. Выбор платформы СУБД для будущей ИС очень важен — это одна из основополагающих частей ИТ-инфраструктуры. Поэтому применение Oracle и MS SQL было не просто удобным, а практически безальтернативным: помимо распространенности, они обладали еще и сопутствующей

Схема «Архитектура информационной системы при использовании Oracle»



экосистемой из сервисов, библиотек разработки и прочих инструментов, а также развитым сообществом специалистов. Особенностью использования этих платформ является многослойная программная архитектура бизнес-приложений, написанных специально под них.

В идеале в архитектуре ИТ-инфраструктуры должен быть предусмотрен коннектор, который позволяет всему ПО быть независимым от СУБД. Это дает инфраструктуре гибкость при необходимости замены СУБД.

Схема «Проблема замены СУБД в архитектуре информационной системы»



Однако, когда речь идет об Oracle DB и MS SQL, замена СУБД влечет за собой потерю значимой части экосистемы, что часто приводило и по сей день приводит к замедлению принятия решения (например, о замене на отечественный аналог) либо к полному отказу от внедрения каких-либо изменений.

По некоторым наблюдениям, до 85% значимых информационных систем России так и не удалось перевести на новые, безопасные платформы СУБД в рамках импортозамещения.

Зависимость программного обеспечения в информационных системах от встроенных сервисов западных СУБД крайне высокая. Бизнес-приложения глубоко интегрированы в систему, поэтому резкий переход от зарубежных платформ к российским осуществить сложно. Более семи лет — с момента активизации программы импортозамещения — не было фактора,

который бы сдвинул с мертвой точки этот процесс, потому что это тянуло за собой неприятную череду трансформаций в ИТ-архитектуре и возможное замедление бизнес-процессов.

В 2022 году владельцы крупных информационных систем столкнулись с внезапным уходом зарубежных вендоров СУБД с российского рынка. Время, которое могло быть потрачено на плавный и безболезненный переход, упущено, а к уже знакомым рискам добавились новые. Чаще всего фокус внимания бизнеса сконцентрирован на угрозе отзыва технической поддержки СУБД со стороны производителя, но мало кто задумывается, что при продолжении использования Oracle и MS SQL могут возникнуть более острые проблемы, связанные с безопасностью ценных информационных ресурсов, хранящихся в этих базах данных.

В условиях политического противостояния западные вендоры СУБД действительно могут осуществить отзыв лицензий как права на использование ПО СУБД. Это проблема больше административная, чем техническая. Инструменты обхода и оптимизации такой хищнической лицензионной политики вендора хорошо известны в нашей стране, а технические процедуры резервирования данных и ПО, как правило, хорошо освоены отечественными ИТ-специалистами.

Более существенным является риск дистанционной блокировки СУБД со стороны производителя, и сегодня уже существуют реальные примеры подобных вмешательств. При таком сценарии организация-пользователь теряет доступ к обрабатываемой в СУБД информации. Потеря контроля над СУБД может повлечь возникновение цепочки новых угроз информационной безопасности — нарушение целостности и конфиденциальности информации в заблокированной СУБД, превращение отлаженной и работающей системы в «кирпич». Причем в «кирпич» СУБД превращается для владельца системы, но это абсолютно не значит, что

в этот момент она недоступна для злоумышленника.

Так называемое «окирпичивание» может стать крайне болезненным средством давления «коллективного Запада» на опорные отечественные организации или ведомства: такие мероприятия осуществляются не для запугивания, они носят сугубо целевой характер и выводят из строя отечественные информационные системы.

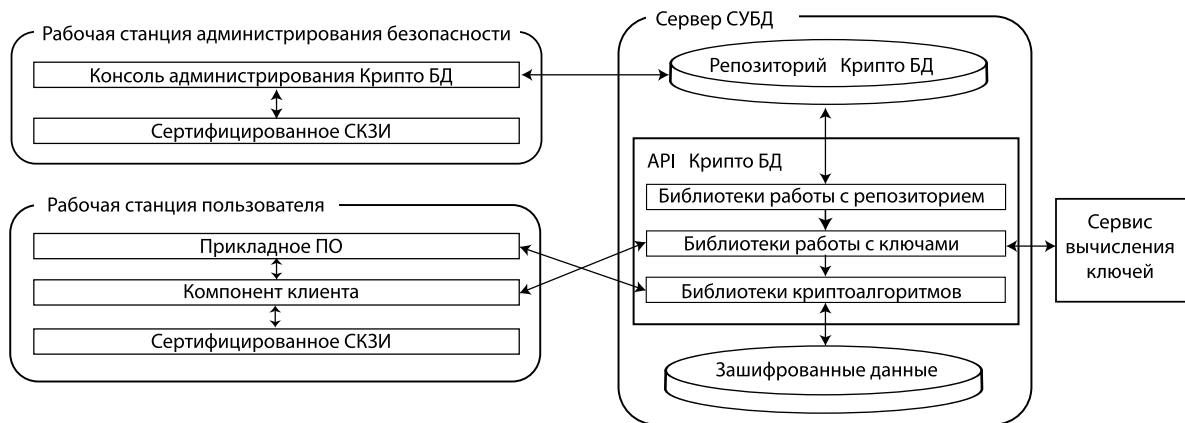
Таким образом, крупные российские организации оказались в непростой ситуации — полноценное замещение импортных СУБД в отдельно взятой информационной системе займет не менее 1,5–2 лет, но угроза санкционного давления существует прямо сегодня. Что делать?

Золотое правило импортозамещения в области ИТ гласит: «Если не можешь быстро заместить платформу, замещаешь средства защиты информации внутри неё». Оперативная защита информации доверенными и безопасными инструментами сможет резко снизить уровень новых угроз и создать необходимый задел по времени для реализации осознанного и поэтапного перехода на новую платформу СУБД. И такие средства защиты информации на отечественном рынке есть. Система защиты информации в базах данных «Крипто БД» компании «Аладдин Р.Д.» является отличным примером оперативного устранения угроз безопасности информации в базах данных.

Программный продукт «Крипто БД» изначально спроектирован и построен как система защиты, позволяющая решать задачи импортозамещения. «Крипто БД» поддерживает сразу несколько платформ баз данных, что позволяет защитить информацию в исходной СУБД (например, Oracle или MS SQL) и одновременно в новой, строящейся (например, Postgres Pro или PostgreSQL).

Защитные механизмы «Крипто БД» основаны на реализации стойких отечественных криптоалгоритмов и соответствуют всем требованиям ФСБ России к СКЗИ. Это позволяет системе защиты

Схема взаимодействия компонентов



обеспечивать противодействие наиболее критичным угрозам — нарушению целостности и конфиденциальности информации.

Функции и возможности «Крипто БД»

Шифрование таблиц/столбцов базы данных. Эта функция позволяет зашифровывать отдельные столбцы таблиц в СУБД. Ее уникальность заключается в том, что в одно и то же время авторизованным пользователям она позволяет видеть расшифрованные данные, а всем остальным — их маскирующие значения. Авторизованным пользователем является тот, кто имеет доступ к ключу шифрования. Этот доступ должен быть назначен администратором безопасности. Такой метод защиты исключает нежелательный доступ к данным со стороны системного администратора, обладающего высочайшим уровнем привилегий в ИТ-системе. Защита основана на использовании наиболее актуальных отечественных алгоритмов шифрования.

«Прозрачность» для приложений. Приложения, работающие с незашифрованными данными, после шифрования таблиц с помощью «Крипто БД» не требуют какой-либо доработки как на стороне клиентского ПО, так и на сервере БД.

Двухфакторная аутентификация. Для подтверждения права доступа

к защищенной информации производится дополнительная авторизация пользователей, требующая предъявления аппаратного ключа или смарт-карты и ввода пин-кода. Таким образом реализуется композитный метод защиты информации, при котором функция шифрования данных значительно усиливается с помощью двухфакторной аутентификации.

Необратимое удаление данных. Удаление ключей шифрования из системы приводит к необратимой потере зашифрованных данных. Это исключает возможность их дальнейшего восстановления.

Отложенные процедуры зашифрования/расшифрования. Первичное зашифрование таблиц или перешифрование в случае смены ключа шифрования может проводиться без остановки функционирования ИС в целом. Возможно выполнение таких задач по частям, например, во время наименьшей загрузки БД.

Централизованное управление. Выполнение большинства сервисных операций и действий с настройкой системы «Крипто БД» через консоль управления, которая позволяет работать с неограниченным количеством СУБД.

Централизованный мониторинг и аудит. Централизованный сбор информации. Единый центр мониторинга и аудита аккумулирует информа-

цию о различных служебных событиях «Крипто БД» и доступе пользователей к зашифрованным данным.

Разграничение доступа на основе ролевой модели. Реализация гибкой ролевой модели с надежным разделением операций по управлению «Крипто БД», изменяемой в полном соответствии с действующей политикой организации.

Архитектура системы «Крипто БД»

Назначение компонентов

- API «Крипто БД» — ядро «Крипто БД»: осуществляет все криптографические операции, включая шифрование информации, защиту ключей шифрования, безопасную передачу ключей шифрования, обеспечение целостности данных, служебного ПО, служебной информации.
- Репозиторий «Крипто БД» — набор информации о зашифрованных таблицах, ключах шифрования, пользователях, настройках аудита, истории изменения указанной информации.
- Сервис вычисления ключей — служба, предназначенная для безопасной передачи ключей шифрования между клиентом и сервером.
- Консоль администрирования «Крипто БД» — консоль администратора безопасности, позволяющая выполнять следующие операции:

Вопросы экспертам:

Какими методами защиты обеспечивается решение основных задач безопасности в продукте «Крипто БД»?

Сочетание таких мер, как контроль доступа к защищаемой информации, двухфакторная аутентификация и шифрование данных, дает высокую степень защиты ценной информации в СУБД. «Крипто БД» поддерживает ГОСТ 28147–89 и ГОСТ 34.12–2018 (алгоритмы шифрования «Магма», «Кузнечик»), соответствует требованиям к СКЗИ класса КС1, КС2, КС3 и может использоваться для криптозащиты информации в СУБД.

Насколько сильно проседает нагрузка на сервер СУБД при шифровании?

После включения шифрования данных в СУБД нагрузка на вычислительную систему сервера, конечно, возрастает. Вопрос производительности защищенной системы нужно рассматривать в двух аспектах. Производительность регулярных операций добавления, чтения или поиска информации в базе данных «просядет» незначительно. То есть рядовой пользователь ИС, работающий в окнах бизнес-приложений, не сможет определить разницу работы в защищенном и не защищенном режиме.

Производительность так называемых масс-операций, при которых производятся глобальные выборки данных из защищаемых таблиц, будет чувствительнее к изменениям. Как правило, защищенная система потребляет на 25–35% больше вычислительных мощностей СУБД. То есть если условная операция «закрытие операционного дня» в системе раньше совершалась за 60 минут, то после активации средств шифрования такая операция может выполняться 80–90 минут.

Может ли «Крипто БД» использовать альтернативные алгоритмы шифрования? Например, AES-256 и т. п.?

Сертифицированная версия продукта имеет ограничения в использовании альтернативных алгоритмов шифрования,

это связано в первую очередь с высоким уровнем доверия к защитным механизмам, а также с формальной оценкой степени надежности защиты. По желанию заказчика продукт может быть оснащен модулями поддержки альтернативных алгоритмов шифрования. В данном случае нужно иметь в виду, что сертификат соответствия на такую систему распространяться не будет. В нашем арсенале есть кейсы адаптации как к AES-256, так и к другим алгоритмам шифрования, например, по требованиям регуляторов ряда стран СНГ.

Как решается проблема защиты СУБД от администратора?

Здесь все просто. Администратор СУБД обладает максимальными правами доступа к любым данным, однако ролевая модель и принцип разделения полномочий "segregation of duty", реализованный в «Крипто БД», гарантируют отсутствие у администратора СУБД ключа шифрования данных. Защитные механизмы также контролируют целостность своего программного кода и среды выполнения в процессе функционирования СКЗИ. Таким образом, администратор СУБД не сможет нарушить правила доступа к информации, либо его вмешательство приведет к отказу штатной работы СКЗИ.

Как защищены журналы аудита «Крипто БД»?

Вся информация о доступе пользователей и администраторов к защищаемым данным записывается в отдельный журнал аудита, который может быть направлен по сети на выделенный сервер (коллектор данных аудита) и далее использован при расследовании инцидентов ИБ. Дополнительно существуют конфигурации внедрения «Крипто БД», при которых данные аудита записываются и хранятся на том же сервере СУБД в зашифрованном виде. В таком случае, что очевидно, доступ к этой информации может получить только администратор безопасности.

- обеспечение жизненного цикла ключей шифрования;
- шифрование и перешифрование данных в таблицах БД;
- управление пользователями (ключами шифрования пользователей);
- управление аудитом;
- контроль целостности собственного ПО и объектов пользователей;
- контроль ошибочных ситуаций.
- Компонент клиента (клиент «Крипто БД») — интерфейсное ПО для осу-

ществления взаимодействия с СКЗИ для выполнения на сертифицированном СКЗИ криптографических операций.

Выводы

В складывающейся критичной ситуации вынужденного использования платформ СУБД, которые стали крайне опасными, нет ничего удивительного и нового. Стоит признать, что до марта 2022 года многие ИТ-специалисты воспринимали тер-

мин «импортозамещение» как что-то неадекватное и навязанное государством, мешающее бизнесу. Использовать довольно комфортный период в 6–7 лет для поэтапного, управляемого и безболезненного перехода на российские платформы СУБД удалось не многим. Для остальных компаний, попавших в трудное положение, такие продукты, как «Крипто БД», являются «спасительной таблеткой», позволяющей надежно сохранить самое ценное — свою информацию. 🍎