Система мониторинга UDV ITM

Комплексное решение
для полного контроля инфраструктуры

Ксения Могилева
Менеджер продукта UDV ITM

Сергей Овчинников
Директор по маркетингу UDV Group

udv|group

UDV Group — ведущий разработчик в области кибербезопасности

UDV Group предоставляет единый портфель решений для защиты технологических сетей, корпоративного сегмента и автоматизации в области объектовой безопасности:

- защита АСУ ТП и объектов КИИ
- мониторинг инфраструктуры
- реагирование на инциденты ИБ
- автоматизация работы SOC
- выполнение требований регуляторов

200+
разработчиков в штате

Распределённая команда
со штаб-квартирой в Екатеринбурге

1000+
инсталляций

Проекты по защите АСУ ТП
и корпоративных сетей

10+
патентов

Собственный исследовательский
центр в области кибербезопасности

10
лет на рынке

Подтвержденный опыт
интеграции в крупных предприятиях
нефтегазовой отрасли, энергетики,
металлургии и других

udvgroup

Продукты UDV Group

Защищают технологические сети от киберугроз, поддерживая бесперебойность производственных процессов.

Автоматизируют реагирование на инциденты и другие процессы ИБ, выстраивая целостную систему защиты информации в соответствии с требованиями регуляторов.

Управляют жизненным циклом оборудования инженерно-технических средств охраны (ИТСО) и мониторингом их работы, а также позволяют автоматизировать управление доступом на охраняемую территорию.

* Релиз UDV NTA запланирован на 2025 год

О чём поговорим?

- Сервер мониторинга. ITM-M и ITM-RM
- Результаты нашего исследования в 2024 году
- Зонтичная система мониторинга: визуализация данных и управление системой. ITM-VM
- Мониторинг инженерных систем
- Live demo продукта
- Q&A

Сервер мониторинга. «Просто Zabbix?»

Наши Заказчики действительно привыкли к Zabbix

Но столкнулись с трудностями

- Отсутствие официальной поддержки в РФ
- Отсутствие документации на русском языке
- Ужесточение требований со стороны регуляторов привело к сложностям использования open-source-решений

С другой стороны

- Внедрение альтернативных решений требует дополнительных затрат (не только на внедрение само по себе, но и на обучение персонала)
- Благодаря активному сообществу пользователей Zabbix, возможен обмен опытом между пользователями

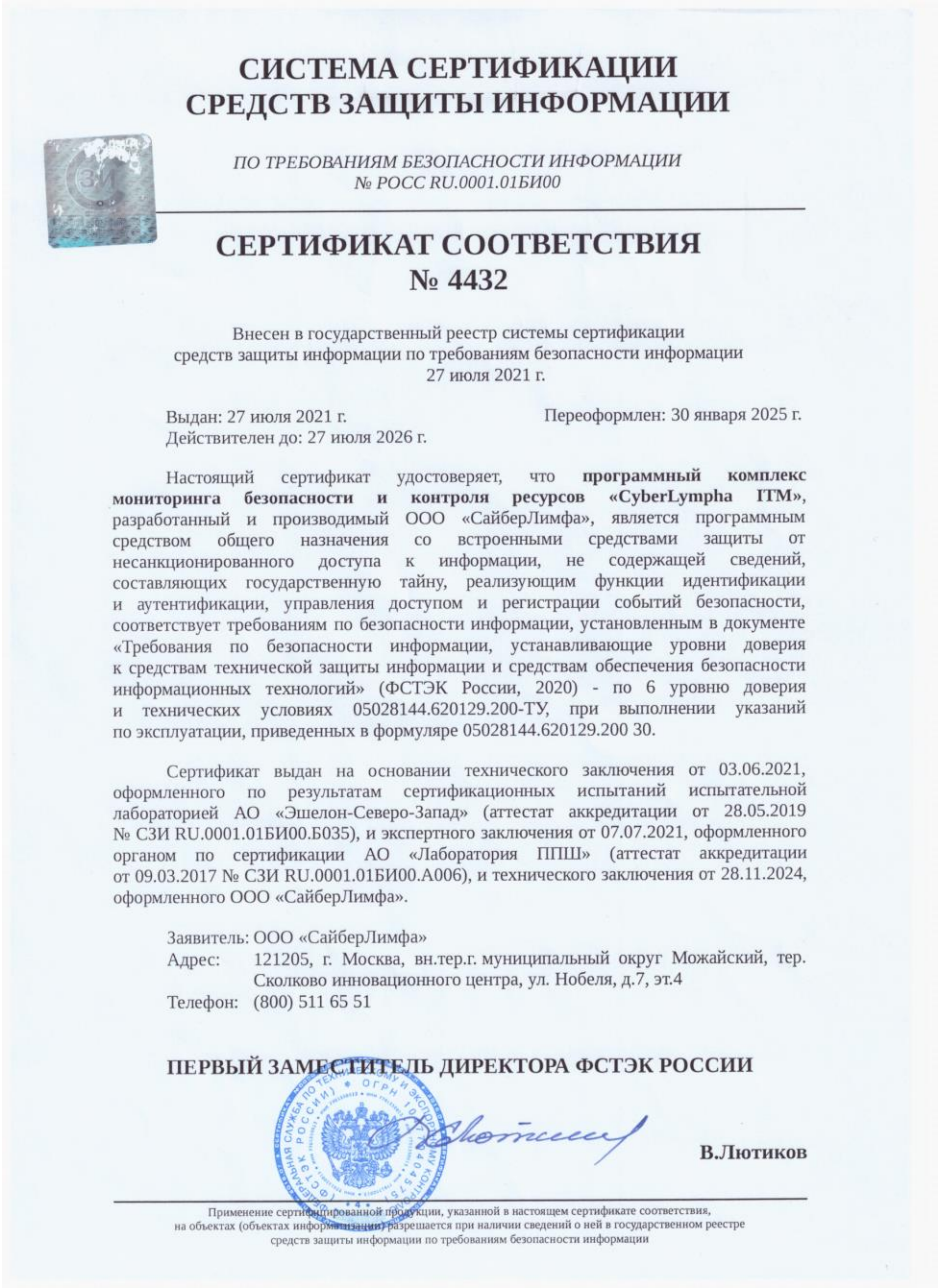
Мы предложили ITM: сервер мониторинга на базе Zabbix

Подходит для защиты значимых объектов КИИ

Сертификат соответствия ФСТЭК России №4432, переоформлен 30.01.2025 г., 6 УД, ТУ

С поддержкой в России

- Помощь в настройке системы
- Библиотека шаблонов и написание новых для специфичного оборудования
- Консалтинг
- Документация



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. Переоформлен: 30 января 2025 г.
Действителен до: 27 июля 2026 г.

Настоящий сертификат удостоверяет, что **программный комплекс мониторинга безопасности и контроля ресурсов «CyberLympha ITM»**, 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 сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

ФСТЭК России выявила критическую уязвимость CVE-2024-42327 в продукте для мониторинга корпоративных сетей с открытым исходным кодом Zabbix, которая позволяет злоумышленникам выполнять произвольные SQL-запросы.

Уязвимость в Zabbix не коснется пользователей UDV ITM

Система мониторинга инфраструктуры UDV ITM основана на Zabbix. Решение разрабатывается в соответствии с принципами безопасной разработки и регулярно проходит ряд испытаний:

- анализ состава модулей, конфигурации и интерфейсов;
- анализ безопасности решения на основе открытых источников, в том числе поиск известных и потенциальных уязвимостей;
- экспертная оценка исходного кода;
- статический и динамический анализ исходного кода.

Уязвимость CVE-2024-42327 не затрагивает какие-либо версии UDV ITM, находящиеся в эксплуатации у заказчиков. Релиз новой версии UDV ITM 1.8 с сервером мониторинга на базе Zabbix 7.0.2 планируется в декабре 2024 г., все испытания уже завершились. Планируемое обновление сертификата ФСТЭК России в связи с выпуском новой версии ожидается также в I квартале 2025 г.

Уязвимость в Zabbix не коснется пользователей UDV ITM – udv.group

Что ещё ждут от системы мониторинга и с какими проблемами сталкиваются Заказчики?

Исследование 2024 результаты

Метод глубинных интервью

Респонденты — ИТ-специалисты,
которые несут ответственность за работоспособность инфраструктуры
и имеют опыт внедрения и эксплуатации различных систем мониторинга

Выводы

- Есть потребность консолидировать информацию из разных источников
- Нет желания эксплуатировать сложный инструмент – «швейцарский нож»
- Есть потребность в отечественном продукте для инфраструктурного мониторинга
- Необходимость в сертификате ФСТЭК России зависит от вида деятельности компании
- Пользователи сталкиваются с «белым шумом» из-за трудностей с тонкой настройкой пороговых значений
- Есть потребность не обнаруживать, а предотвращать инциденты
- Система мониторинга должна быть интегрирована с ITSM/Service Desk-системами

Исследование подтвердило интерес в зонтичном мониторинге, как в единой системе визуализации и управления

Наше решение: ITM-VM

Архитектура системы

Сервер визуализации и управления

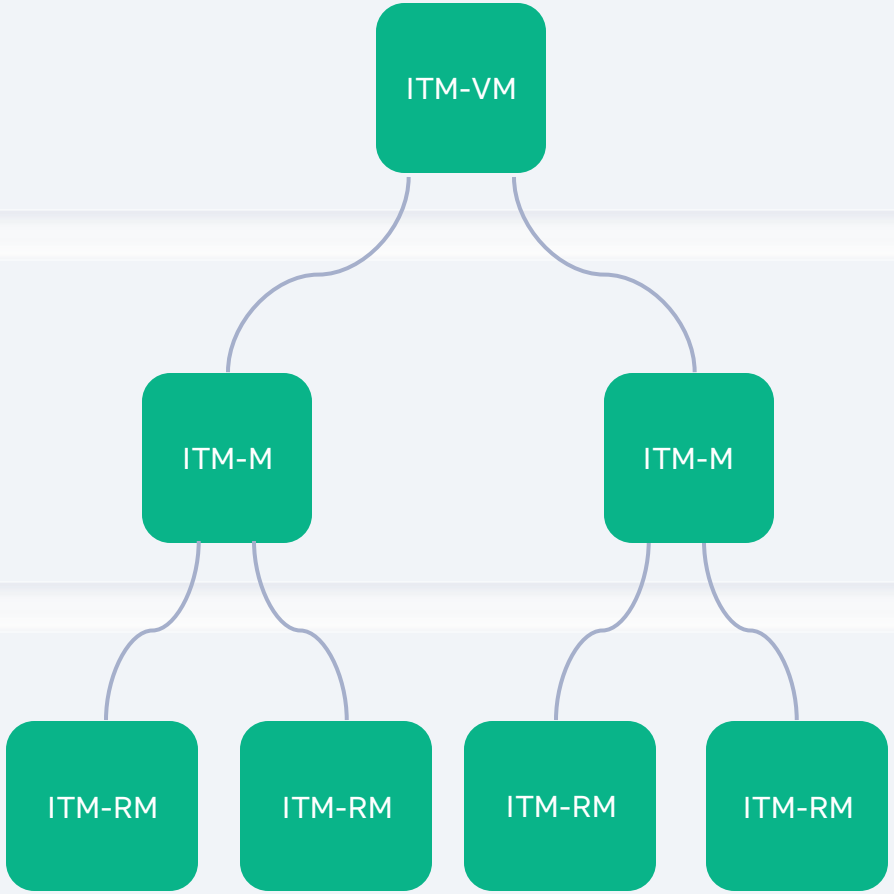
- консолидация информации об объектах мониторинга
- зонтичный мониторинг всех филиалов

Сервер мониторинга

- агентный и безагентный мониторинг ИТ-ресурсов
- управление в том числе серверами удаленного мониторинга

Сервер удаленного мониторинга

- агентный и безагентный мониторинг удаленных объектов
- оптимизация трафика системы мониторинга

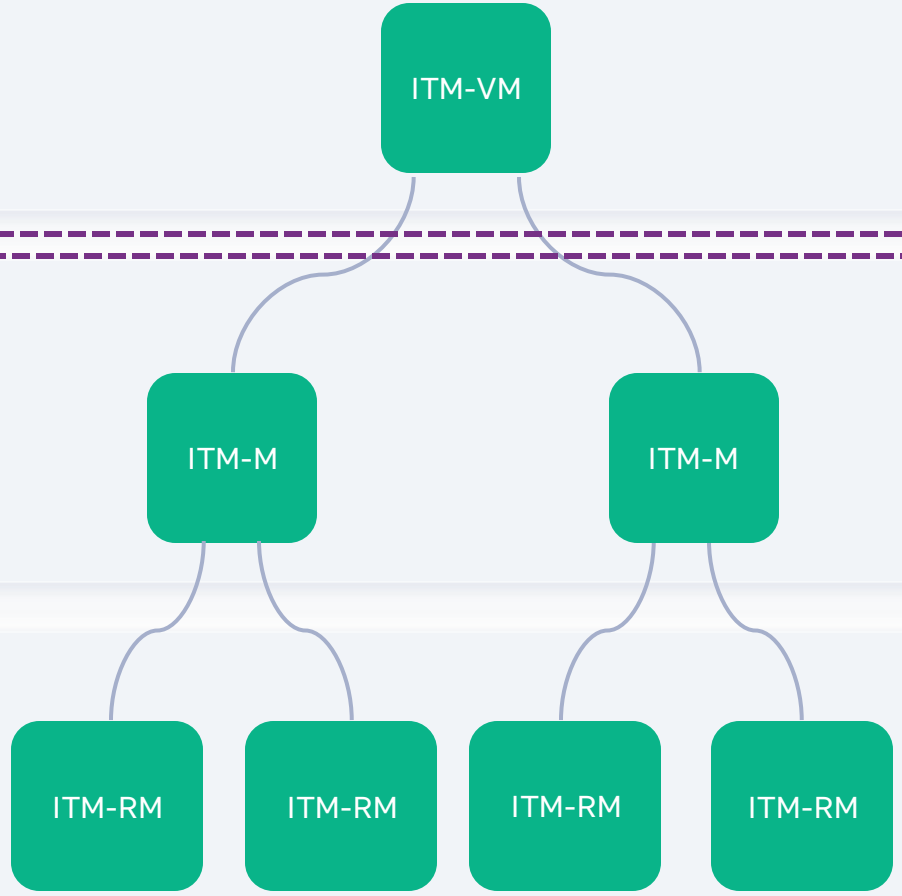


Архитектура системы

Система зонтичного мониторинга ITM

Сервер визуализации и управления

- консолидация информации об объектах мониторинга
- зонтичный мониторинг всех филиалов



Сервер мониторинга

- агентный и безагентный мониторинг ИТ-ресурсов
- управление в том числе серверами удаленного мониторинга

Сервер удаленного мониторинга

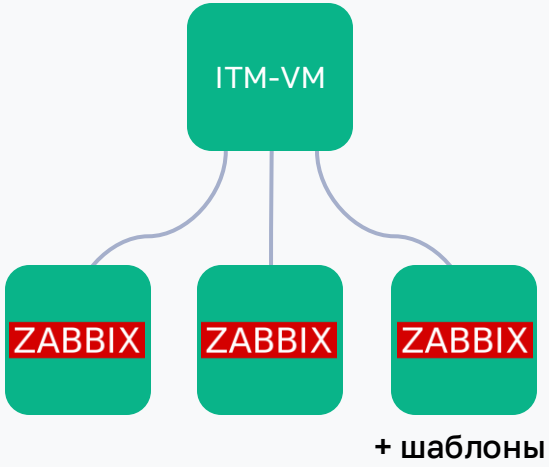
- агентный и безагентный мониторинг удаленных объектов
- оптимизация трафика системы мониторинга

Сервер мониторинга ITM

Сценарии использования в инфраструктуре с Zabbix

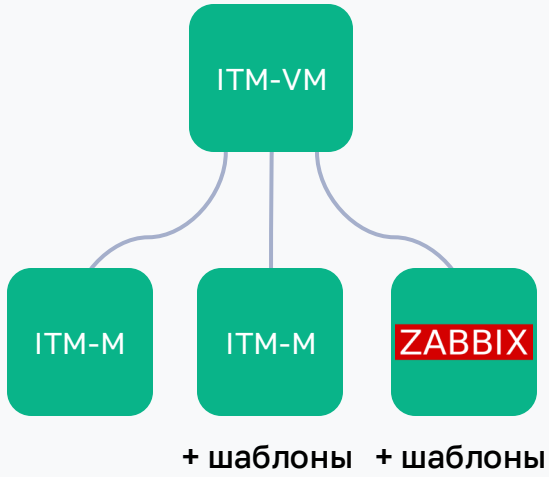
Только консолидация

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



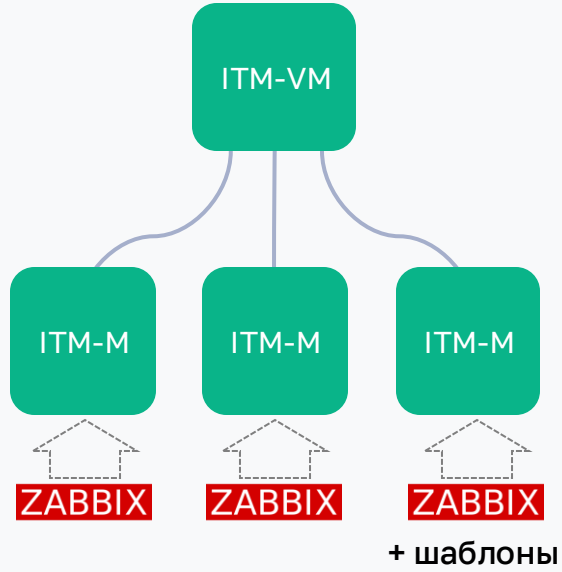
Смешанный

- 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



Импортозамещение

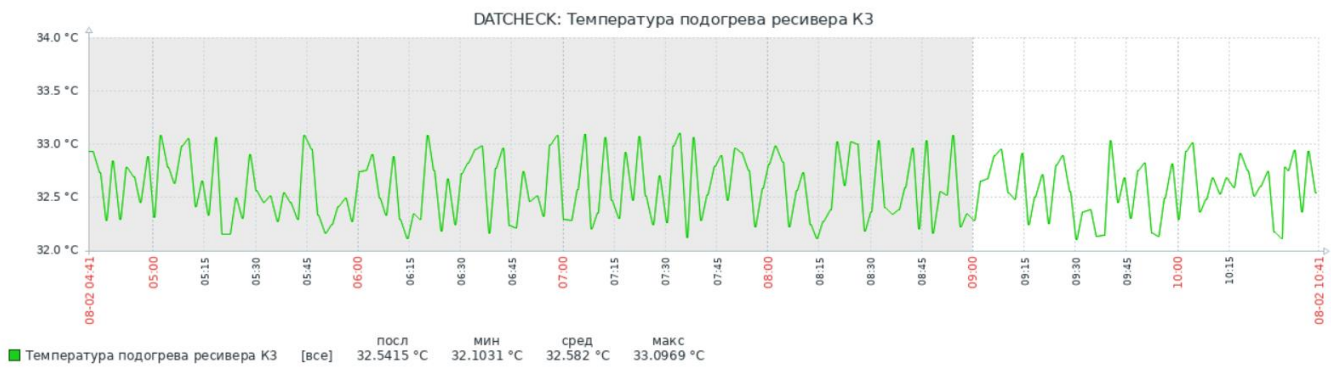
- Первым этапом мигрировать данные с Zabbix на ITM-M, вторым – подключить системы к единому «зонтику» ITM-VM
- Разработать шаблоны под специфичное оборудование



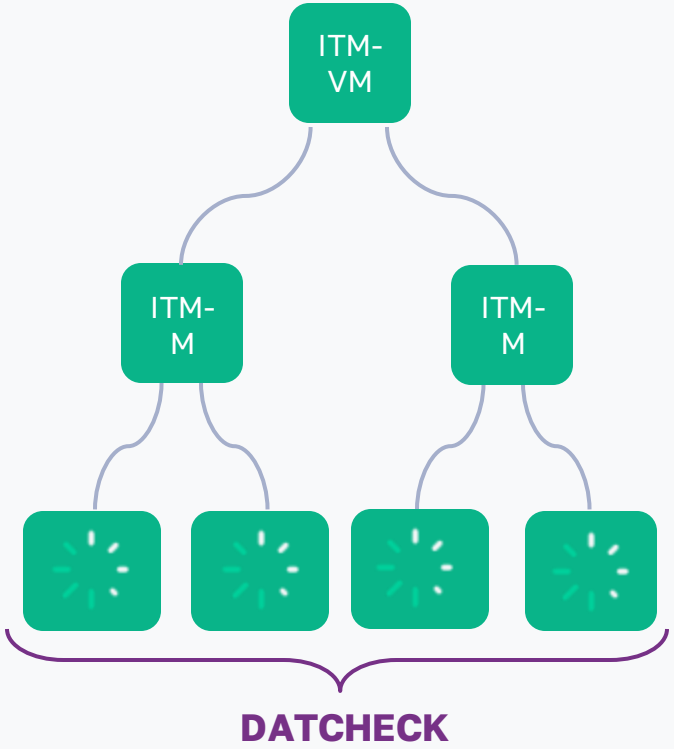
Мониторинг инженерных систем

Подтверждена интеграция с DATCHECK*

DATCHECK	**Обрывы датчиков** (2 элемента данных)				
	Обрыв датчика наружней температуры	29.07.2024 01:08:30	False		История
	Обрыв датчика температуры притока	29.07.2024 01:08:30	False		История
DATCHECK	**Система безопасности** (7 элементов данных)				
	Автоматика отключена	29.07.2024 01:08:30	False		История
	Сигнал "Авария АУГПТ"	29.07.2024 01:08:30	False		История
	Сигнал "Авария СБ"	29.07.2024 01:08:30	True		История
	Сигнал "Взлом"	29.07.2024 01:08:30	False		История
	Сигнал "На охране"	29.07.2024 01:08:30	True		История
	Сигнал "Пожар"	29.07.2024 01:08:30	False		История
	Сигнал "Пуск газа"	29.07.2024 01:08:30	False		История
DATCHECK	**Температура** (7 элементов данных)				
	Температура двери	29.07.2024 01:08:30	0 °C		График
	Температура подогрева ресиврера К1	29.07.2024 01:08:30	28.639 °C	-0.2385 °C	График
	Температура подогрева ресиврера К2	29.07.2024 01:08:30	36.3509 °C	-0.6602 °C	График
	Температура подогрева ресиврера К3	29.07.2024 01:08:30	32.7947 °C	-0.1499 °C	График
	Температура подогрева ресиврера К4	29.07.2024 01:08:30	39.4385 °C	-0.6397 °C	График
	Температура тамбура	29.07.2024 01:08:30	20.707 °C	+0.4222 °C	График
	Уличная температура	29.07.2024 01:08:30	20.371 °C	-0.5509 °C	График



Интерфейс ITM



*ПАК для мониторинга и управления ЦОД

ITM – это:

Единое решение для мониторинга

- удалённых площадок и филиалов
- ИТ-инфраструктуры и инженерных систем

Сервер мониторинга на базе актуального Zabbix 7 LTS

Зонтичный мониторинг и бесшовная интеграция с существующими Zabbix-системами предприятия

Техническая поддержка от российского разработчика

Входит в Единый реестр отечественного ПО и БД

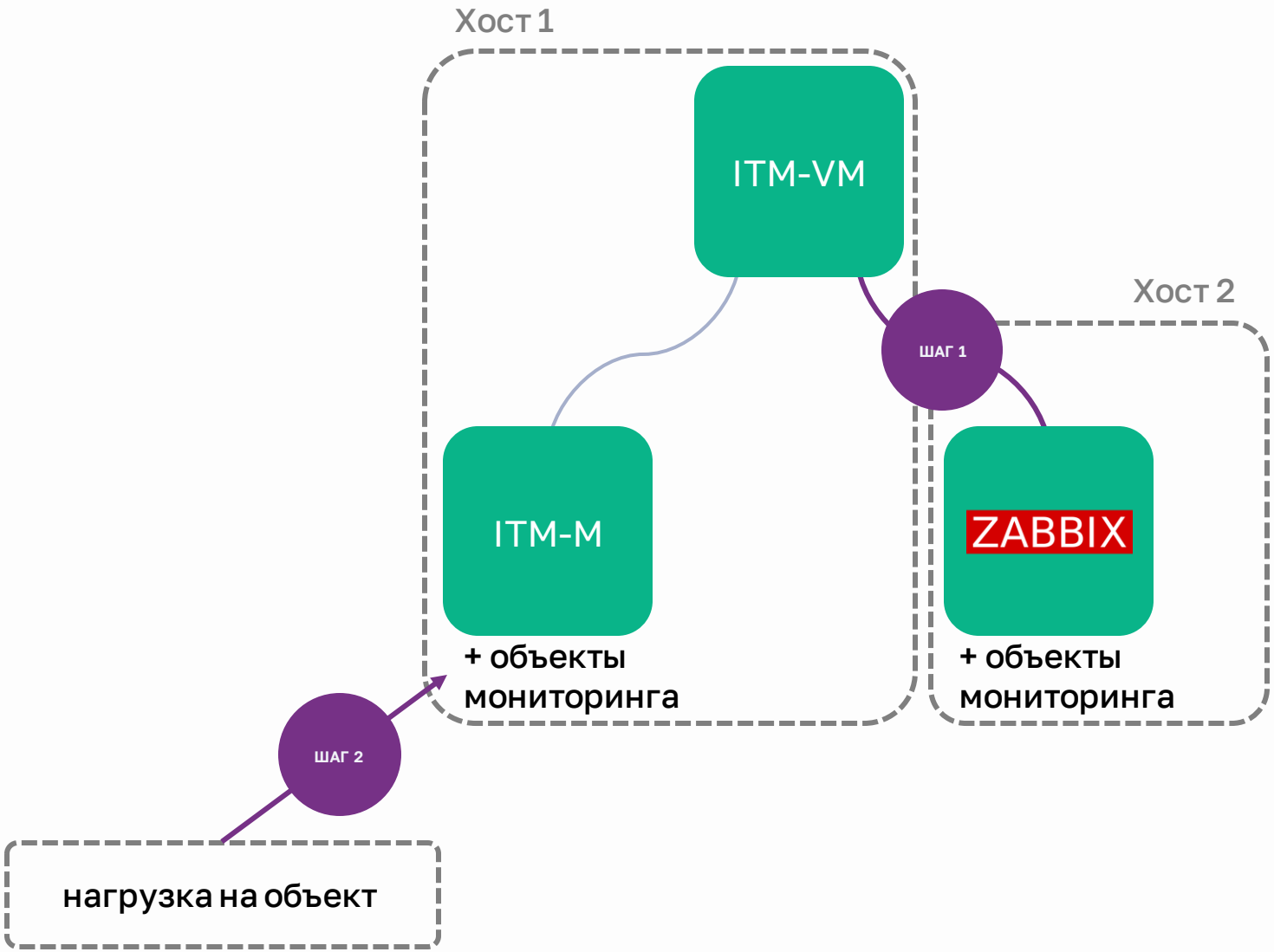
Безопасность, подтверждённая Сертификатом ФСТЭК России

Единое «окно здоровья» с набором необходимых виджетов из коробки

Пополняемая библиотека шаблонов мониторинга

Live demo

Сценарий демонстрации



ШАГ 1:

Подключим Zabbix к ITM-VM

ШАГ 2:

Дадим нагрузку
на подключенный объект
мониторинга

udv|group

Вопросы?

Контакты

commercial@udv.group
https://udv.group/