

# Комплексный мониторинг с UDV ITM

Мониторинг IT-инфраструктуры,  
оборудования, приложений  
и сервисов предприятия  
с помощью одной платформы

# udv.group — разработчик надежных решений ИБ и ИТ

12+

лет на рынке ИБ и ИТ

Подтвержденный опыт интеграции в нефтегазовой отрасли, энергетике, металлургии

10+

патентов

Собственный исследовательский центр в области кибербезопасности

200+

разработчиков

Распределенная команда со штаб-квартирой в Екатеринбурге

1500+

инсталляций

Внедренные проекты по защите АСУ ТП и корпоративных сетей

Проблематика

# Актуальные вызовы предприятий

01

## Потеря критически важных данных

Выход из строя объектов хранения данных влечет за собой потерю критически важной информации, включая производственные логи, проектную документацию и прочее

02

## Нарушение бизнес-процессов

Сбой ИТ предприятия влияет на качество:  
– выполнения технологических расчетов;  
– управления производственными процессами.

03

## Финансовые и репутационные потери

Штрафы и судебные иски за причинение ущерба окружающей среде, простой оборудования, невыполнение договорных обязательств перед заказчиками

04

## Сбой или остановка производственного процесса

Резкая остановка производства может спровоцировать неконтролируемые выбросы или утечки опасных веществ в атмосферу, почву или воду



On-premise решение

# Зонтичный мониторинг с UDV ITM



## Сертифицированное ПО

Сертификат соответствия ФСТЭК России №4432, от 27.07.2021 г.



## Работает с разными ОС

Доступна инсталляция на Astra Linux, РЕД ОС и АЛЪТ СП



## Сделано в РФ

Внесено в реестр ПО. Реестровая запись №17690 от 19.05.2023

## Анализ сегментов ИТ-инфраструктуры

Позволяет контролировать нагрузку, повысить отказоустойчивость систем, снизить эксплуатационные расходы

## Система виджетов мониторинга

Обеспечивает прозрачность всей инфраструктуры ИТ, сокращает необходимое время на принятие мер по устранению неисправностей

## Агрегация данных со всех уровней

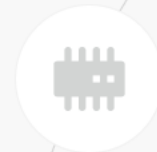
Возможность создания многоуровневой системы мониторинга, которая позволяет отслеживать распределенные объекты мониторинга

## Инвентаризация ИТ-объектов

Позволяет поддерживать актуальность перечня оборудования ИТ-инфраструктуры и учитывать их фактическое состояние

## Система уведомлений

Своевременно оповещает ответственных о возникновении проблемы, минимизируя простой оборудования и сокращая финансовые издержки





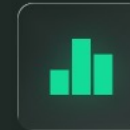
Функционал UDV ITM

# Эффективное решение для мониторинга ИТ-инфраструктуры



## Единая карта здоровья

- Общая картина компонентов
- Карта здоровья сервисов
- Отчеты SLA



## Минимизация рисков

- Мониторинг ИТ-объектов
- Оценка влияния ИТ на бизнес
- Оповещения о возможных сбоях



## Эффективное устранение сбоев

- Быстрый поиск источника
- Приоритизация работы над сбоями



## Уведомления и автоматизация

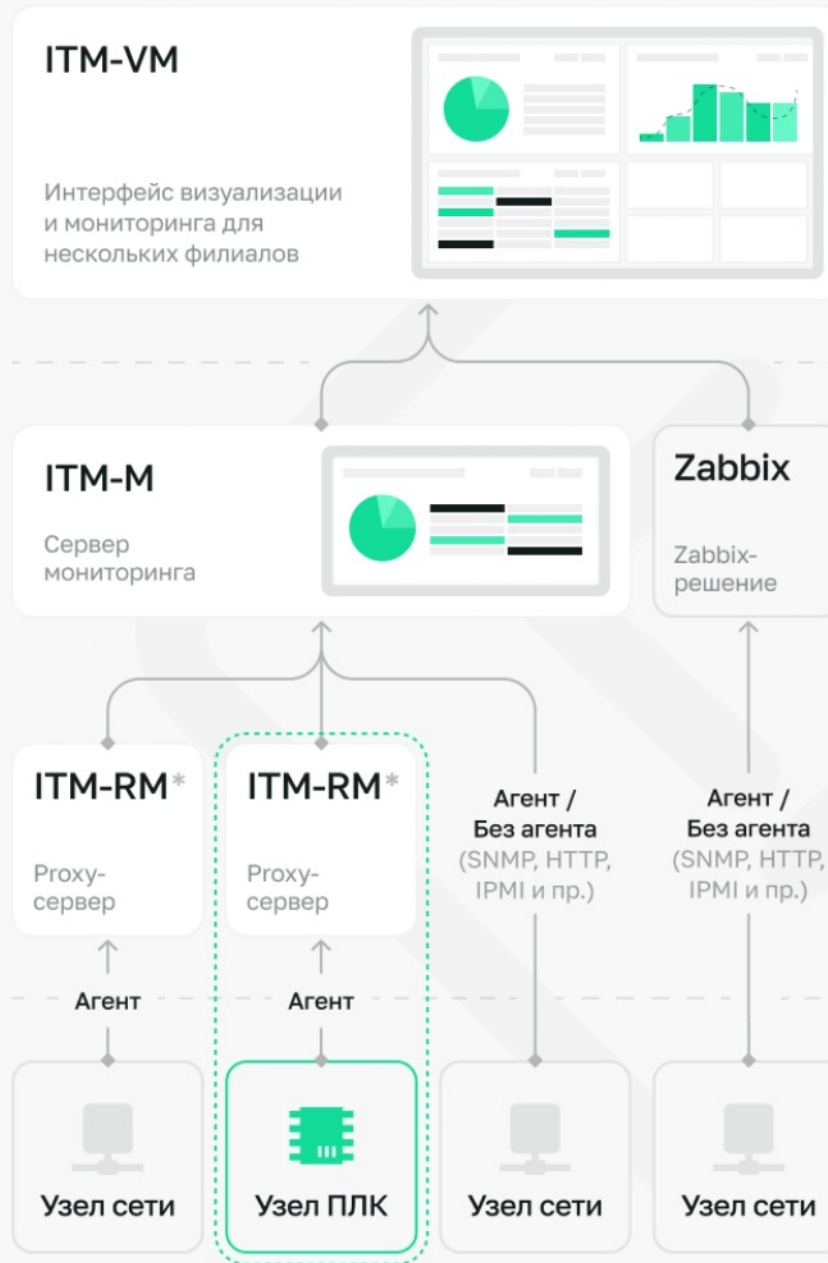
- Уведомления об отклонениях и автоэскалация
- Автооткрытие тикетов

Комплексный подход

# Архитектура UDV ITM

«Безопасный Zabbix», который позволяет контролировать ИТ-инфраструктуру предприятия из единого окна интерфейса

- ✓ **Консолидация данных** со всех систем мониторинга в масштабах всего предприятия
- ✓ **Поддержка Zabbix-систем** для бесшовной интеграции с текущими Zabbix-системами предприятия
- ✓ **Миграция данных с Zabbix-систем** на отечественные серверы мониторинга UDV ITM в рамках импортозамещения
- ✓ **Автоматизация рутинных задач** сбор дополнительных данных для анализа, установка агентов на узлы сети и пр.



Современная визуализация в графическом интерфейсе

Вывод обработанных данных с нескольких филиалов в едином окне интерфейса

Сборка и обработка данных со всех узлов ИТ-инфраструктуры

- Мониторинг узлов и сервисов
- Инвентаризация и опрос объектов мониторинга
- Консолидация и корреляция данных

\* ITM-RM не является обязательным элементом архитектуры. Опрос может осуществляться при помощи ITM-M

События и инциденты в ИТ-инфраструктуре

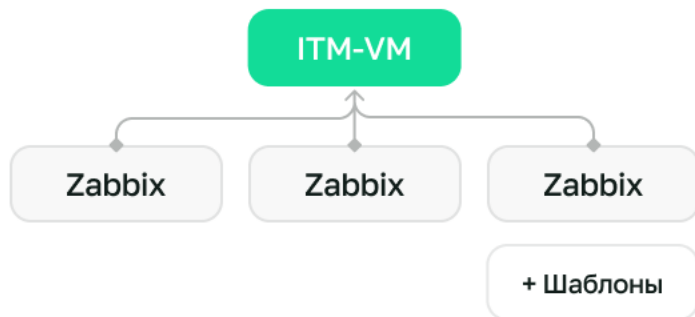
«Сырые» данные с узлов сети



# Этапы внедрения комплексного решения в инфраструктуре с Zabbix

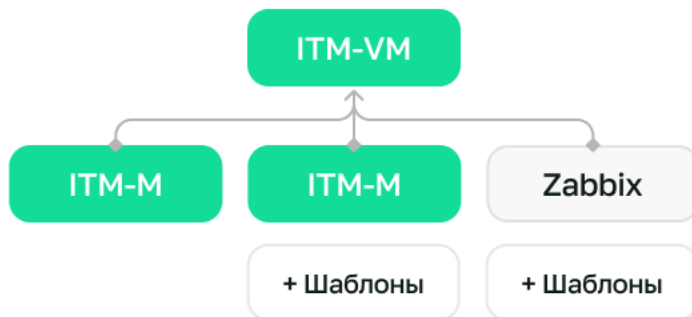
## 01 Только консолидация

- Оставить Zabbix-системы в инфраструктуре и консолидировать информацию с них в ITM-VM
- Разработать Zabbix-шаблоны под специфичное оборудование



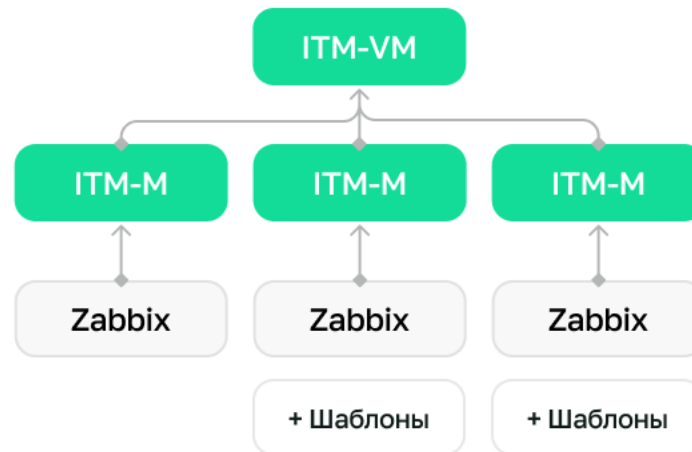
## 02 Смешанный

- Оставить Zabbix-системы и постепенно внедрять сервер мониторинга ITM-M, консолидировать данные со всех систем в ITM-VM
- Разработать шаблоны под специфичное оборудование, использовать их как в Zabbix, так и в ITM-M



## 03 Безопасный мониторинг на базе сертифицированного решения

- Первым этапом мигрировать данные с Zabbix на ITM-M, вторым – подключить системы к единому «зонтику» ITM-VM
- Разработать шаблоны под специфичное оборудование



Контроль качества

# Безопасная разработка

Решение UDV ITM разрабатывается в соответствии с принципами безопасной разработки и регулярно проходит испытания:

✓ **Анализ состава**  
модулей, интерфейсов  
и конфигурации

✓ **Анализ безопасности**  
и поиск потенциальных  
уязвимостей

✓ **Независимая  
экспертная оценка**  
исходного кода

✓ **Динамический  
и статический  
анализ кода**

ФСТЭК России выявила критическую уязвимость CVE-2024-42327 в Zabbix, которая позволяет злоумышленникам выполнять произвольные SQL-запросы

Благодаря поддержке, строгому контролю качества и принципам безопасной разработки, пользователи UDV ITM эта уязвимость не коснулась



## Драйверы рынка UDV ITM



Гос. сектор

Импортозамещение Zabbix

### Остальные субъекты КИИ

#### Субъекты КИИ

- Гос. органы
- Гос. учреждения
- Юр. лица
- ИП

→ которым принадлежат

#### Объекты КИИ

- Информационные системы
- Информационно-телекоммуникационные сети
- Автоматизированные Системы Управления

→ которые обеспечивают взаимодействие

↓ работающие в отраслях

#### Отрасли

Горно-добывающая, металлургическая, химическая, оборонная, ракетно-космическая, энергетика, ТЭК, банки, связь, транспорт и др.

**Коммерческий  
сегмент**

Потребность коммерческого сегмента в обеспечении безопасности инфраструктуры

## СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ  
№ РОСС RU.0001.01БИ00

### СЕРТИФИКАТ СООТВЕТСТВИЯ № 4432

Внесен в государственный реестр системы сертификации  
средств защиты информации по требованиям безопасности информации  
27 июля 2021 г.

Выдан: 27 июля 2021 г.  
Действителен до: 27 июля 2026 г.

Переформлен: 30 января 2025 г.

Настоящий сертификат удостоверяет, что программный комплекс мониторинга безопасности и контроля ресурсов «CyberLympha ГТМ», разработанный и производимый ООО «СайберЛимфа», является программным средством общего назначения со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции идентификации и аутентификации, управления доступом и регистрации событий безопасности, соответствует требованиям по безопасности информации, установленным в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 6 уровню доверия и технических условиях 05028144.620129.200-ТУ, при выполнении указаний по эксплуатации, приведенных в формуляре 05028144.620129.200 30.

Сертификат выдан на основании технического заключения от 03.06.2021, оформленного по результатам сертификационных испытаний испытательной лабораторией АО «Эшелон-Северо-Запад» (аттестат аккредитации от 28.05.2019 № СЗИ RU.0001.01БИ00.Б035), и экспертного заключения от 07.07.2021, оформленного органом по сертификации АО «Лаборатория ППШ» (аттестат аккредитации от 09.03.2017 № СЗИ RU.0001.01БИ00.А006), и технического заключения от 28.11.2024, оформленного ООО «СайберЛимфа».

Заявитель: ООО «СайберЛимфа»

Адрес: 121205, г. Москва, вн.тер.г. муниципальный округ Можайский, тер. Сколково инновационного центра, ул. Нобеля, д.7, эт.4

Телефон: (800) 511 65 51

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ



В. Лютиков

Применение сертификата информационной безопасности, указанной в настоящем сертификате соответствия, на объектах (объектах информации) осуществляется при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

Сертификат соответствия ФСТЭК России  
№4432, от 27.07.2021 г., 6 УД, ТУ

Сертифицированное решение



# Подходит для защиты

Объектов КИИ (пр. № 239) и АСУ ТП (пр. № 31):

- ОДТ.3: Контроль безотказного функционирования средств и систем
- ОДТ.8: Контроль предоставляемых вычислительных ресурсов и каналов связи
- АУД.1: Инвентаризация информационных ресурсов

ГИС, МИС (пр. №117) и ИСПДн (пр. № 21):

- ОДТ.3: Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование
- ОДТ.7: Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации
- АНЗ.4: Контроль состава технических средств, программного обеспечения и средств защиты информации



Безопасный инструмент для мониторинга инфраструктуры на базе уже знакомого решения, не требующий переобучения

# Следующие шаги

01

Предоставим доступ  
к демо-стенду

02

Поможем с миграцией  
на решение UDV ITM

03

Консалтинг  
и разработка шаблонов

04

Проведение  
испытаний

05

Перевод продукта в режим  
эксплуатации

06

Осуществление  
технической поддержки



При необходимости готовы провести пилот в вашей инфраструктуре

Закажите пилотный проект  
или персональную демонстрацию  
наших решений

# Контакты

8-800-511-65-51

Телефон для связи

commercial@udv.group

Электронная почта

udv.group

Сайт

@udv\_group

Телеграм

620100, г. Екатеринбург, ул. Сибирский тракт, 12, строение 7, этаж 4

Адрес



udv.group