



Построение и автоматизация процесса управления уязвимостями на объектах КИИ (АСУ ТП)

Алексей Орехов

Руководитель производственно-технологического
управления HTS «Вулкан»

Контекст и вызовы VM

32% от всех методов атак по данным PT на март 2025

+15% и более рост числа уязвимостей в год (NVD)

+12% рост доли кибератак на российские компании с использованием уязвимостей (ГК Солар)

85,5% активов имеют уязвимости (Edgescan)

273 552 уязвимости в NIST NVD на 01.04.2025

Уязвимости в KillChain

Этап	Использование уязвимостей (%)	Комментарий	Источник
Reconnaissance	~0-5%	Редко - разведка обычно пассивна	MITRE ATT&CK, 2023
Initial Access	40-60%	Фишинг с эксплойтами, RDP/VPN-уязвимости	IBM X-Force 2023
Defense Evasion	10-20%	Использование уязвимостей в EDR/антивирусах	CrowdStrike 2024
Execution	70-80%	RCE, эксплуатация уязвимостей в ПО	Verizon DBIR 2023
Persistence	30-50%	Уязвимости в автозапуске, сервисах	Mandiant M-Trends 2024
Privilege Escalation	50-70%	LPE-уязвимости в ОС/ПО	Microsoft Digital Defense Report 2023
Lateral Movement	30-50%	Эксплуатация SMB, RPC, AD-уязвимостей	CISA Known Exploited Vulnerabilities
Collection	~5-10%	Редко - чаще легитимные инструменты	MITRE ATT&CK
Exfiltration	~5-15%	Уязвимости в DLP/брандмауэрах	Symantec Threat Report 2023
Impact	20-40%	Эксплуатация уязвимостей в шифровании/деструктивных атаках	Kaspersky ICS CERT 2023

Распространенный подход

Отсутствуют мониторинг
и отчетность –
«уязвимость
Шрёдингера»

Нет обратной
связи по
устранению

Отсутствие
информации об
активах

Нет гарантий, что «все»
доступные обновления
устанавливаются «езде»

Автоматическая установка
всех доступных обновлений

Нет регламентов
взаимодействия
участвующих сторон

Не вовлечены ИТ
и Бизнес

Установка
ведется
бессистемно

И дает бессистемные
«результаты»



ИБ

ИТ

АСУ

вендор

Управление уязвимостями как процесс



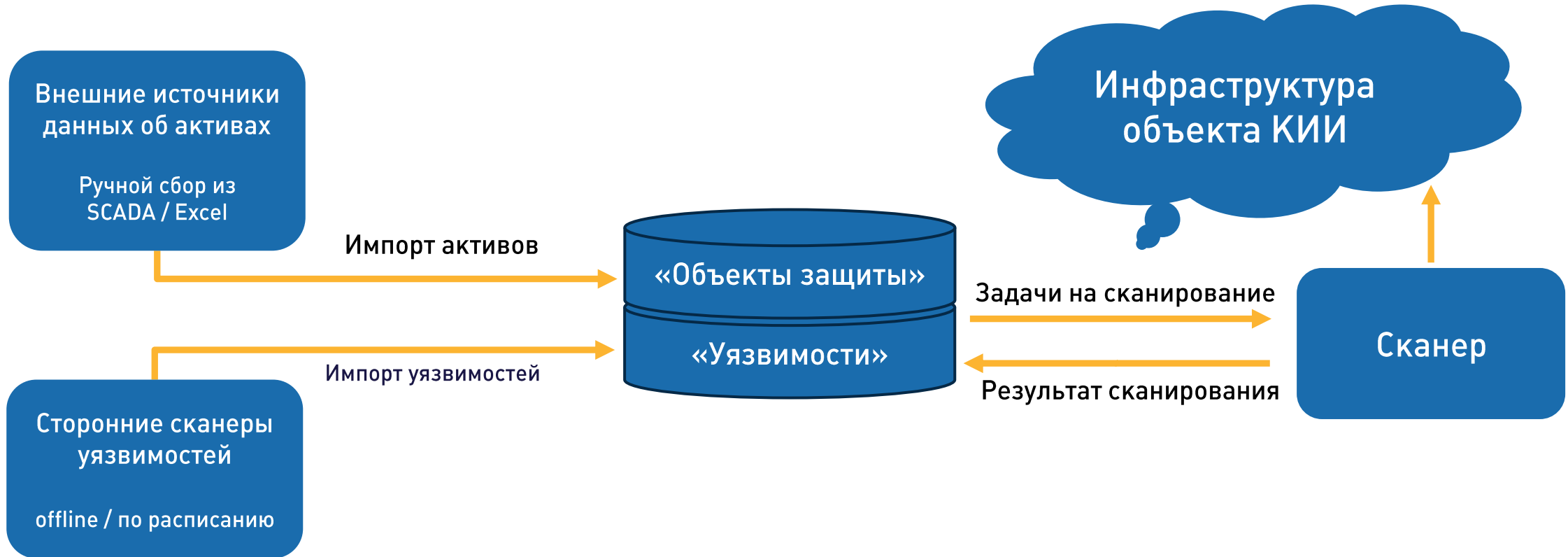
Масштаб процесса VM в АСУ ТП (КИИ)



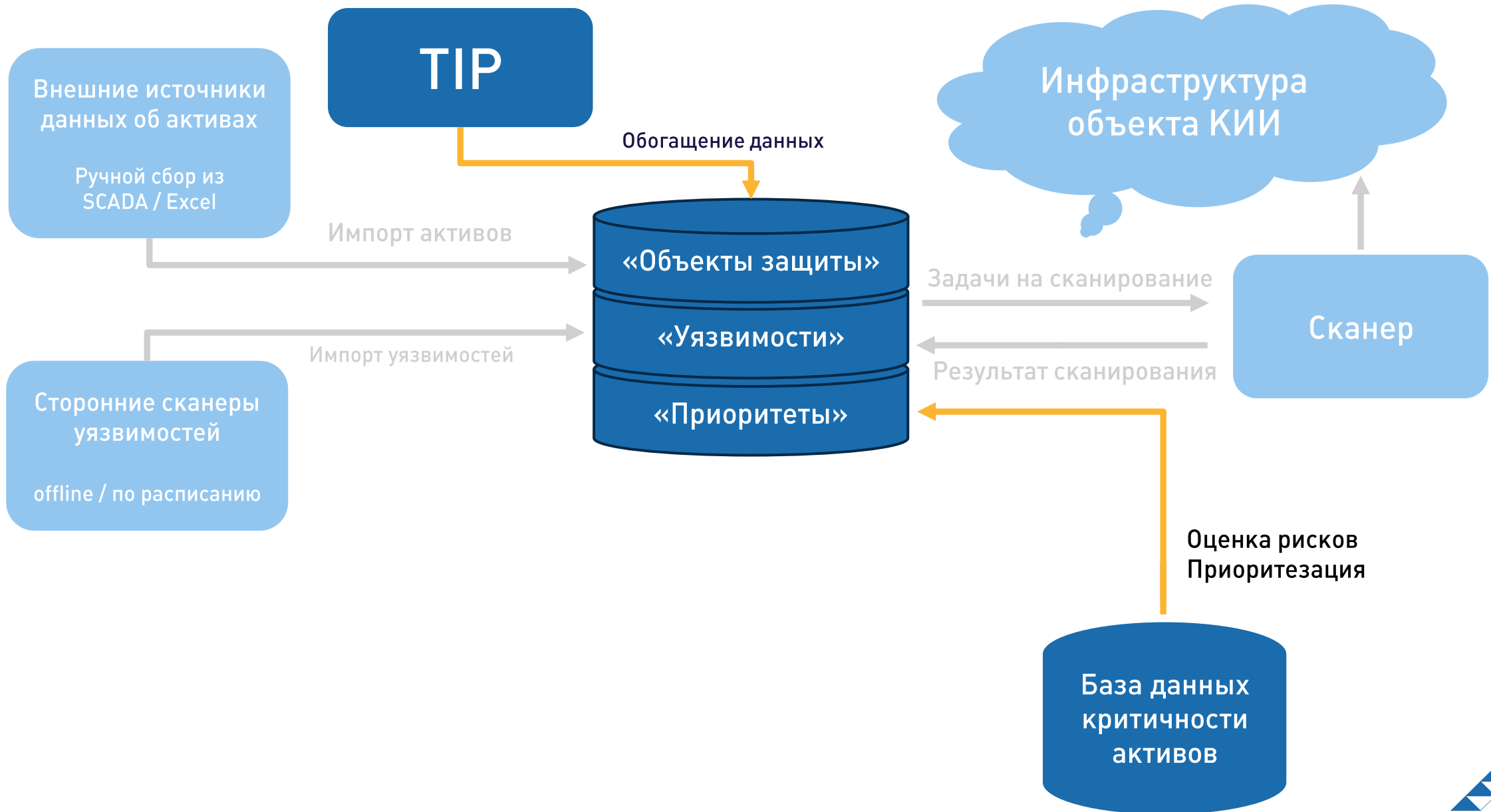


Подход к автоматизации VM

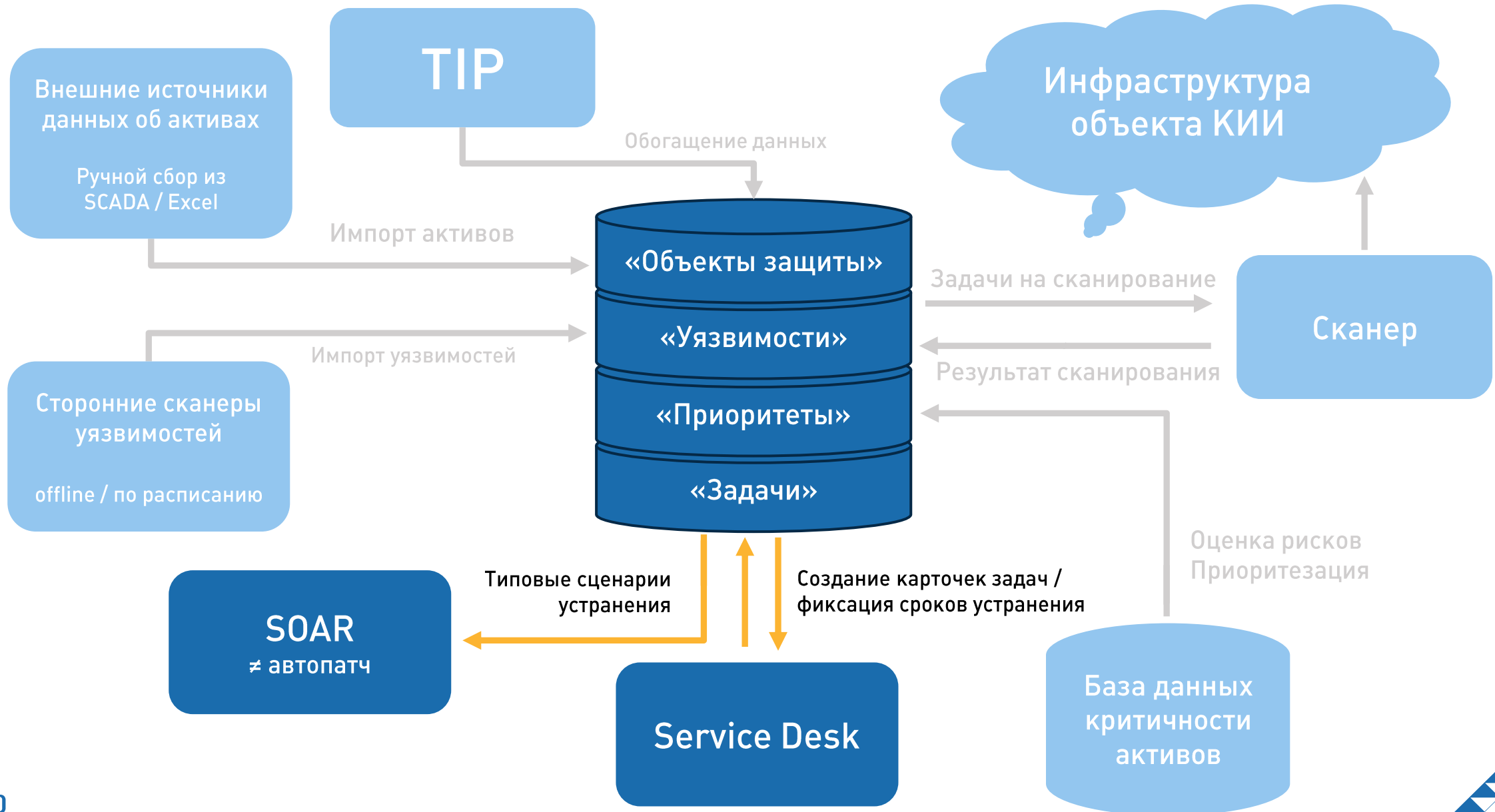
Инвентаризация объектов защиты



Поиск уязвимостей и их систематизация в привязке к объектам

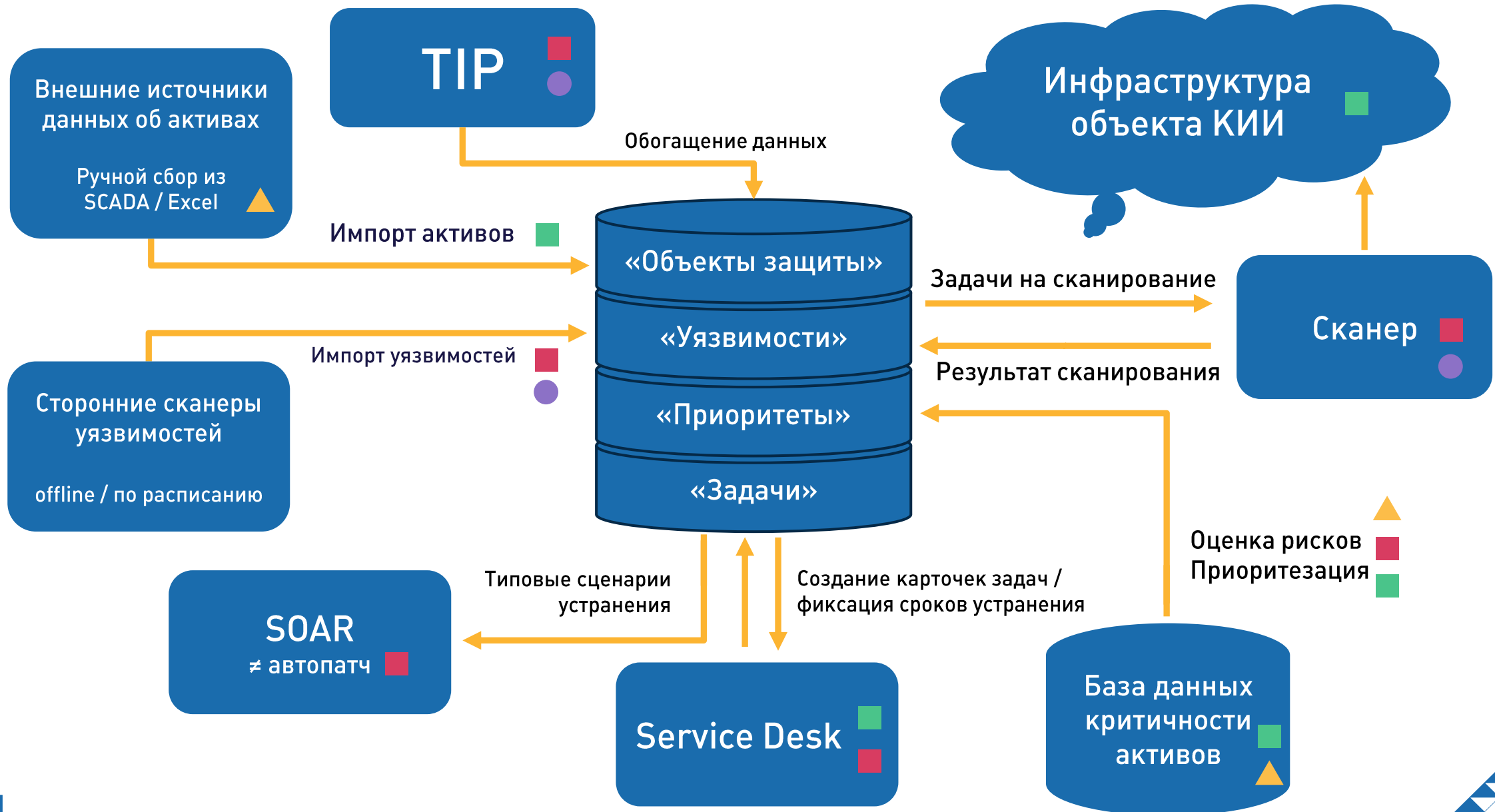


Обработка данных об уязвимостях для их устранения

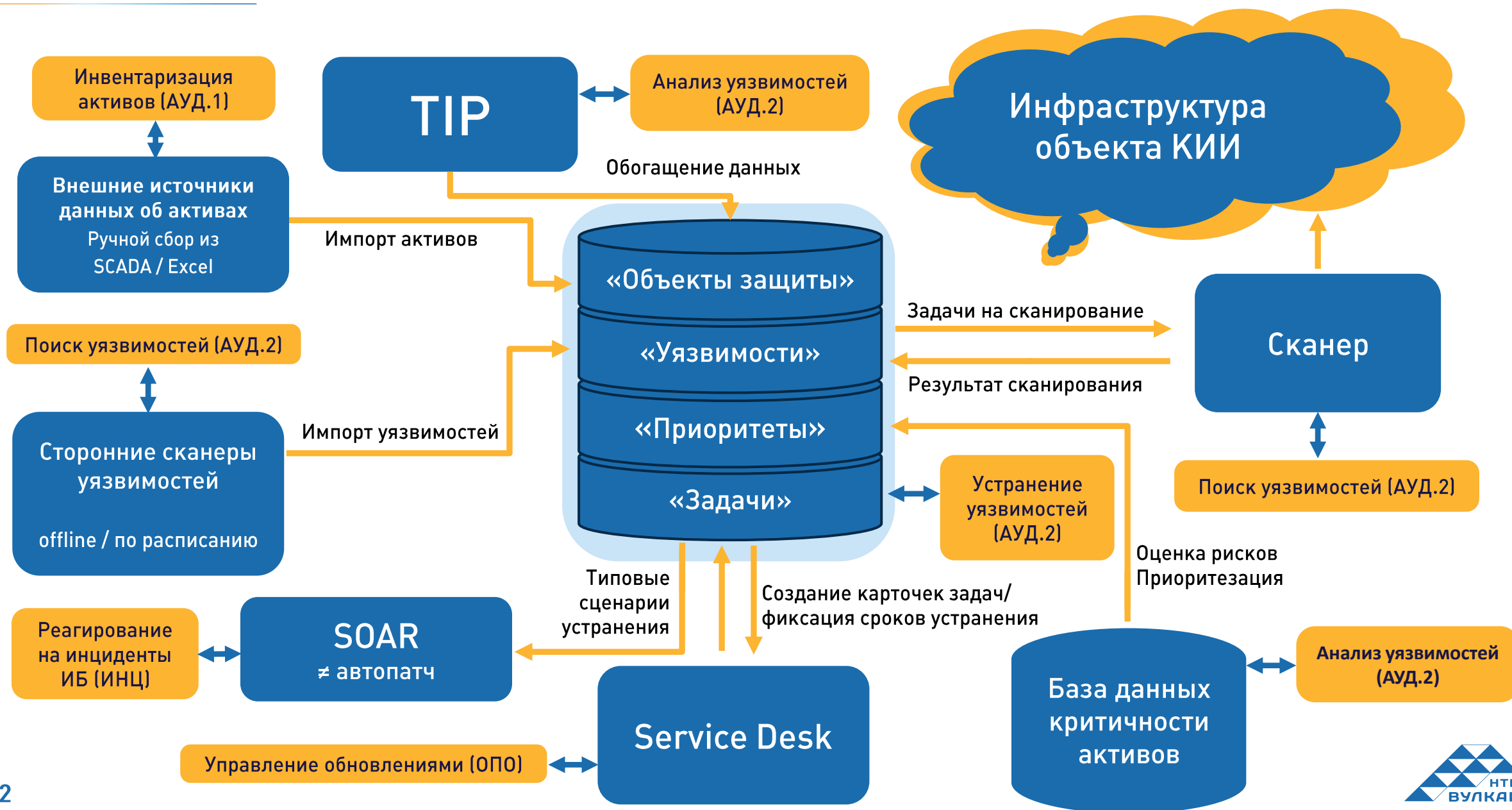


Модель автоматизации

▲ АСУ ТП ■ ИТ ■ ИБ ● Вендор



Интеграция процесса VM с приказом ФСТЭК 239



Платформа автоматизации

Оптимальный набор функций,
обеспечивающий быстрый запуск
«из коробки»

Инвентаризация

- Быстрое сканирование discovery и inventory
- Импорт информации из внешних источников

Выявление уязвимостей

- Управление работой средств сканирования
- В том числе собственный модуль сканирования

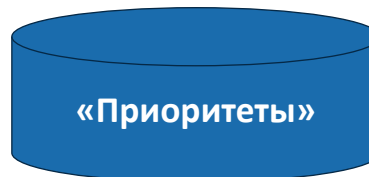
Обогащение результатов сканирования и приоритезация

- Рейтинг критичности по любым атрибутам
- Внешние источники или свой TI

Устранение и контроль

- Интеграция с внешними ServiceDesk
- Активоцентричная модель работы с уязвимостями

и/или



Гибкий конструктор
с возможностью дальнейшего
развития и кастомизации

Управление активами

- Формирование базы активов
- Выполнение автоматизированных действий по администрированию

Сканирование на уязвимости

- Управление сканированием на Windows/Linux хостах, средах контейнеризации, прикладном ПО, сетевых устройствах, базах данных
- В том числе собственный модуль сканирования

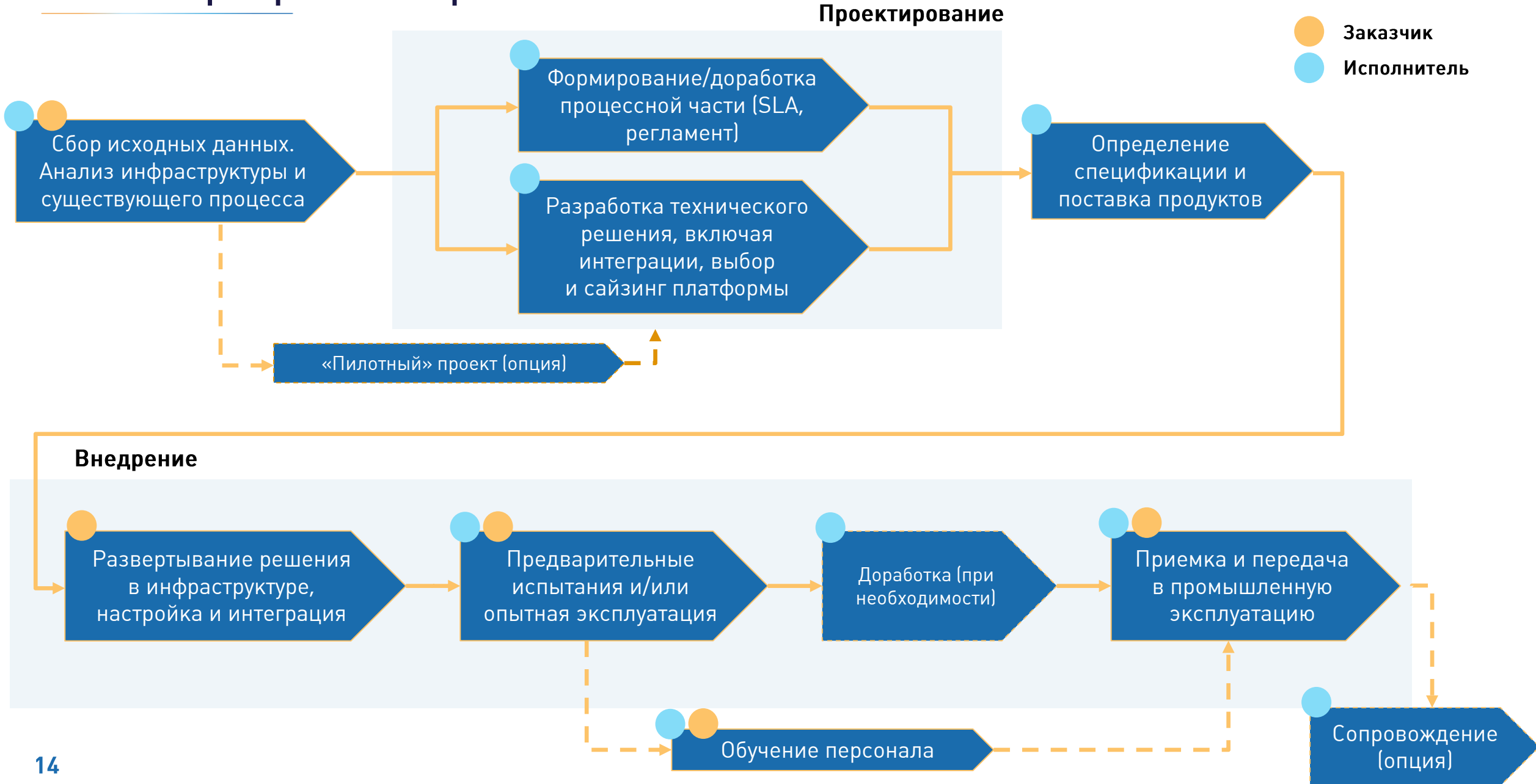
Обогащение экспертизой

- Дополнение информацией из БД ФСТЭК, NVD NIST, Microsoft
- Приоритезация на устранение

Устранение обнаруженных уязвимостей

- Интеграция с внешними Service Desk
- Автоподтверждение устранения
- Автопатчинг

Роль интегратора и состав работ





Спасибо за внимание

Москва

Электrozаводская, 27с4

ntc-vulkan.ru

+7 (495) 777-1310

marketing@ntc-vulkan.ru