Защита СУБД и данных

ТОП-10 методов обеспечения защиты СУБД от Беляева Дмитрия

17 июня 2025 | Radisson Blu Belorusskaya, Москва | 11:30 — 15:00

BELYAEV

Директор по КБ: Беляев Дмитрий Александрович

Обо мне

- Более 10 лет в ИБ
- Имею более 140 сертификатов/ дипломов и благодарностей по тематике ИБ
- В прошлом руководил пятью стартапами (в т.ч и по ИБ) и командой из более 100 человек
- Имею 3 образования (ИБ, юриспруденция, безопасная разработка)
- Победитель в рейтинге ТОП-100 Лидеров ИТ (GlobalCIO)
- Член клуба 4CIO;
- Член клуба GlobaCIO;
- Основатель клуба TCCR.
- Имею за плечами более 80 выступлений на публику суммарной численностью >5000 человек (TADVISER, ТБ Форум, Территория Безопасности, CISO Форум, CNews, ITsec, Security Summit, Код ИБ, ТБ, SmartGoPro и т.д)
- Амбассадор платформы «Цифровой прорыв» в 2021-2022

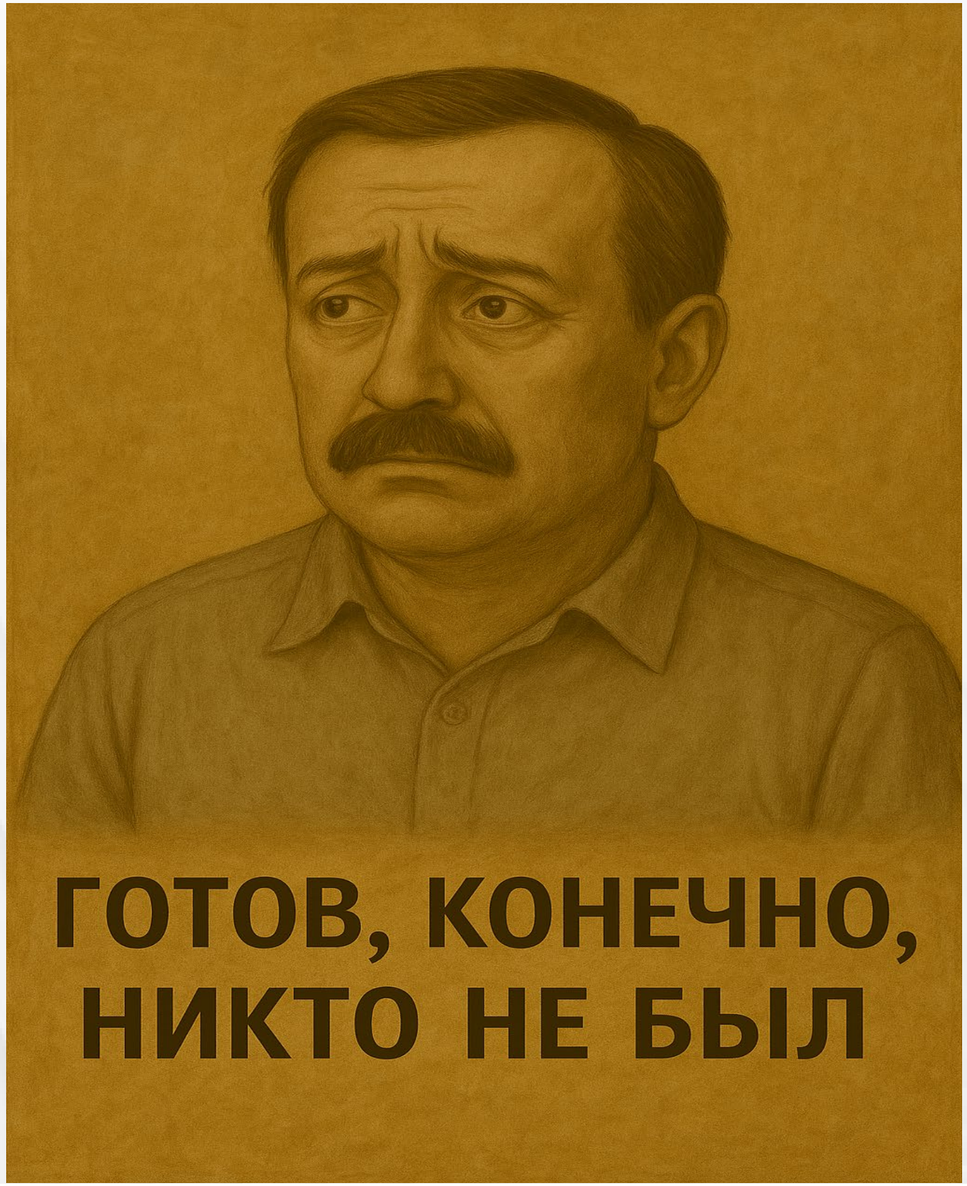
Дмитрий Александрович Беляев

Директор по Кибербезопасности (CISO)

Средняя стоимость утечки персональных данных (ПДн) в 2024–2025 годах ~11,5 млн рублей за один инцидент.

Максимальный ущерб >41 млн рублей, а в отдельных случаях достигать 140 млн рублей для среднего и крупного бизнеса

А ГОТОВ ЛИ БИЗНЕС К ЭТИМ ИЗМЕНЕНИЯМ?

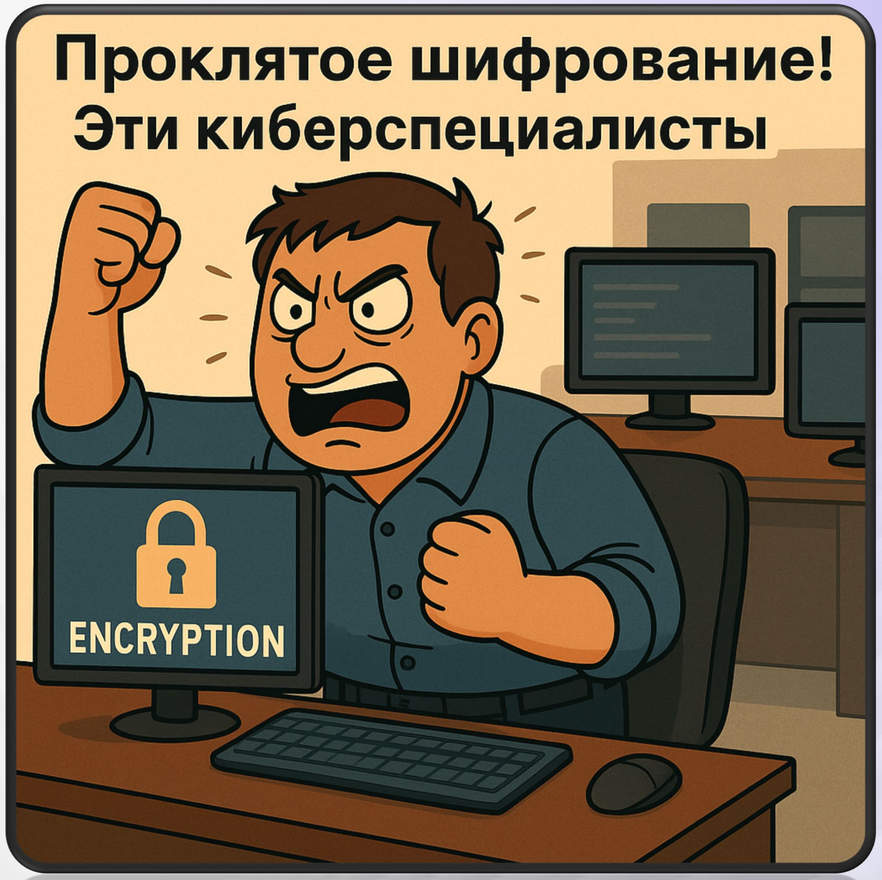

ГОТОВ, КОНЕЧНО,
НИКТО НЕ БЫЛ

Метод №1: Многофакторная аутентификация и управление доступом (IAM)

- Обязательность MFA для административных аккаунтов
- Role-Based Access Control (RBAC) + Attribute-Based Access Control (ABAC)
- Just-in-Time доступ для снижения постоянных привилегий
- Регулярный аудит и ротация привилегий
- Статистика: 70% снижение риска несанкционированного доступа

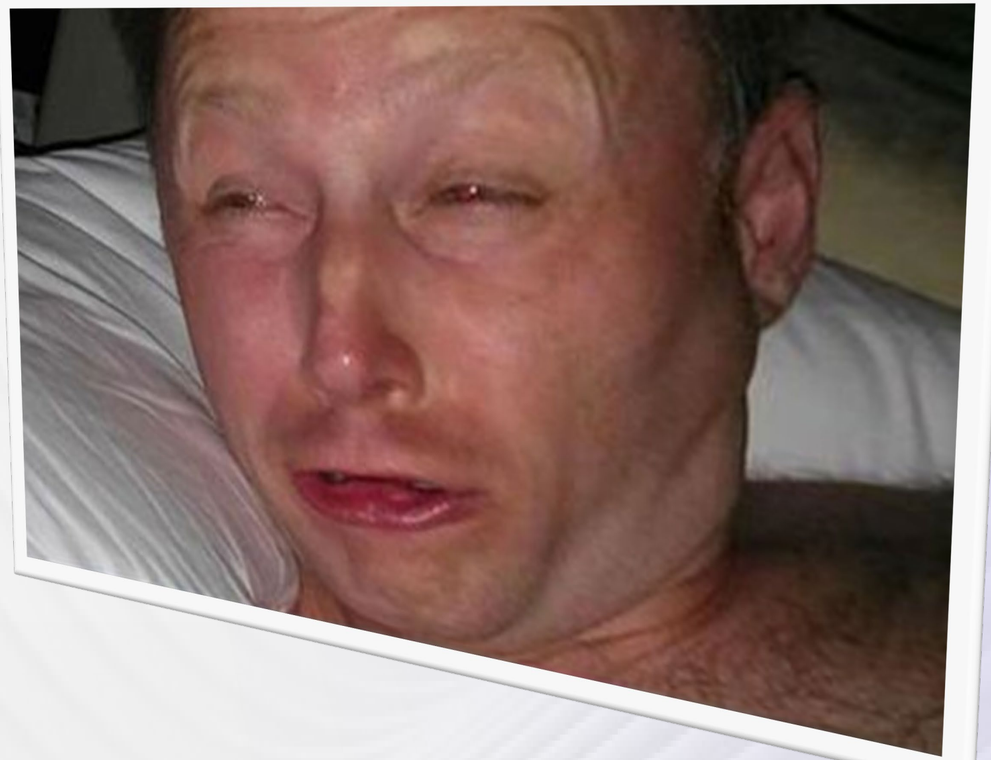
Метод №2: Многоуровневое шифрование данных

- Transparent Data Encryption (TDE) для защиты на уровне файлов
- Always Encrypted для защиты конфиденциальных колонок
- Шифрование данных в покое, движении и использовании
- Централизованное управление ключами с HSM



Метод №3: Database Activity Monitoring (DAM)

- Мониторинг в реальном времени без влияния на производительность
- Поведенческая аналитика для обнаружения аномалий
- Интеграция с SIEM-системами
- Автоматическое блокирование подозрительных запросов
- Статистика: 90% ускорение реагирования на угрозы



Метод №4: Архитектура Zero Trust для СУБД

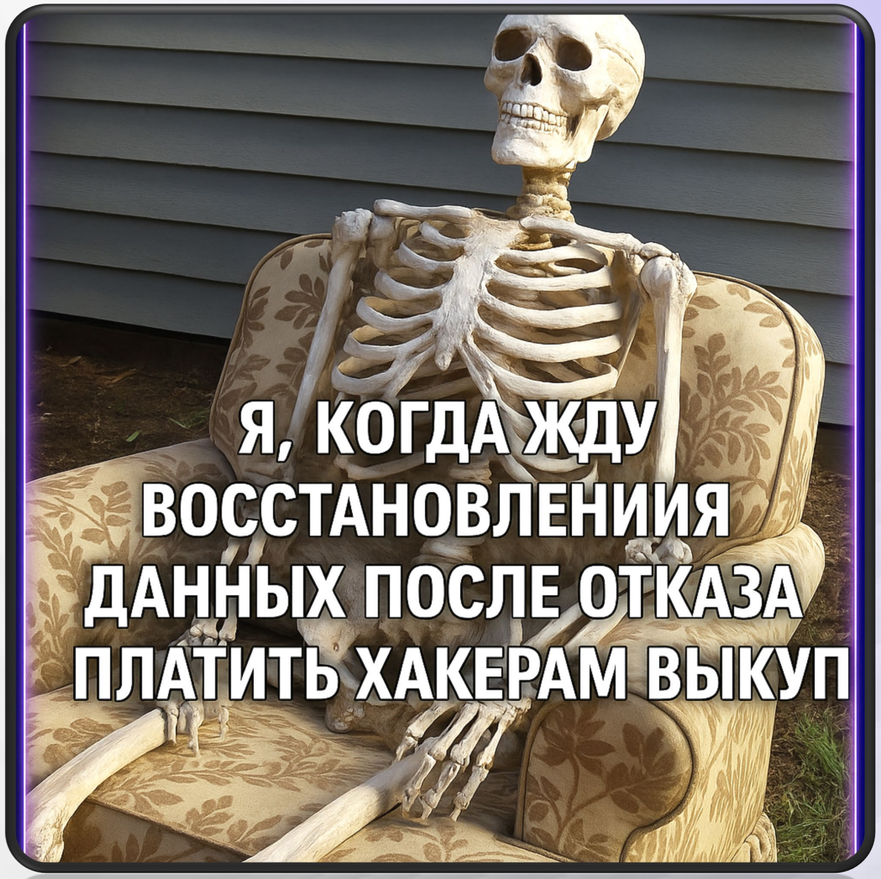
- Принцип "никому не доверяй, всегда проверяй"
- Непрерывная верификация пользователей и устройств
- Микросегментация базы данных
- Контекстная аутентификация
- Статистика: 60% снижение инсайдерских угроз

Метод №5: Проактивное управление уязвимостями

- Автоматизированное сканирование и оценка рисков
- Приоритизация патчей на основе CVSS
- Тестирование в изолированной среде
- Непрерывный мониторинг новых CVE

Метод №6: Защищенное резервное копирование

- Принцип 3-2-1: 3 копии, 2 носителя, 1 offsite
- Шифрование всех бэкапов
- Изоляция резервных копий от основной сети
- Регулярное тестирование процедур восстановления
- Статистика: 100% восстановление данных при атаках ransomware

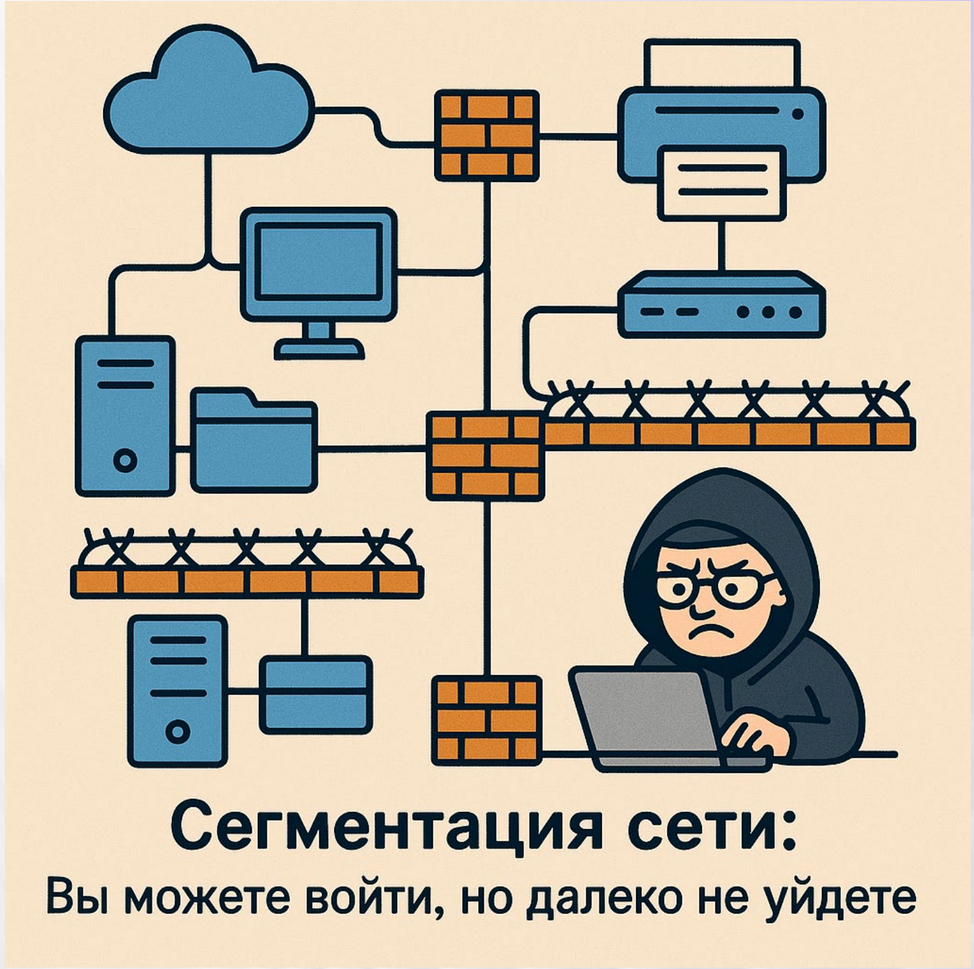


Метод №7: Сегментация сети и микросегментация

- Мониторинг в реальном времени без влияния на производительность
- Поведенческая аналитика для обнаружения аномалий
- Интеграция с SIEM-системами
- Автоматическое блокирование подозрительных запросов
- Статистика: 90% ускорение реагирования на угрозы

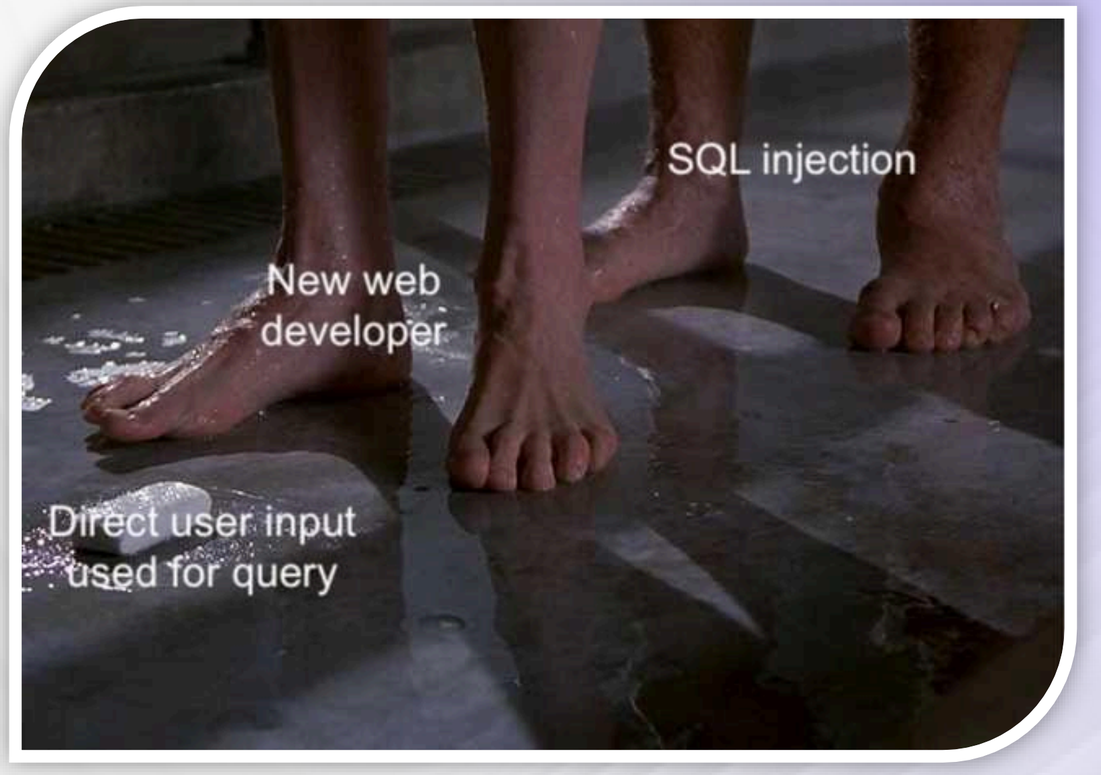
Метод №7: Сегментация сети и микросегментация

- Изоляция критически важных баз данных
- Файрволы между сегментами с строгими правилами
- Secure VPN для удаленного доступа
- Контроль и фильтрация межсегментного трафика
- Статистика: 80% ограничение латерального движения атакующих



Метод №8: Комплексная защита от инъекций

- Использование параметризованных запросов
- Web Application Firewall (WAF) с правилами для СУБД
- Строгая валидация и санитизация входных данных
- Белые списки разрешенных SQL-команд
- Статистика: 95% блокировка попыток SQL-инъекций



Метод №9: Непрерывный аудит и соответствие требованиям

- Комплексное журналирование всех операций
- Соответствие 152-ФЗ, отраслевым стандартам
- Автоматизированные отчеты для регуляторов
- Централизованная система аудита
- Статистика: 100% готовность к регуляторным проверкам

Метод №10: ИИ и машинное обучение в защите

- Поведенческая аналитика на основе ML
- Предиктивная защита от неизвестных угроз
- Автоматическая классификация и маскирование данных
- Адаптивная аутентификация на основе контекста
- Статистика: 85% точность обнаружения аномальной активности

Рекомендуемое распределение бюджета на защиту СУБД

А что на счет ROI?

Успешные внедрения:

- Банковский сектор: 35% снижение попыток несанкционированного доступа после внедрения AES-256
- FinTech компания: 65% снижение попыток взлома после комплексного внедрения
- Google Cloud SQL: автоматическое внедрение множественных методов защиты

Экономическая эффективность:

- ROI 3:1 — каждый вложенный рубль экономит 3 рубля
- Окупаемость инвестиций: 3.33 года
- Избежание штрафов Роскомнадзора до 18 млн рублей

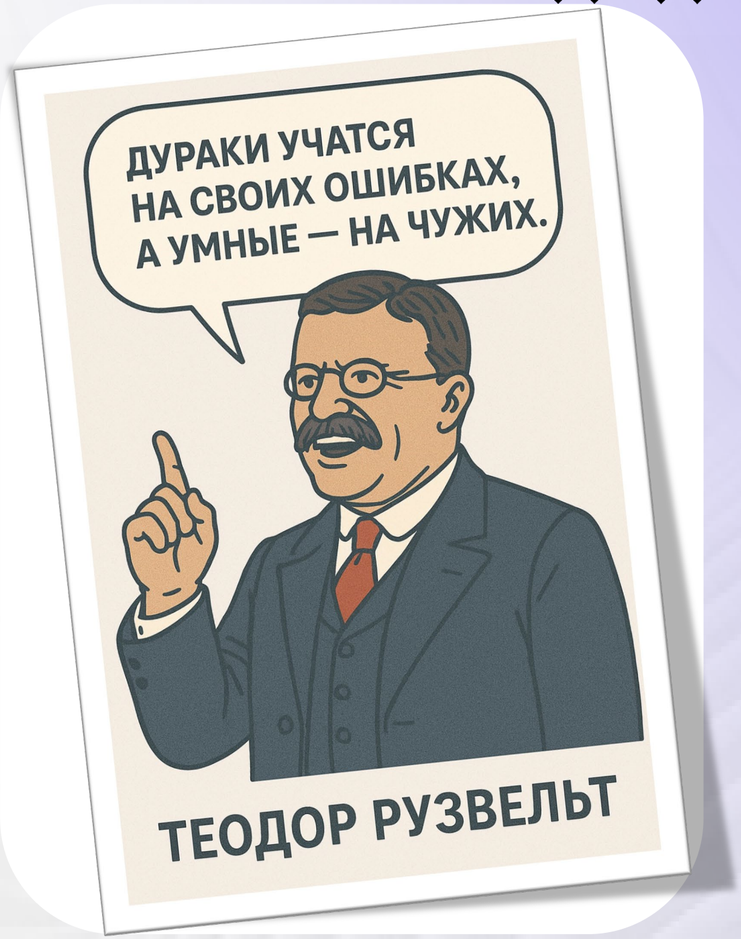
Заключение и Q&A

Ключевые выводы:

- Комплексный подход — единственный эффективный путь
- Автоматизация — ключ к масштабируемой защите
- Непрерывное обучение и адаптация к новым угрозам
- Инвестиции в защиту окупаются предотвращенными потерями

«Дураки учатся на своих ошибках, а умные — на чужих»

Теодор Рузвельт



Чек-лист проверки безопасности СУБД

Контакты

Беляев Дмитрий Александрович

Телефон: **8-905-486-49-11**

E-mail: da.belyaev@mail.ru

Сайт: https://belyaev.expert/

Канал: https://t.me/belyaevsec

↗ Канал «**BELYAEV_SECURITY**»: Твой проводник в мир защищенной информации (новости, статьи, экспертиза, юмор)

Отсканируй

Вступи