

Актуальные вопросы защиты СУБД ИСПДн с внешними пользователями

КОНСТАНТИН САМАТОВ

Члена Правления

Ассоциации руководителей служб информационной
безопасности

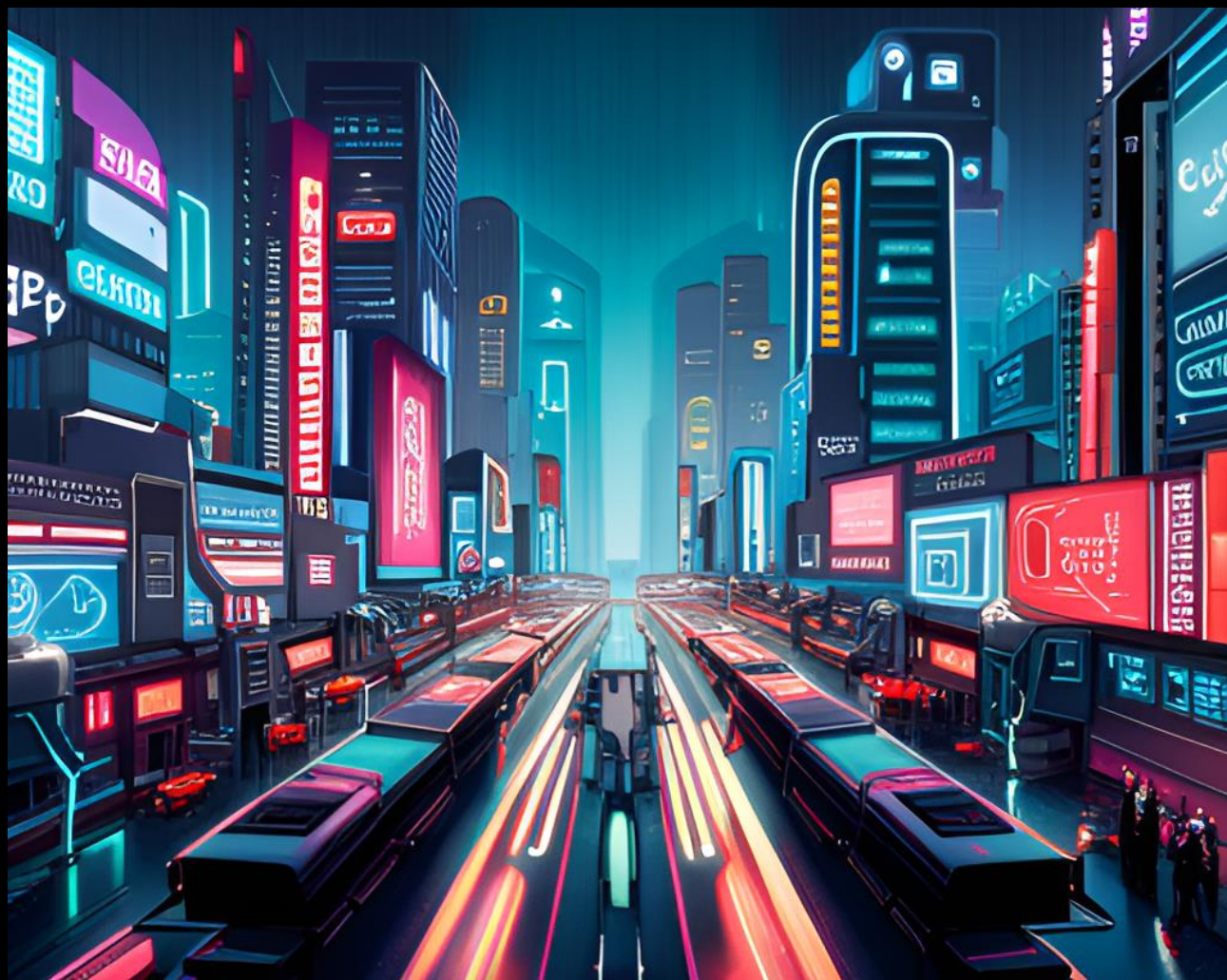


Основные термины

База данных (БД) - совокупность взаимосвязанных данных, организованных таким образом, чтобы с ними мог работать пользователь при помощи ЭВМ.

Система управления базой данных (СУБД) – система, позволяющая при помощи определенного вида запросов, управлять базами данных (работать с содержащейся в них информацией)

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных (БД) персональных данных и обеспечивающих их обработку информационных технологий (в т.ч. СУБД) и технических средств.



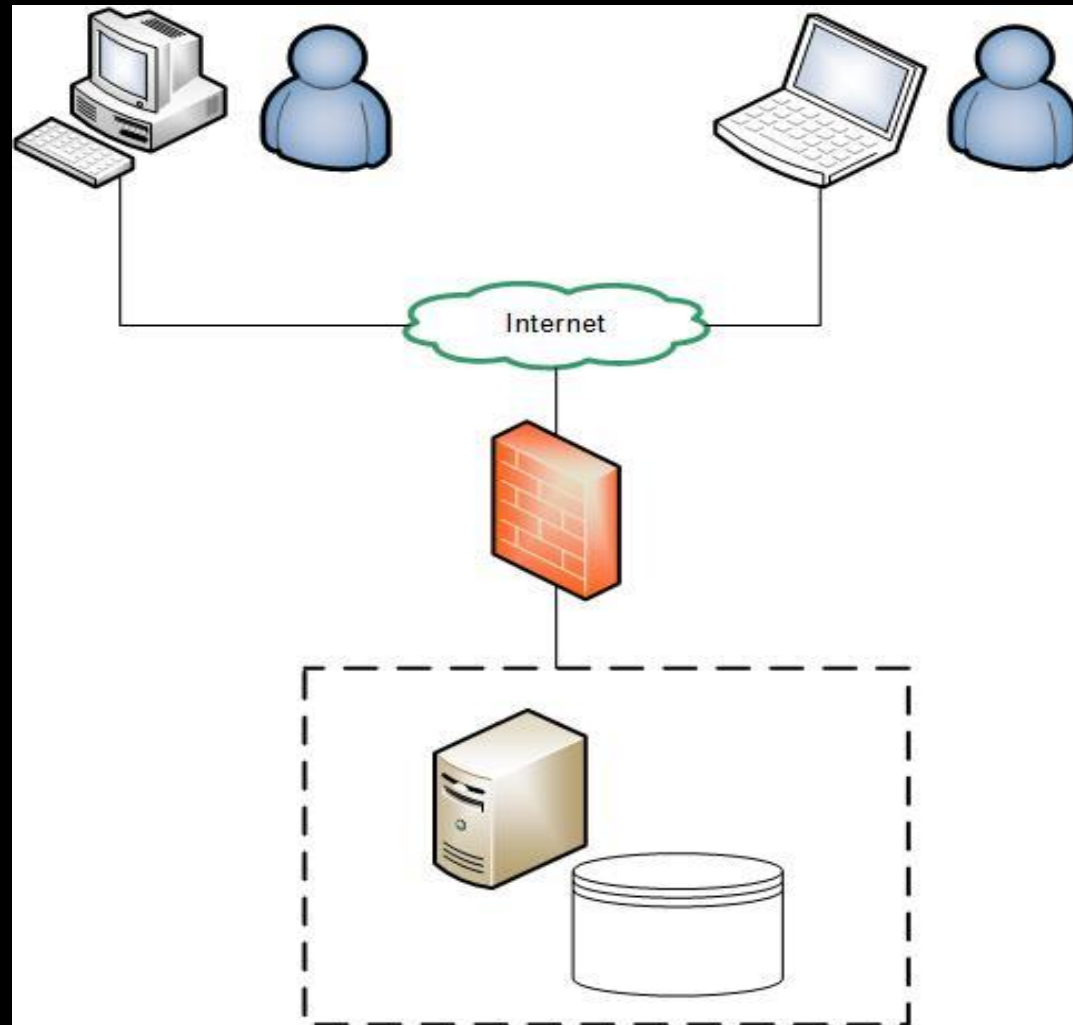
Основные уязвимости (связанные с БД и СУБД)

- Одним из главных слабых мест в системах защиты баз данных являются **слабые пароли**. Часто пользователи используют простые комбинации, которые легко поддаются взлому. Например, пароль 123456 или qwerty не требуют особого усилия для взлома.
- Еще одной уязвимостью в системах защиты баз данных являются **ошибки в коде программного обеспечения СУБД**. Злоумышленники могут использовать эти уязвимости для получения доступа к базе данных или для изменения ее содержимого.



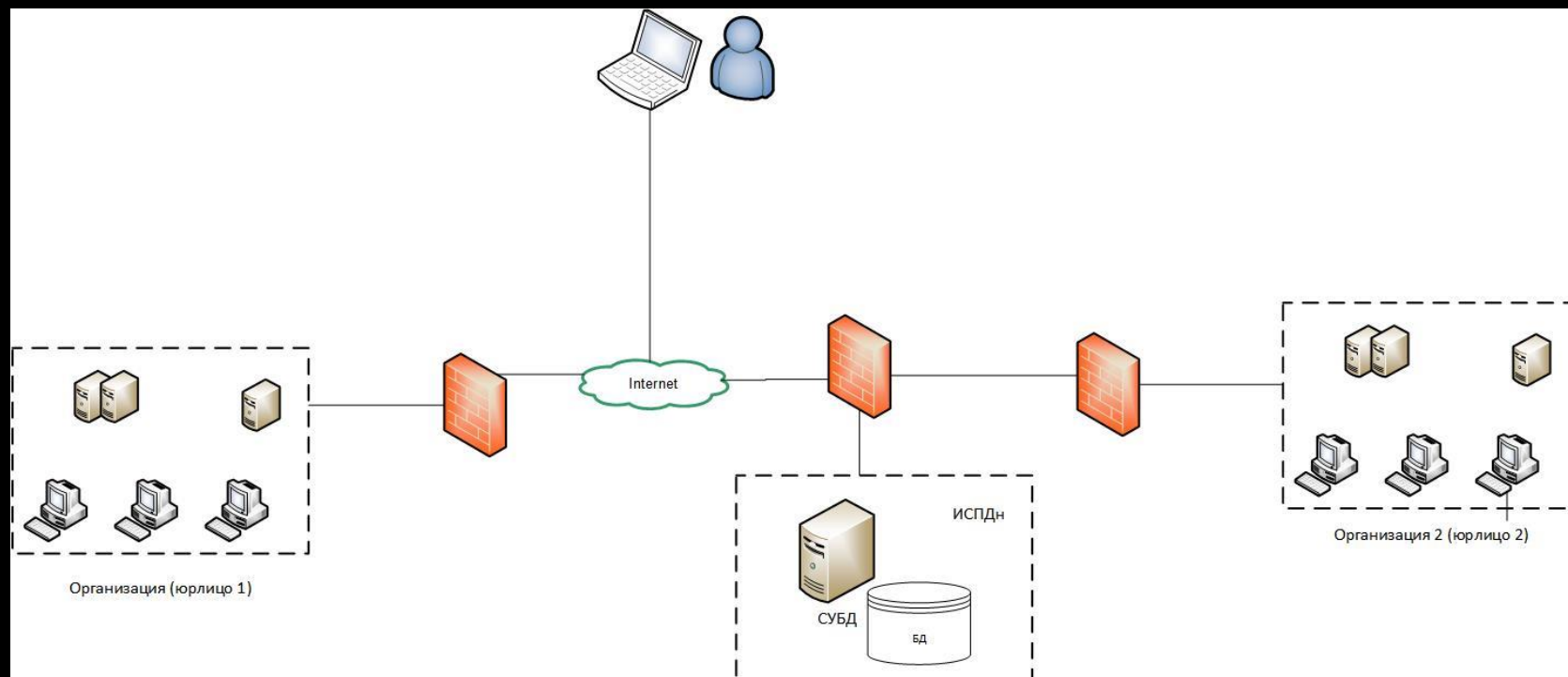
Кейс 1: Слабые пароли

- Подбор/перебор пароля
- Хищение (персональных) данных
- Нарушение работоспособности (в т.ч. ГИС или КИИ)
- Использование инфраструктуры для атаки на другую информационную инфраструктуру



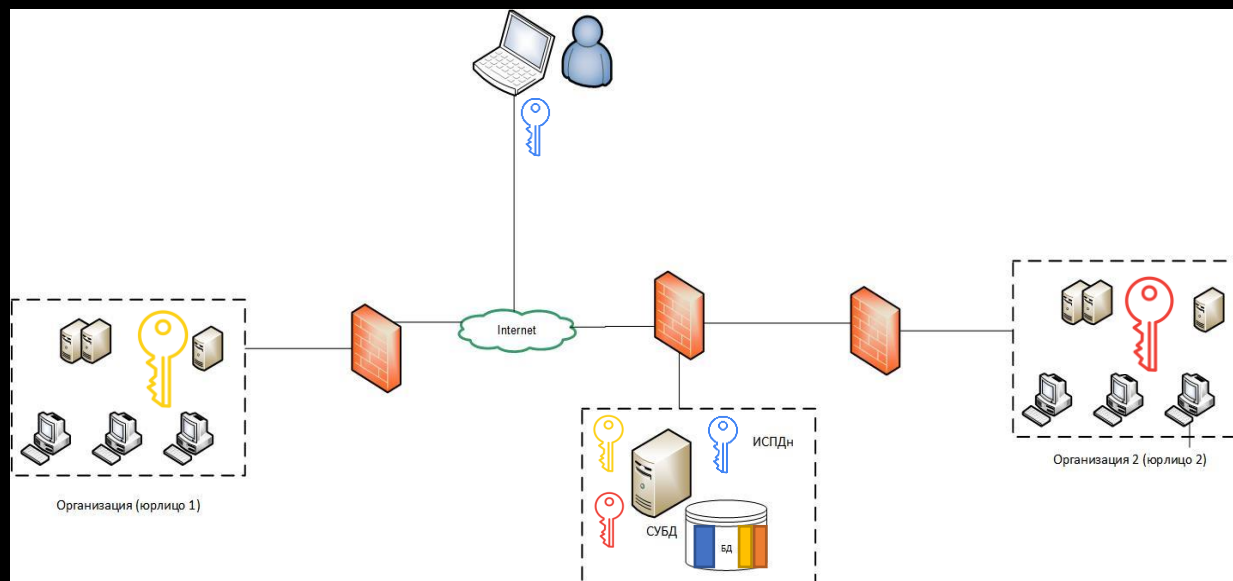
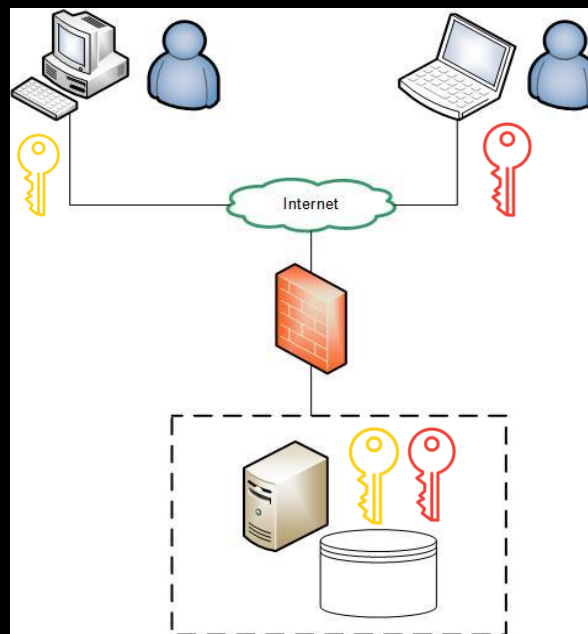
Кейс 2. Уязвимости в коде

- Уязвимый код позволяющий внешнему пользователю (**внутреннему нарушителю**) получить большие привилегии, чем заданные администратором или выполнять вредоносные команды в базу данных
- Хищение базы ПДн
- Нарушение работы системы
- Уничтожение данных



Пути решения

- Настроенная парольная политика
- Мониторинг
- БРПО
- Сертификация
- Использование средств криптографической защиты информации, осуществляющих шифрование таблиц баз данных и двухфакторную аутентификацию пользователей посредством применения криптографических ключей



Спасибо за внимание!

КОНСТАНТИН САМАТОВ

Члена Правления

Ассоциации руководителей служб информационной
безопасности

