PLATFORM V

SBER

Владимир Комаров

Безопасность БАЗ ДАННЫХ

Важна ли безопасность?

+17%

к эффективности

Иванов И. М.	127500
Кузнецов П. Г	231670
Орлов О. Е.	188100
Соколов С. А.	220300
Воробьёв А. Ю.	311007
Синицын С. К.	95608
Петухов А. В.	191800

+3%

к безопасности

Platform V Pangolin – ключевой компонент Platform V

Реляционная СУБД на основе

PostgreSQL

с повышенными требованиями
к безопасности, отказоустойчивости
и удобству обслуживания

Ролевая модель

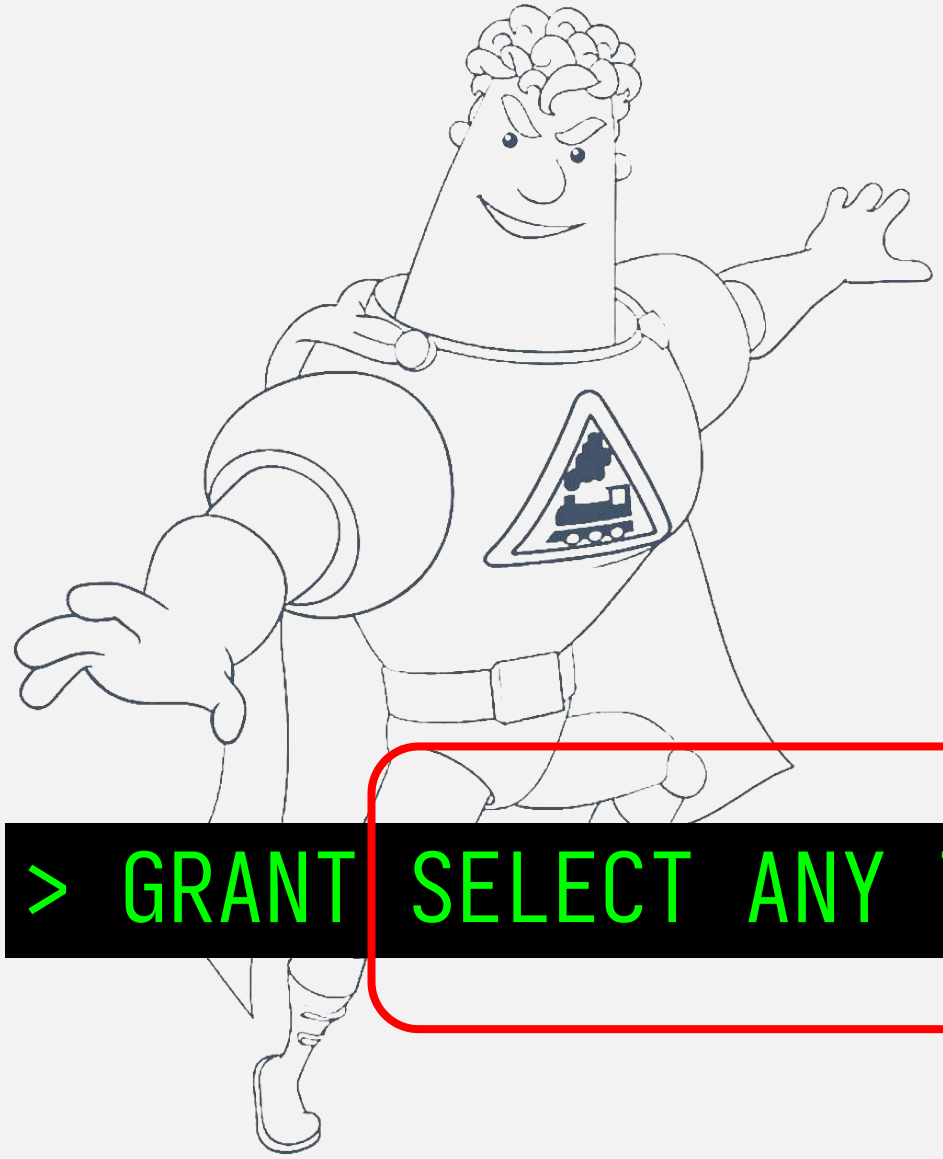
Атрибуты

```
> CREATE USER SCOTT LOGIN
```

Привилегии

```
> GRANT SELECT ON PUBLIC.ACCOUNT TO SCOTT
```

Суперсилы!



```
> GRANT SELECT ANY TABLE TO SCOTT
```

Русско-английский словарь

	Действия над системой	Действия над классом объектов (суперсилы)	Действия над объектом
Oracle	Системные привилегии (system privileges)		Объектные привилегии (object privileges)
PostgreSQL	Атрибуты (attributes)	Предопределённые роли (predefined roles)	Права (privileges)
Microsoft SQL Server	Разрешения уровня сервера (server level permissions)	Разрешения уровня БД (database level permissions)	Разрешения на объект (object permissions)
Db2	Полномочия (administrative authority) уровня системы, БД, схемы (system-level, database-level, schema-level)		Привилегии (privileges)
MySQL	Административные привилегии (administrative privileges)	Привилегии работы с БД (database privileges)	Объектные привилегии (privileges for database objects)
MongoDB	Привилегии над кластером или БД (cluser privileges, database privileges)	Привилегии над базой данных (database privileges)	Привилегии над коллекцией (collection privileges)
Cassandra			Разрешения (permissions)

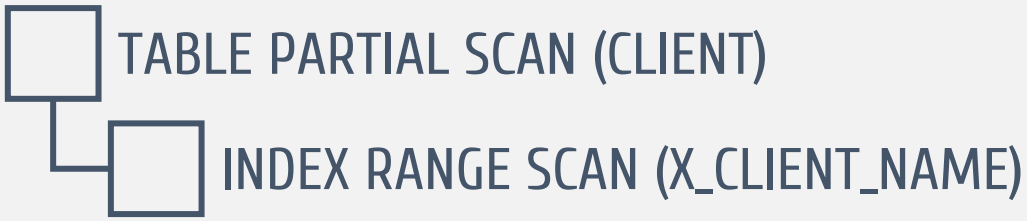
Безопасность на уровне строк

RLS — Row-level security
VPD — Virtual private database
FGAC — Fine-grained access control

RCAC — Row and Column Access Control
RSP — Row Security Policy

```
> CREATE OR REPLACE FUNCTION MYRLS (P_SCH VARCHAR2, P_OBJ VARCHAR2)
RETURN VARCHAR2 IS
BEGIN
   IF (USER = 'K_PETROV') THEN RETURN 'OFFICE IN (10, 20, 30)';
   ELSE
      RETURN 'OFFICE = (SELECT OFFICE FROM USERS WHERE NAME=USER)';
   END IF;
END;
/
> EXEC DBMS_RLS.ADD_POLICY (...)
```

Раз-два... и в продакшен!




```
> SELECT * FROM CLIENT
WHERE NAME LIKE 'ЗАГОРУЙКО%'
AND OFFICE = (
  SELECT OFFICE FROM USERS WHERE NAME=USER
)';
```

Метки безопасности

Label security — Oracle;
Label-based access control (LBAC)

Row Level Access Control (RLAC)
Mandatory Access Control (MAC)

ID	NAME	INS_ID	
1	Мартышка	41	20 : Ударные, Смычковые : FR
2	Осёл	43	40 : Щипковые : DE
3	Козёл	41	30 : Ударные, Щипковые : ES
4	Медведь	54	10 : Ударные, Деревянные : CN

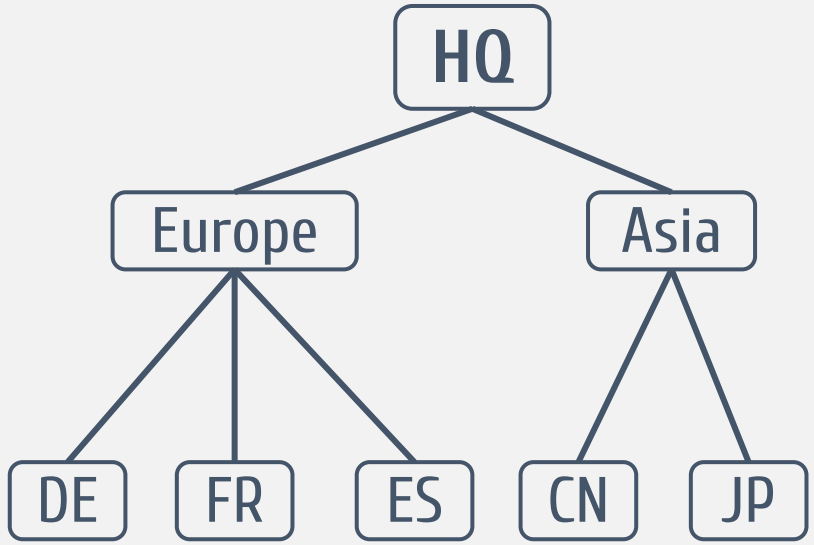
30 : Ударные, Щипковые, Смычковые : Europe

Как сравнивать метки безопасности?

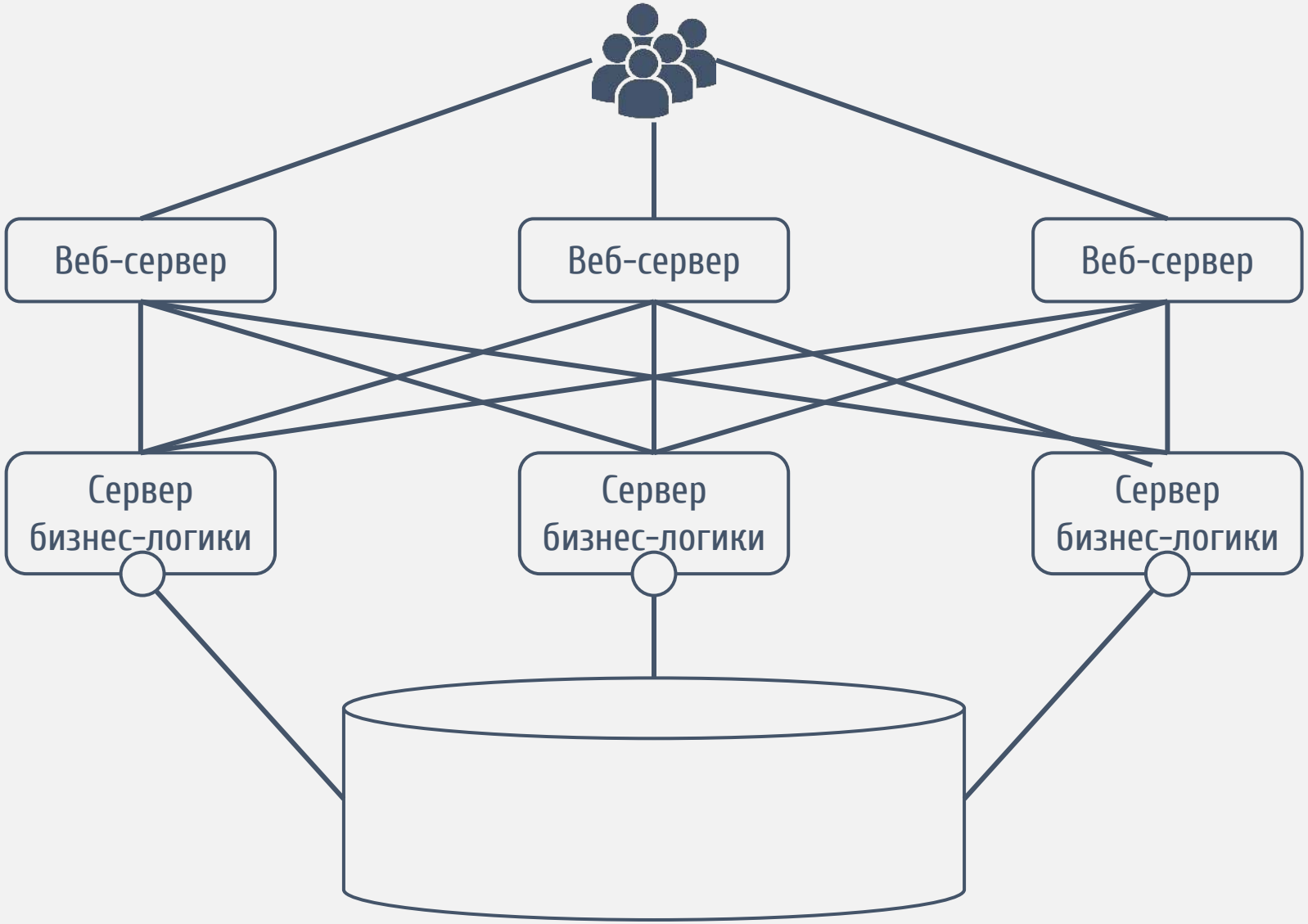
Ранг

Набор

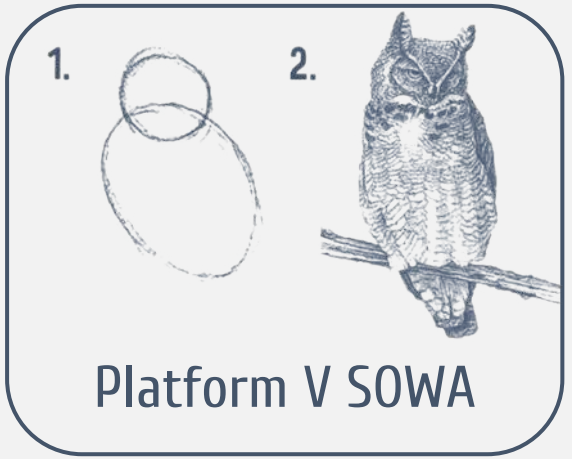
Иерархия



Почему всё бесполезно?



Web Application Firewall



А надо ли защищать данные?

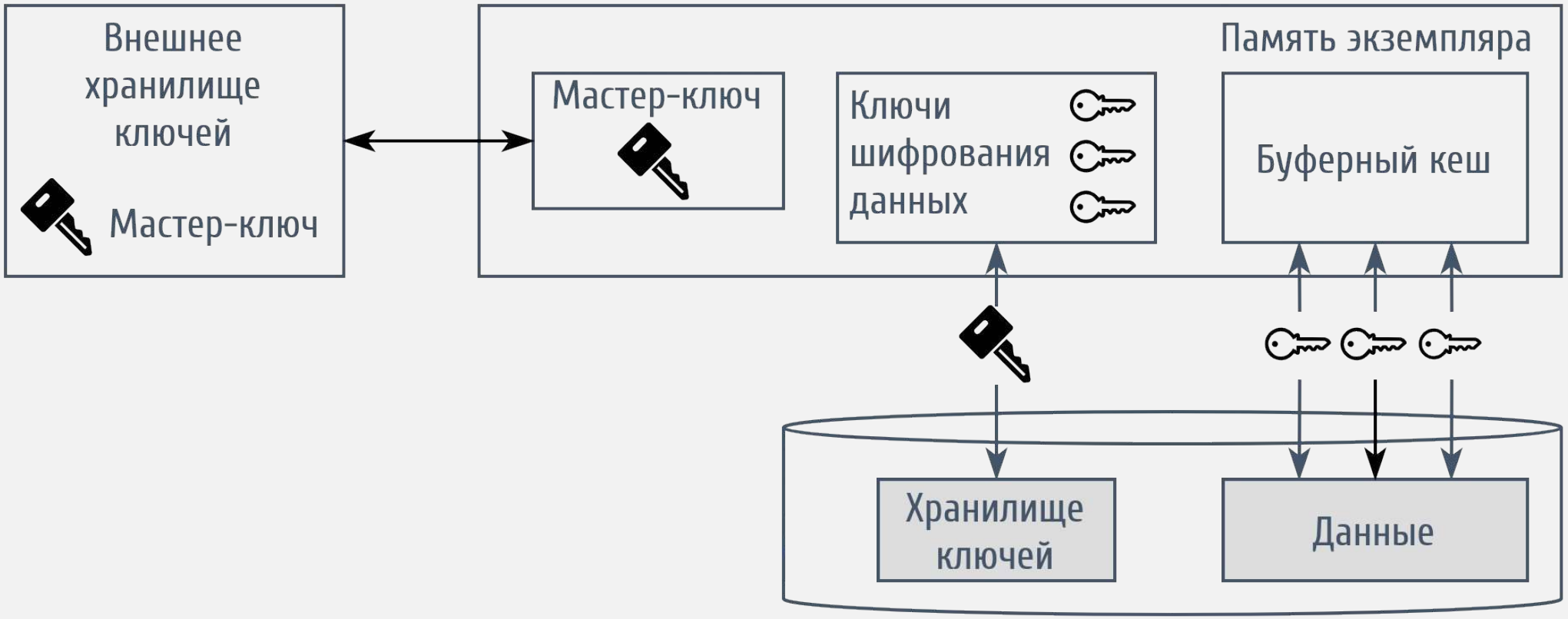
Категория	Описание	Примеры
Public Domain	Данные из открытых источников Данные для распространения	ФИАС, ОКВЭД Формы 101, 102
Internal Use	Данные, не предназначенные для открытой публикации	Структура внутренней сети
Confidential	Коммерческая тайна	Остатки по счетам, персональные данные клиентов
Top Secret	Государственная тайна	[удалено в соответствии с 432-ФЗ]

Модель угроз

Роль	Права доступа
Администратор базы данных	Выполнение над системой управляющих действий, включая изменение параметров экземпляра БД, управление учётными записями пользователей, управление ролями
Администратор ОС	Полный доступ к файлам и процессам со стороны ОС
Администратор РК	Доступ на чтение к файлам БД и полный доступ к файлам резервных копий
Администратор безопасности	Управление параметрами системы, относящимися к безопасности, включая настройки аудита, парольные политики, параметры шифрования, полномочия на доступ к данным
Администратор приложения	Доступ на чтение и запись к данным приложения
Учётная запись мониторинга	Доступ к метрикам мониторинга экземпляра БД и ОС
Учётная запись владельца данных	Полный доступ к данным приложения
Учётная запись для работы приложения	Доступ на чтение и запись к данным приложения

Шифрование данных

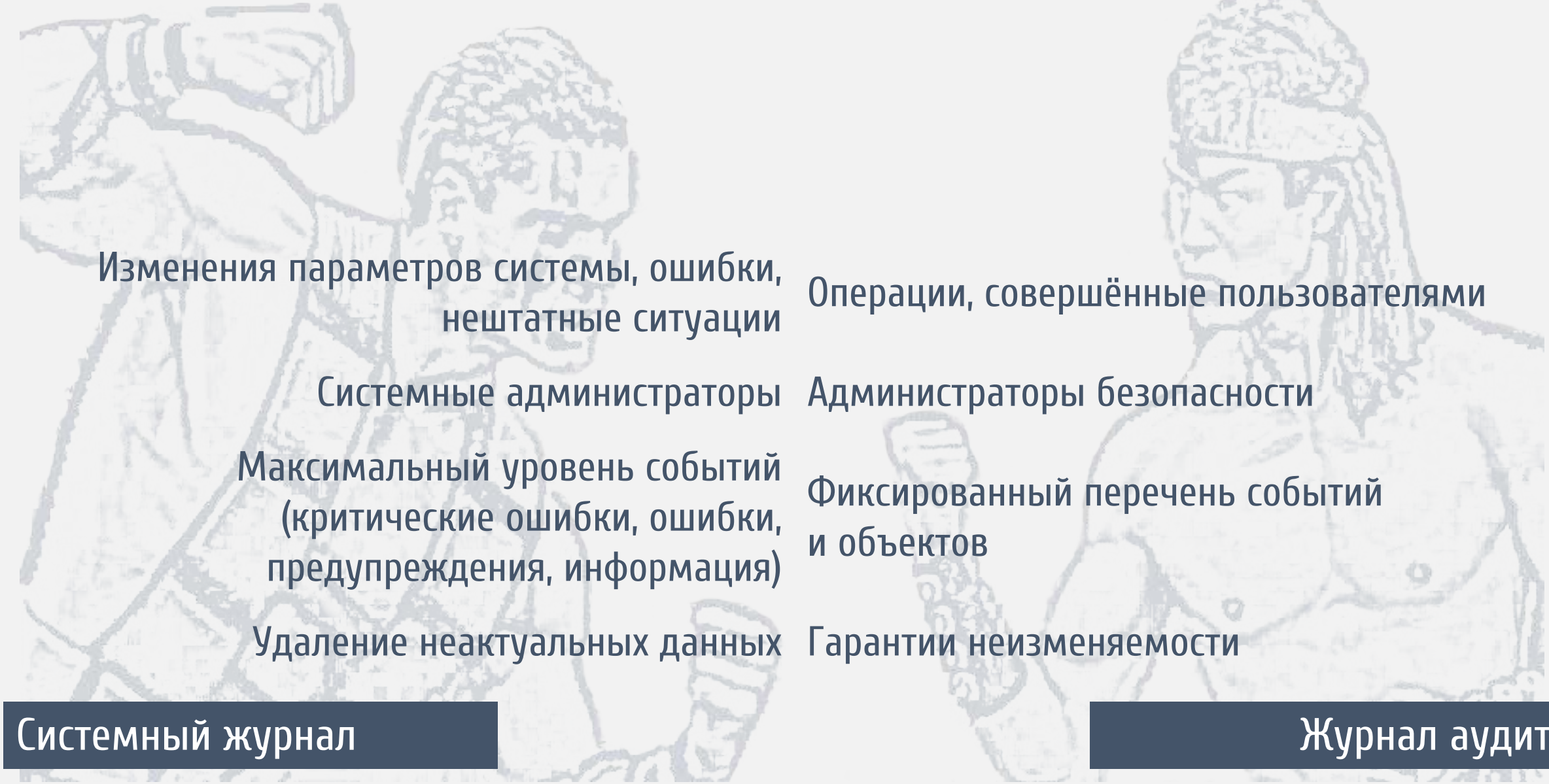
Transparent Database Encryption (TDE)
Encryption at rest



Матрица ролей

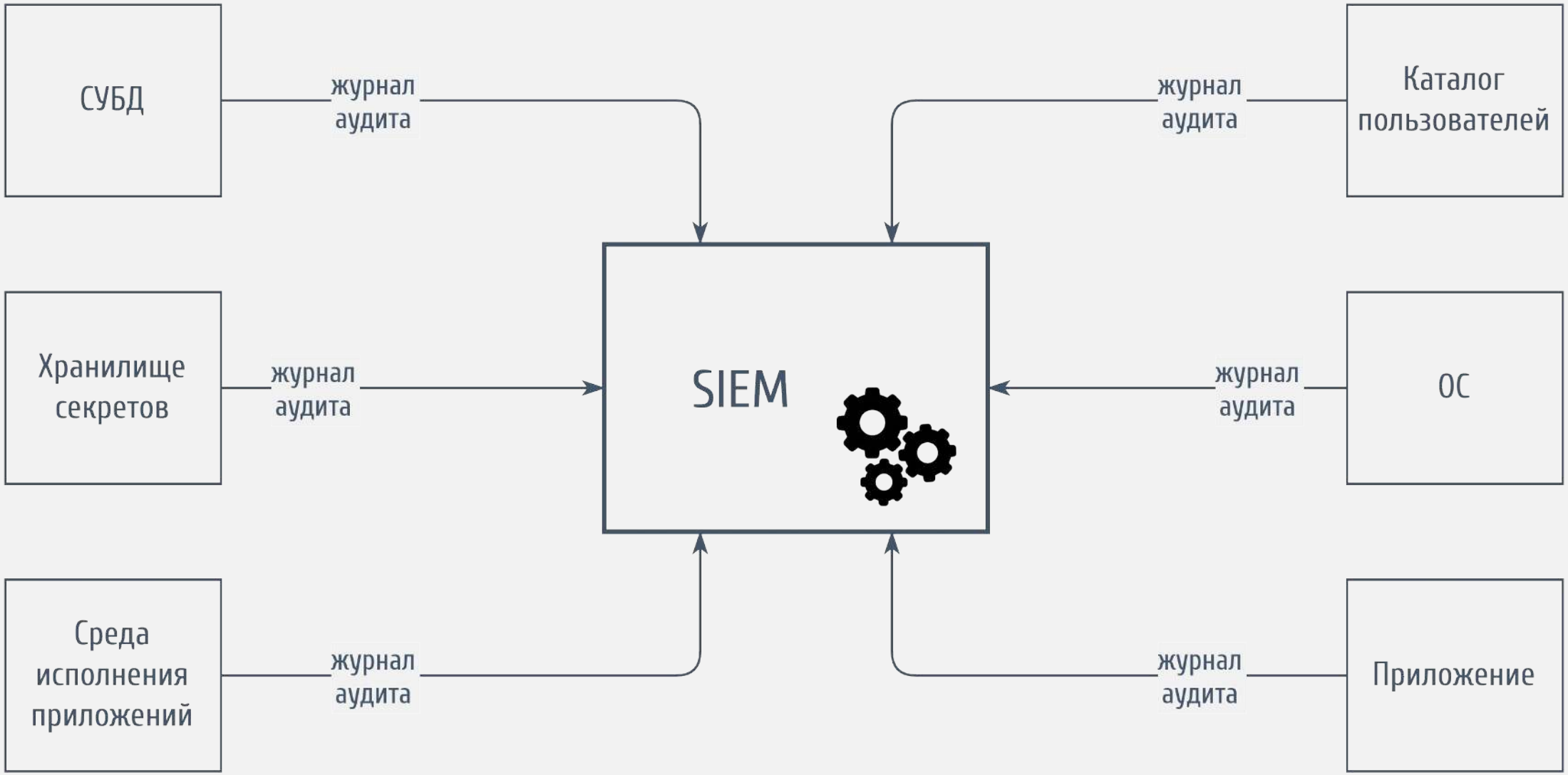
	Администратор БД	Администратор ОС	Администратор РК	Администратор ИБ	Администратор приложения	Технологическая УЗ	Владелец данных	УЗ приложения
Администратор БД	+							
Администратор ОС		+						
Администратор РК			+					
Администратор ИБ				+				
Администратор приложения					+			
Технологическая УЗ						+		
Владелец данных							+	
УЗ приложения								+

Аудит vs. системный журнал



Системный журнал	Журнал аудита
Изменения параметров системы, ошибки, нештатные ситуации	Операции, совершённые пользователями
Системные администраторы	Администраторы безопасности
Максимальный уровень событий (критические ошибки, ошибки, предупреждения, информация)	Фиксированный перечень событий и объектов
Удаление неактуальных данных	Гарантии неизменяемости

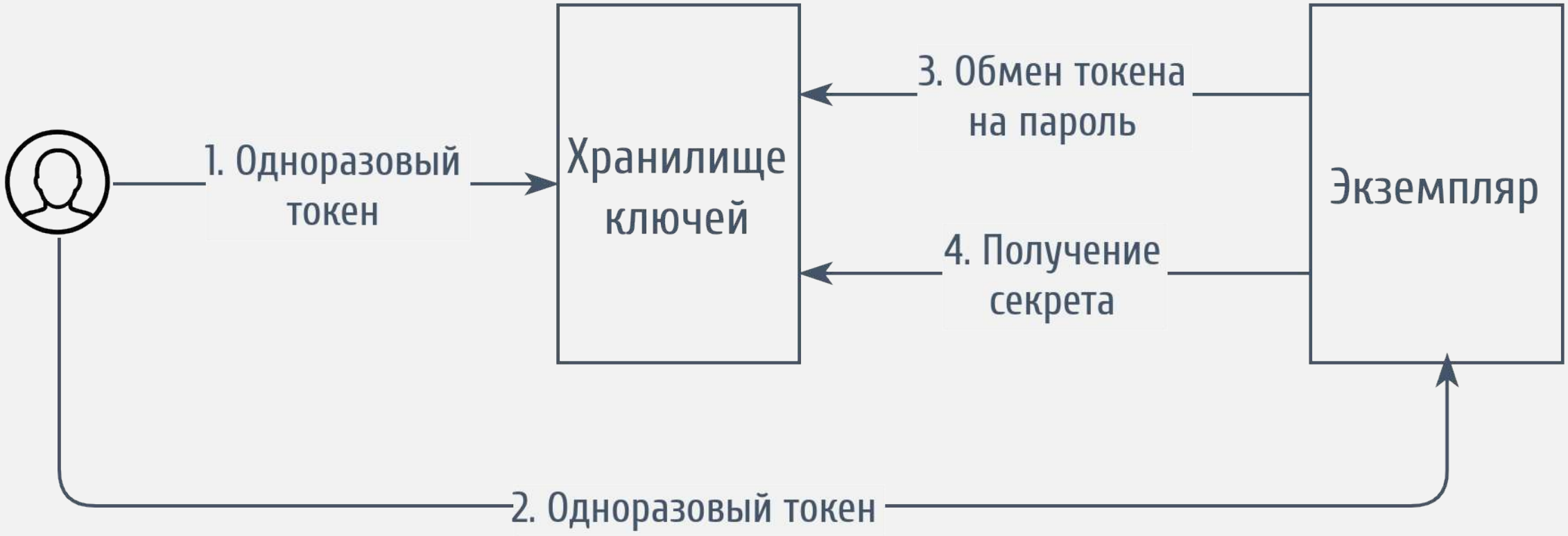
SIEM — security information and event management



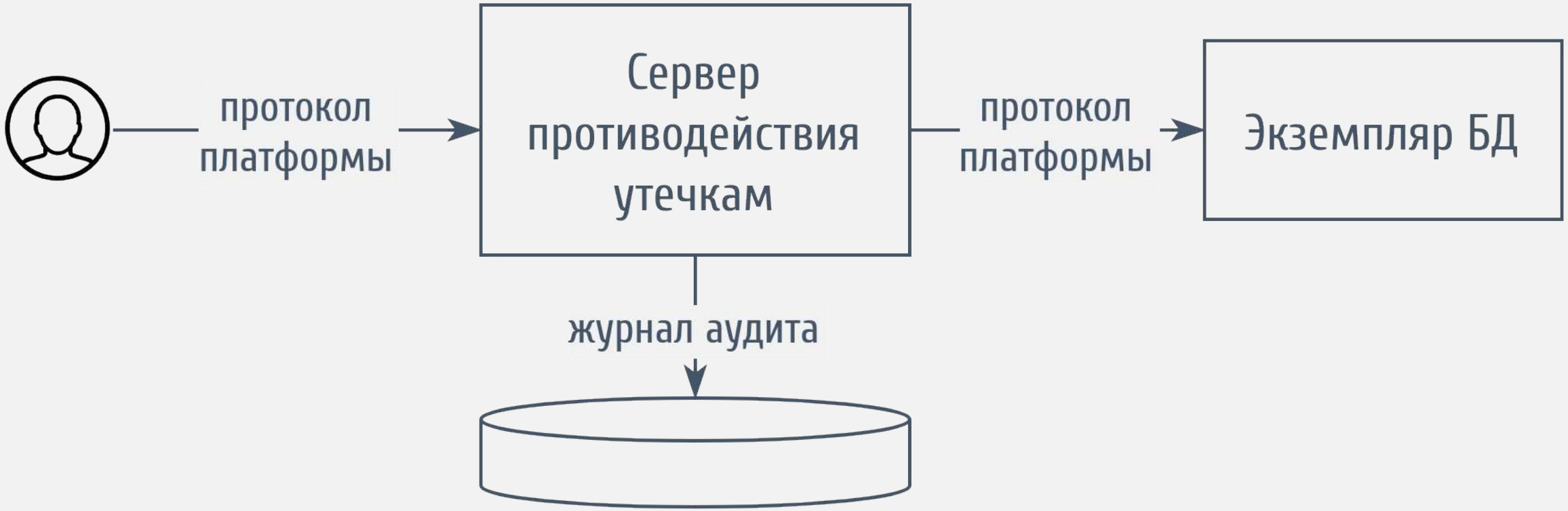
Управление секретами

KMIP, Key Mgmt Interoperability Protocol
HSM — Hardware Security Module

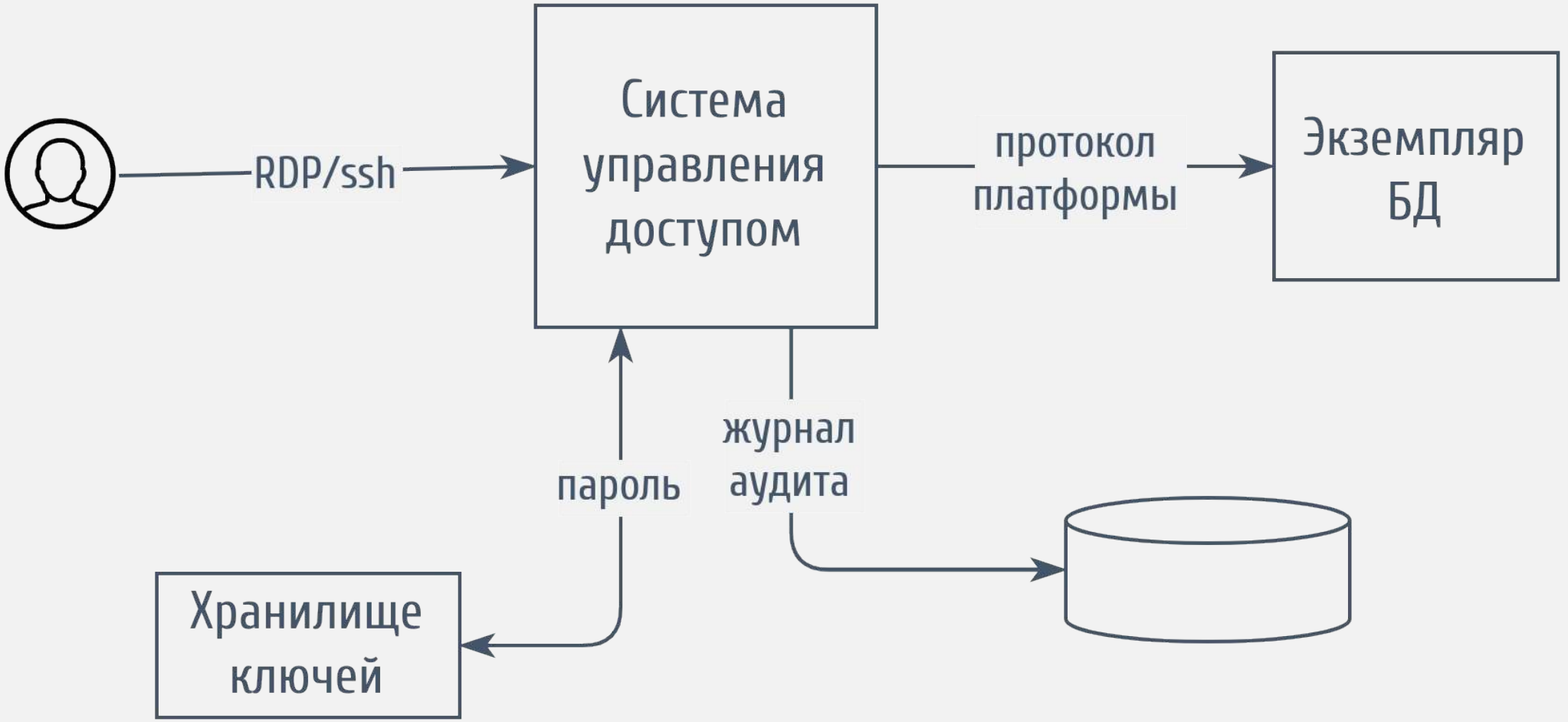
Windows Data Protection API
HashiCorp Vault



Data leak prevention (DLP)



Privileged access management (PAM)



Что же из этого следует?

Ролевая модель

Матрица ролей

WAF

Хранилище секретов

SIEM

Шифрование данных

DLP

PAM

RLS, LBAC

Ещё два слова о Platform V Pangolin

- Прозрачное шифрование данных
- Расширенные возможности аудита
- Управление парольными политиками
- Защита от привилегированных пользователей

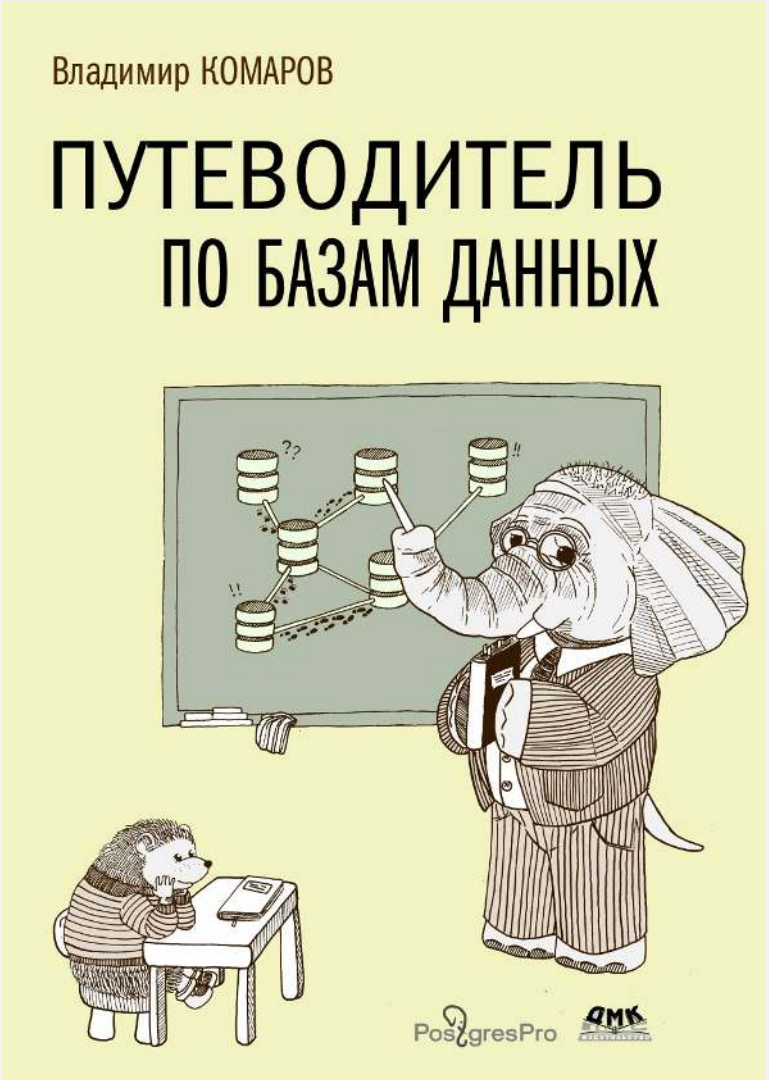
- Скрипты для развёртывания отказоустойчивого кластера
- Кинцуги (金継ぎ) – консоль управления

- Фиксация и подмена планов запросов
- Подготовленные запросы с использование пула соединений

Пользуясь случаем

Путеводитель по базам данных

- Классификация баз данных
- Архитектура СУБД
- Доступ к данным
- Распределённые СУБД
- Восстановление при сбоях
- Эксплуатация баз данных
- Безопасность баз данных



Спасибо за внимание!

PLATFORM V

Владимир Комаров
vkomarov@sbertech.ru