Чикишев Илья Константинович,
Студент, КВВУ

Кубенко Егор Георгиевич,
Кандидат технических наук, КВВУ

МЕТОДИКА СНИЖЕНИЯ РИСКОВ УТЕЧКИ ИНФОРМАЦИИ В ВЕДОМСТВЕННЫХ БАЗАХ ДАННЫХ С ПРИМЕНЕНИЕМ БЛОКЧЕЙН-ТЕХНОЛОГИЙ.

Аннотация. В статье предложен метод повышения защищённости ведомственных баз данных (БД) путём комбинации реляционной СУБД и блокчейна. Реализуется разделение ответственности между хранилищем и контролем целостности. Описаны четырёхуровневая архитектура, хеширование по ГОСТ Р 34.11–2012, управление доступом через смарт-контракты с автоматическим отзывом прав и мониторинг инцидентов.

Ключевые слова: Блокчейн, смарт-контракты, базы данных, утечка информации, целостность данных, управление доступом.

1. Постановка проблемы

Традиционные системы управления базами данных (СУБД), сертифицированные для работы с информацией ограниченного распространения, не обладают встроенными механизмами, гарантирующими неизменяемость журнала аудита и исключающими злоупотребления со стороны администратора БД. Угроза внутреннего нарушителя, обладающего учётной записью с избыточными или забытыми правами, а также возможность скрытого изменения данных без оставления следов остаются критически значимыми для ведомственных информационных систем.

Современное развитие криптографических методов и распределённых реестров позволяет предложить архитектуру, в которой блокчейн выполняет не функцию основного хранилища, а роль контролирующей надстройки.

2. Архитектура методики

Предлагаемая методика базируется на принципе разделения ответственности. СУБД остаётся основным хранилищем информационных объектов, а блокчейн реализует три критических функции:

Регистрация хешей данных – обеспечение неизменяемости и верификации целостности.

Управление доступом через смарт-контракты – автоматизация выдачи и отзыва прав.

Неизменяемый журнал аудита – фиксация всех операций с временной меткой и подписью.

Архитектура включает четыре уровня:

Уровень 1. Клиентские приложения и АРМ (российская ОС семейства Linux, модуль блокчейн-клиента).

Уровень 2. Шлюз безопасности (API Gateway) – проверяет смарт-контракты, сверяет хеши, логирует действия в блокчейн.

Уровень 3. Традиционная СУБД (например, PostgreSQL с доработками или отечественная СУБД «Линтер», таблицы с служебным полем hash_record).

Уровень 4. Блокчейн-сеть (разрешённый блокчейн, ГОСТ Р 34.10–2012, ГОСТ Р 34.11–2012, консенсус PBFT, $N \geq 4$ узлов, объединённых криптошлюзами).

Система противостоит атакам:

- администратора БД – не может подделать хеш без контроля большинства узлов блокчейна;
- внутреннего пользователя – все его действия фиксируются в неизменяемом журнале;
- перехвата трафика – каналы зашифрованы, хеши не раскрывают содержание;
- компрометации отдельного узла блокчейна – консенсус сохраняет целостность.

3. Обеспечение целостности данных

Для хеширования применяется ГОСТ Р 34.11–2012 (Стрибог) с длиной хеша 256 бит. Хеширование выполняется на уровне кортежа (строки) БД, что позволяет детектировать точечные изменения. При добавлении записи клиент формирует каноническое представление полей, вычисляет хеш, а API Gateway регистрирует его в блокчейне транзакцией RegisterHash. При обновлении записи старый хеш сохраняется – формируется цепочка изменений.

При чтении данных шлюз пересчитывает хеш полученных данных и сравнивает его с hash_record в СУБД и с эталонным хешем из блокчейна. Если hash_record_СУБД не совпадает с hash_блокчейн – фиксируется несанкционированная модификация, запись блокируется.

Для повышения производительности на больших объёмах применяется дерево Меркла на уровне пакета: корень дерева регистрируется в блокчейне одной транзакцией, что позволяет верифицировать отдельные записи без загрузки всех хешей.

4. Управление доступом на основе смарт-контрактов

Предлагается переход от статических моделей (мандатный, дискреционный) к динамической модели временного делегирования. Смарт-контракт доступа содержит: субъект, объект, тип разрешения (read, write), период действия (valid_from, valid_until), опциональные условия, подпись лица, предоставившего доступ, и флаг отзыва.

Алгоритм доступа включает три последовательные проверки:

Мандатные правила (уровень доступа субъекта к объекту).

Наличие активного смарт-контракта.

Дополнительные условия (IP-адрес, время суток).

Доступ разрешается только при выполнении всех трёх условий. По истечении valid_until контракт автоматически аннулируется. Досрочный отзыв производится транзакцией RevokeAccess. Подмена субъекта исключена за счёт использования уникальных криптографических идентификаторов, выпускаемых Удостоверяющим центром.

5. Мониторинг и реагирование на инциденты

Каждое действие через API Gateway фиксируется в блокчейне транзакцией AuditLog (поля: user_id, action, object_id, timestamp, request_hash, result_status, signature). Неизменяемость блокчейна обеспечивает неопровержимость доказательств при служебном расследовании.

На основе журнала строится профиль нормального поведения: количество операций чтения в минуту, типичные таблицы, временные паттерны. Аномалии выявляются по правилам:

- чтение нехарактерно большого объёма данных (например, > 10 000 записей за 10 минут для рядового пользователя);
- доступ к таблицам вне профиля;
- попытка модификации после истечения смарт-контракта;
- несоответствие хешей.

При обнаружении аномалии система может:

- отозвать смарт-контракты нарушителя (RevokeAccess);
- поместить объект в карантин (QuarantineObject);

- принудительно завершить сессии (ForceLogout);
- сформировать сообщение в ведомственную систему учёта инцидентов и занести его хеш в блокчейн.

Приводится сценарий автоматической блокировки внутреннего нарушителя при попытке массового копирования данных за 15 минут до истечения легального доступа.

6. Отказоустойчивость и синхронизация

Шлюзы безопасности развёртываются в активно-активном кластере с единым кэшем смарт-контрактов, обновляемым через подписку на события блокчейна. При потере связи с большинством узлов блокчейна шлюз переходит в ограниченный режим (чтение разрешено, изменение запрещено, верификация приостановлена). При восстановлении связи накопленные подписанные логи отправляются в блокчейн.

Для ограничения роста блокчейна предлагается архивация блоков старше 1 года на автономные носители с сохранением только хеш-корня (checkpointing) и конфигурация с небольшим размером блока (10 МБ).

Заключение

Предложенная методика позволяет существенно снизить риски утечки и несанкционированной модификации информации в ведомственных базах данных за счёт:

- разделения ответственности между СУБД и блокчейном;
- обязательной регистрации хешей всех записей по ГОСТ Р 34.11–2012;
- временных смарт-контрактов доступа, исключающих «забытые права»;
- неизменяемого и неопровержимого аудита всех действий;
- автоматизированного реагирования на аномалии поведения.

Архитектура может внедряться поэтапно как «надстройка» над существующей инфраструктурой и не требует полной замены сертифицированного ПО. В условиях защищённой ведомственной сети с выделенными каналами и использованием отечественных криптоалгоритмов предложенное решение обеспечивает уровень защиты, недостижимый при классическом администрировании БД.

Список литературы:

1. ГОСТ Р 34.10–2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
2. ГОСТ Р 34.11–2012. Информационная технология. Криптографическая защита информации. Функция хеширования.
3. Castro M., Liskov B. Practical Byzantine Fault Tolerance // OSDI. – 1999.
4. Андреев А.В., Петров С.В. Применение распределённых реестров в системах обработки данных ограниченного доступа // Информационные технологии в защищённых системах. – 2025. – № 3. – С. 42-51.