Комплексный ИТ-мониторинг с сертифицированным решением UDV ITM

Владислав Ганжа

Руководитель производственного направления

udv|group

softline

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

1500+
инсталляций

Проекты по защите АСУ ТП
и корпоративных сетей

10+
патентов

Собственный исследовательский
центр в области кибербезопасности

12
лет на рынке

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

udv|group

О чём поговорим?

- Зачем нужен мониторинг ИТ-инфраструктуры
- Как с помощью UDV ITM осуществляется сбор данных об инфраструктуре
- Особенности архитектуры решения
- Как с помощью решения выполнить требования регуляторов
- Live Demo продукта
- Дальнейшие планы по развитию UDV ITM
- Q&A

Зачем нужен мониторинг IT-инфраструктуры

IT-мониторинг – это комплексный процесс наблюдения за IT-инфраструктурой:

- серверы;
- сетевое оборудование;
- приложения;
- базы данных;
- сервисы и пр.

Задачи:

- оперативное выявление сбоев, снижение MTTR;
- выявление узких мест, планирование масштабирования;
- соответствие требованиям регулятора;
- снижение нагрузки на персонал

Зачем нужен мониторинг IT-инфраструктуры

1. Простой IT-инфраструктуры может стоить > $100 000

Что произошло: сентябрь 2023 – 14 заводов Toyota в Японии остановлены на трое суток [1, 2]

Причина: внутренний сбой (нехватка места на сервере БД)

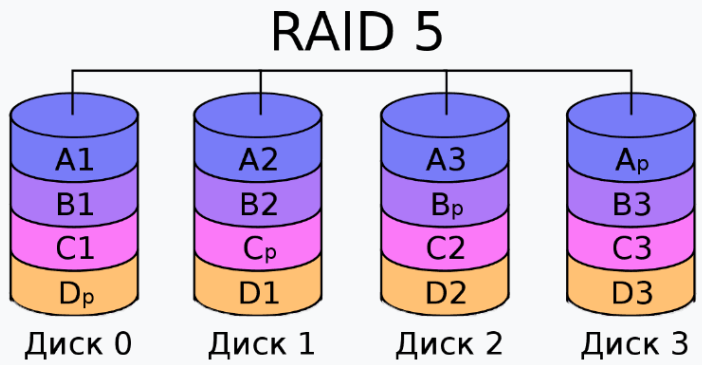
2. Мониторить нужно не только метрики ОС

Что произошло: сервер не загружается, сбой RAID-массива, предупреждающих уведомлений от системы мониторинга не было

В ходе расследования выяснилось:

- вышел из строя второй диск в RAID-массиве;
- первый диск вышел из строя еще 5 месяцев назад (события об этом были в журнале iBMC);
- не был настроен мониторинг iBMC, собираемые метрики ОС аппаратный сбой RAID не показали

В итоге: простой работы сервера на несколько дней, закуп и замена дисков, ручное восстановление ОС и прикладного ПО



Зачем нужен мониторинг IT-инфраструктуры

3. В МСБ размер инфраструктуры исчисляется **сотнями устройств**.

Эту инфраструктуру обслуживают 2-3 человека.

Без системы IT-мониторинга оперативно выявить сбои и принять корректирующие меры **выглядит фантастикой**.

4. В АСУ ТП организован детальный контроль параметров технологического процесса, однако IT-параметры (место на диске, нагрузка на ЦП, каналы связи) **не всегда отслеживаются**. Поэтому без IT-мониторинга высоки риски останова техпроцесса.

udvlgroup

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

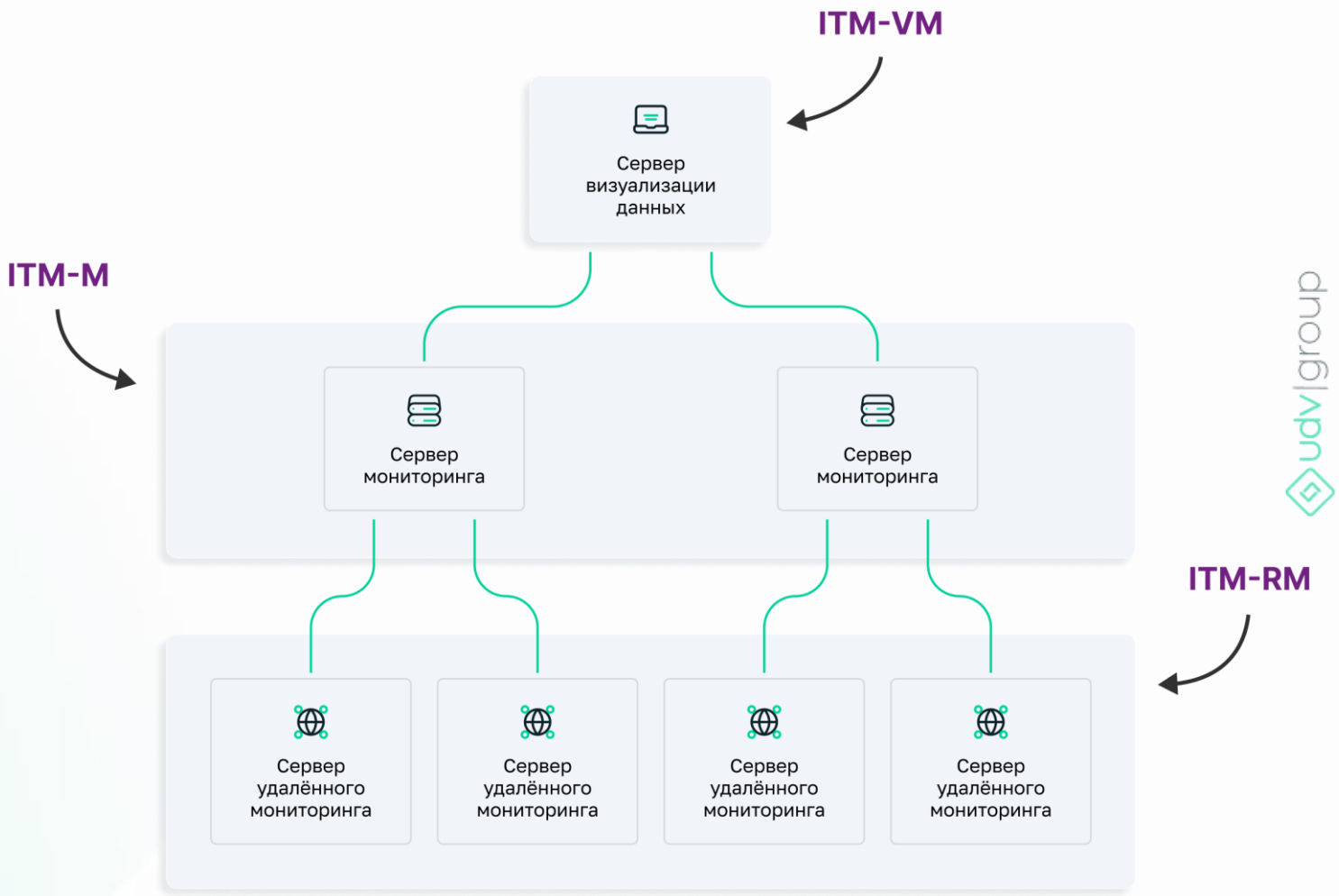
С другой стороны

- 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

Комплексная система мониторинга UDV ITM

Комплексное решение позволяет перейти на «безопасный Zabbix» и начать контролировать инфраструктуру предприятия из единой консоли: все филиалы и удалённые площадки в рамках «Единого окна».

- **Централизованная консолидация** данных с систем мониторинга в масштабах предприятия
- Бесшовная **интеграция с Zabbix-системами,** существующими на предприятии
- **Миграция данных с Zabbix-систем** на отечественные серверы мониторинга UDV ITM в рамках импортозамещения
- **Расширенная техническая поддержка** от российского разработчика: **разработка шаблонов мониторинга** под специфичное оборудование
- Доступ к **репозиторию шаблонов**



Какие задачи Заказчиков решает

ITM-VM

- Контроль сложной распределённой инфраструктуры
- Хаос из-за большого количества Zabbix-инсталляций
- Бизнес может нести денежные и репутационные риски из-за нестабильной ИТ-инфраструктуры
- Потребность в консолидации информации от нескольких систем мониторинга
- Есть необходимость в интеграции с SIEM-системами
- Сокращение MTTR (Mean Time To Repair) и рутинной нагрузки на инженеров

ITM-M

- Поддержка от вендора в РФ имеет значение
- Стоит задача импортозамещения Zabbix или необходимо выполнить требования регулятора
- Наличие специфичного оборудования, которое необходимо мониторить

ITM-RM

- Нестабильная связь с сервером ITM-M на удаленных площадках
- Снижение нагрузки на сервер ITM-M в больших инсталляциях

Сервер визуализации данных ITM-VM

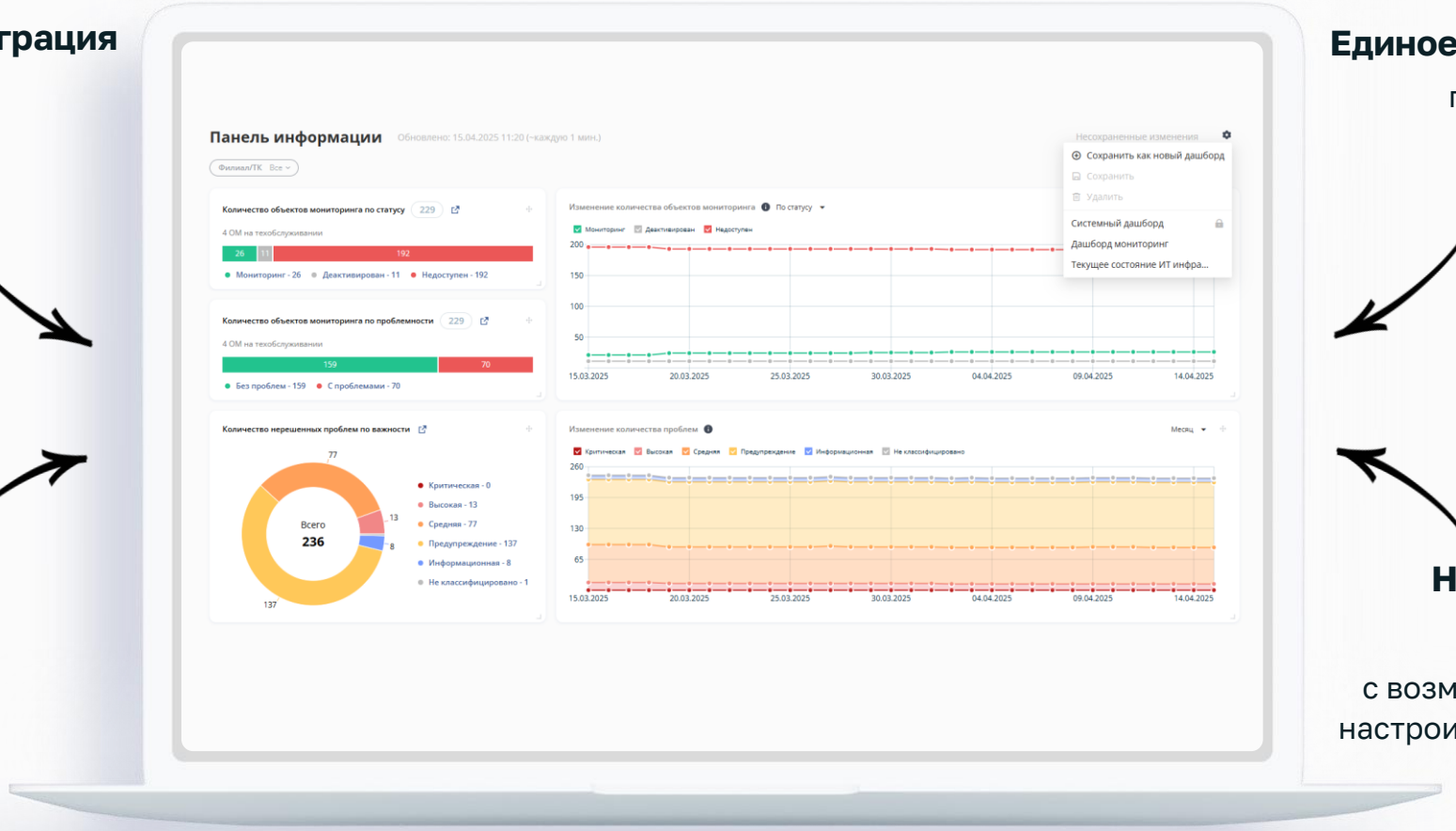
Благодаря удобному пользовательскому интерфейсу и виджетам «из коробки» позволяет контролировать инфраструктуру предприятия из единой консоли

Бесшовная интеграция

с существующими Zabbix-системами предприятия

Внедрение за один день

и инфраструктура всего предприятия под контролем



Единое окно здоровья

по всем филиалам распределённой инфраструктуры

Набор виджетов из коробки

с возможностью удобно настроить единую панель информации

udvgroup

Мониторинг инфраструктуры ITM-M

Безболезненное импортозамещение благодаря российской системе мониторинга на базе популярного решения Zabbix с безопасностью, подтверждённой ФСТЭК России

Как Zabbix,

Сервер мониторинга на базе актуального Zabbix 7

Миграция данных с существующих Zabbix-систем предприятия

Доступ к пополняемой библиотеке шаблонов мониторинга

только лучше:

Входит в Единый реестр российского ПО

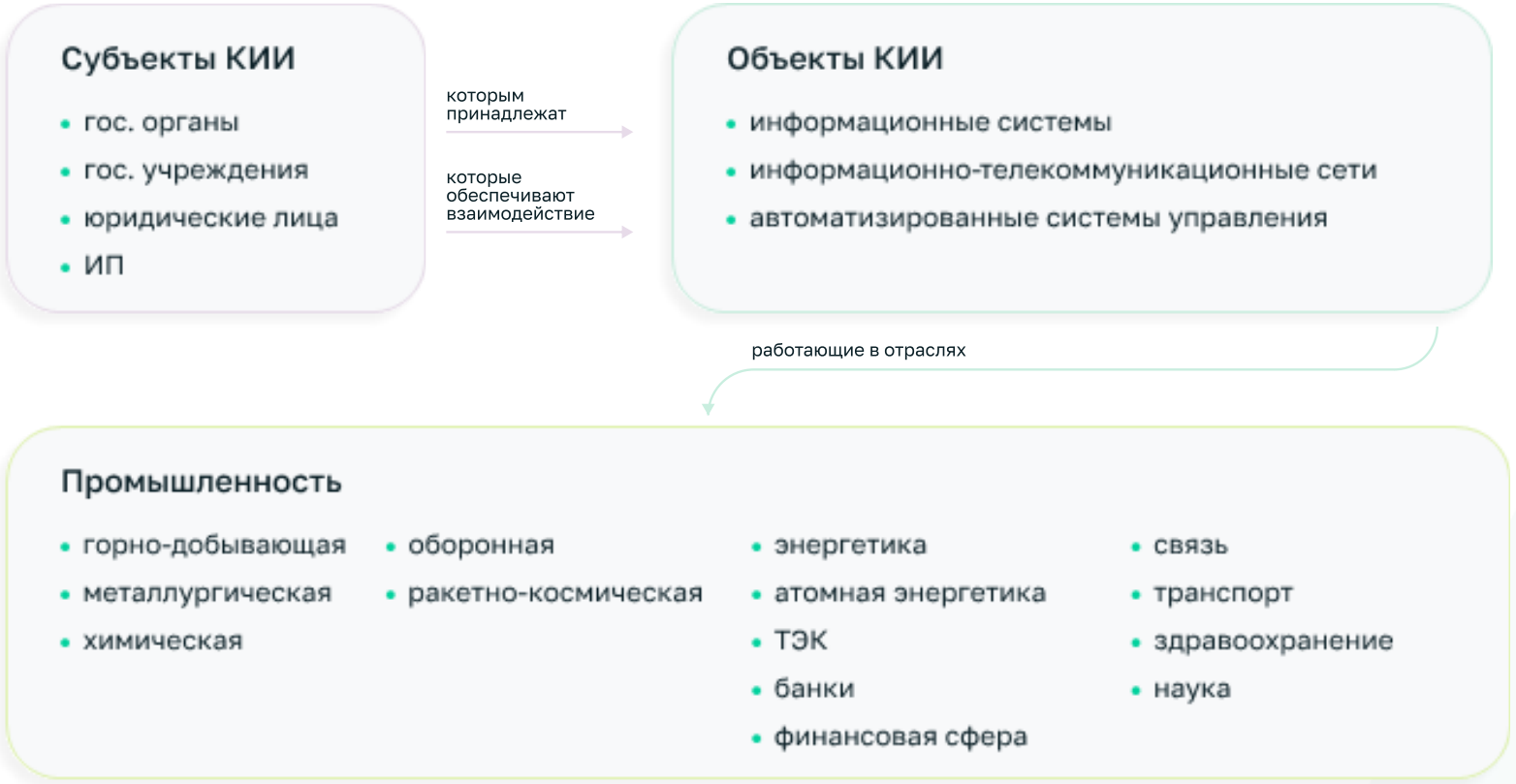
Устранены уязвимости Zabbix – подтверждено сертификатом ФСТЭК России №4432

Техническая поддержка от разработчика

Разработка шаблонов для российского оборудования

Драйверы рынка UDV ITM

- **Государственный сектор:** импортозамещение Zabbix
- Остальные **субъекты критической информационной инфраструктуры**



- **Другие секторы:** агрегация информации с нескольких Серверов мониторинга Zabbix на разных площадках или на разных подразделениях в Сервер визуализации и управления ITM-VM.

UDV ITM 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

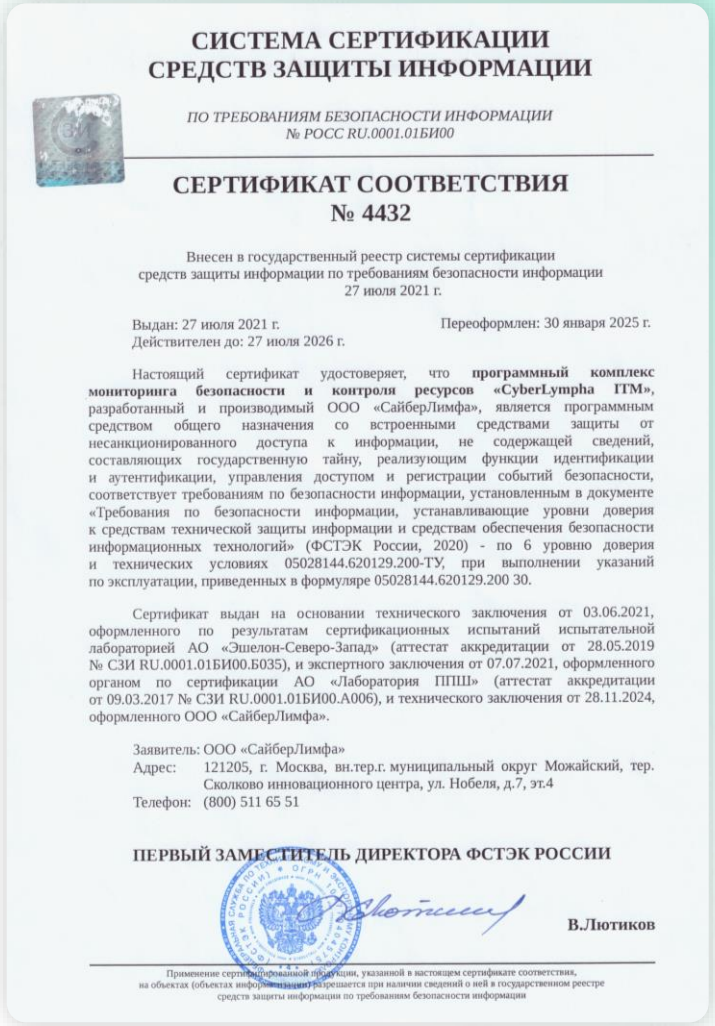
ГИС (пр. № 17) и **ИСПДн** (пр. № 21):

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

АН3.4: Контроль состава технических средств, программного обеспечения и средств защиты информации

Безопасный инструмент для мониторинга инфраструктуры на базе знакомого решения – не требуется переобучать сотрудников



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 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

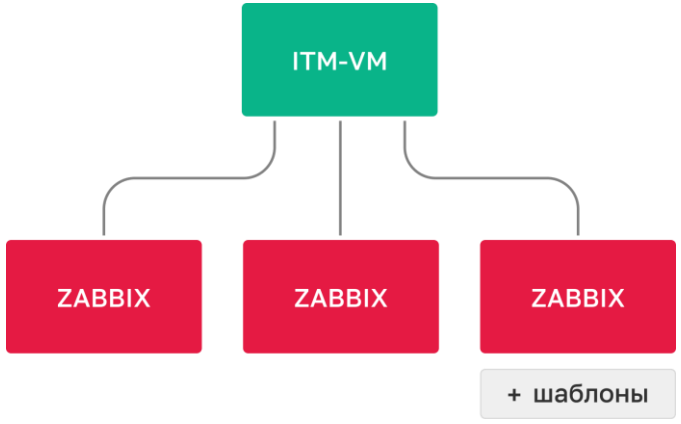
Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

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

Этапы внедрения комплексного решения в инфраструктуре с Zabbix

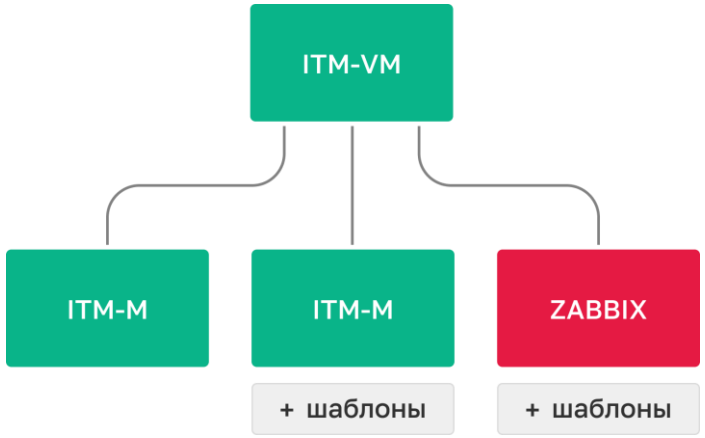
I этап. Только консолидация

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



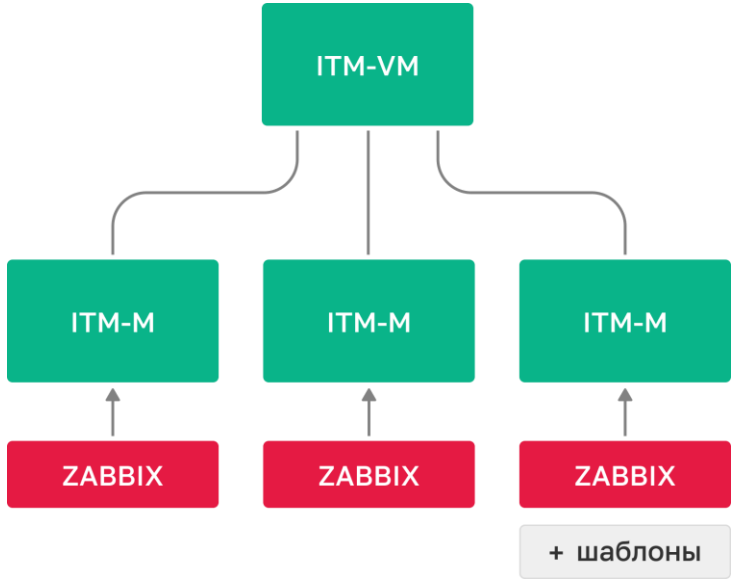
II этап. Смешанный

- 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

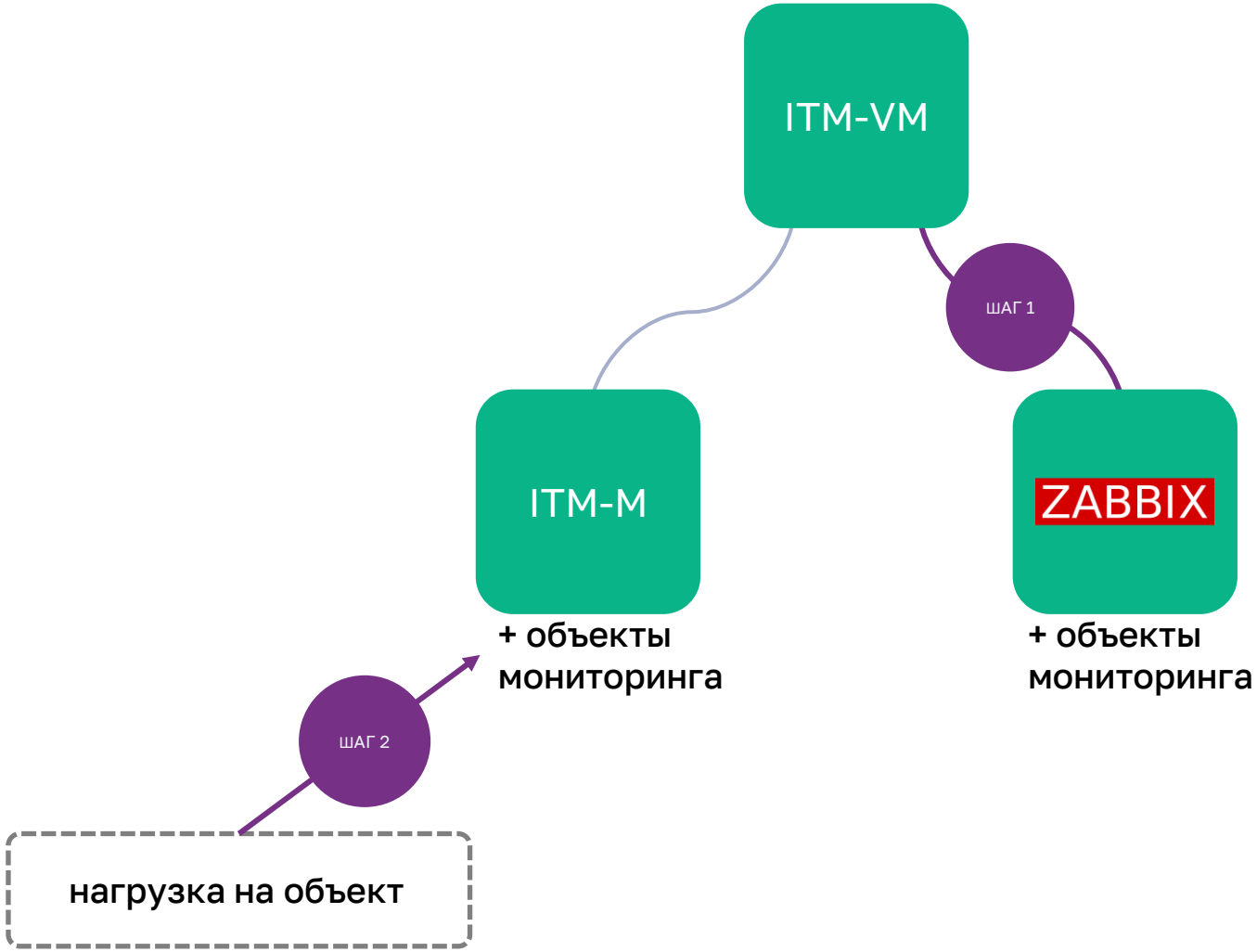


III этап. Безопасный мониторинг на базе сертифицированного ФСТЭК решения

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



Сценарий демонстрации



ШАГ 1:

Подключим Zabbix к ITM-VM

ШАГ 2:

Дадим нагрузку
на подключенный объект
мониторинга

Кейс внедрения: ГБУ СО «Оператор электронного правительства»

Профиль заказчика

Оператор электронного правительства
Государственное бюджетное учреждение Свердловской области

Основная цель деятельности учреждения — обеспечение функционирования межведомственных элементов инфраструктуры электронного правительства в Свердловской области

Кейс внедрения: ГБУ СО «Оператор электронного правительства»

Цели и особенности проекта

Критерии выбора решения:

- продукт в Едином реестре российских программ для ЭВМ и БД;
- действующий сертификат ФСТЭК России
- бесшовная миграция с Zabbix;
- техническая поддержка от российского разработчика;
- невысокая стоимость

Дальнейшие планы

- Переоформление сертификата ФСТЭК России, добавление поддержки ОС Альт СП в качестве дополнительной серверной ОС
- Переход на Zabbix 7.4 и впоследствии на 8.0
- Расширение возможностей интеграции с мессенджерами и сторонними системами
- Сценарии оркестрации (автоматизация установки агентов ITM, сбор дополнительных данных для администратора в случае появления проблемы, интеграция с тикет-системами по API и пр.)
- Улучшение пользовательского опыта, добавление гео-карты
- Построение отчетов по запросам, сформированным на естественном языке, с применением LLM
- Шаблоны для мониторинга нового оборудования (Серверы, сетевое оборудование, ОС, прикладное ПО, ПЛК и пр.)

udv|group

Спасибо!

Закажите пилотный проект или персональную демонстрацию наших решений

Контакты

Email

Анастасия Зырянова,
пресейл-менеджер по сетевой безопасности «Софтлайн Решения»

Anastasiya.Zyryanova@softline.com