Менеджмент конфигураций и оценка уязвимостей сетевых устройств, виртуальных сред и операционных систем в гетерогенной ИТ-инфраструктуре.

EFROS
Config Inspector

Дмитрий Успехов
Ведущий менеджер
ООО «Газинформсервис»

СОВРЕМЕННЫЕ ВЫЗОВЫ ДЛЯ БИЗНЕСА

НОВЫЕ НАПРАВЛЕНИЯ

ОПТИМИЗАЦИЯ

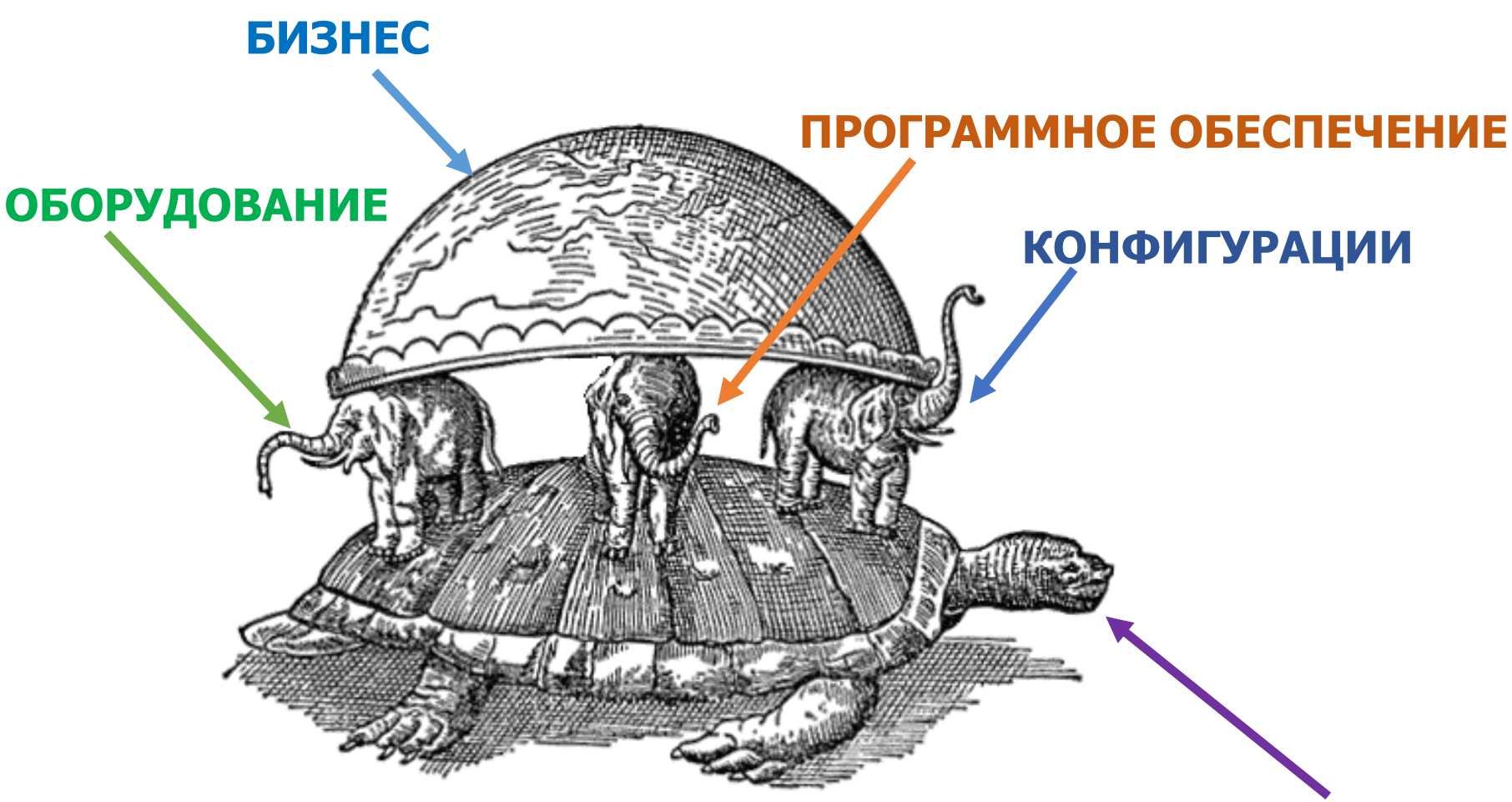
ЭКСПАНСИЯ

АУТСОРСИНГ

РЕСТРУКТУРИЗАЦИЯ

ПОЛИТИКА

БИЗНЕС-ОРИЕНТИРОВАННАЯ ИТ-ИНФРАСТРУКТУРА



ЗАДАЧИ РУКОВОДСТВА

Качество и безопасность бизнес-процессов в сфере ИТ

Повышение устойчивости бизнес-процессов, опирающихся на ИТ-инфраструктуру предприятия

Оптимизация кадрового состава

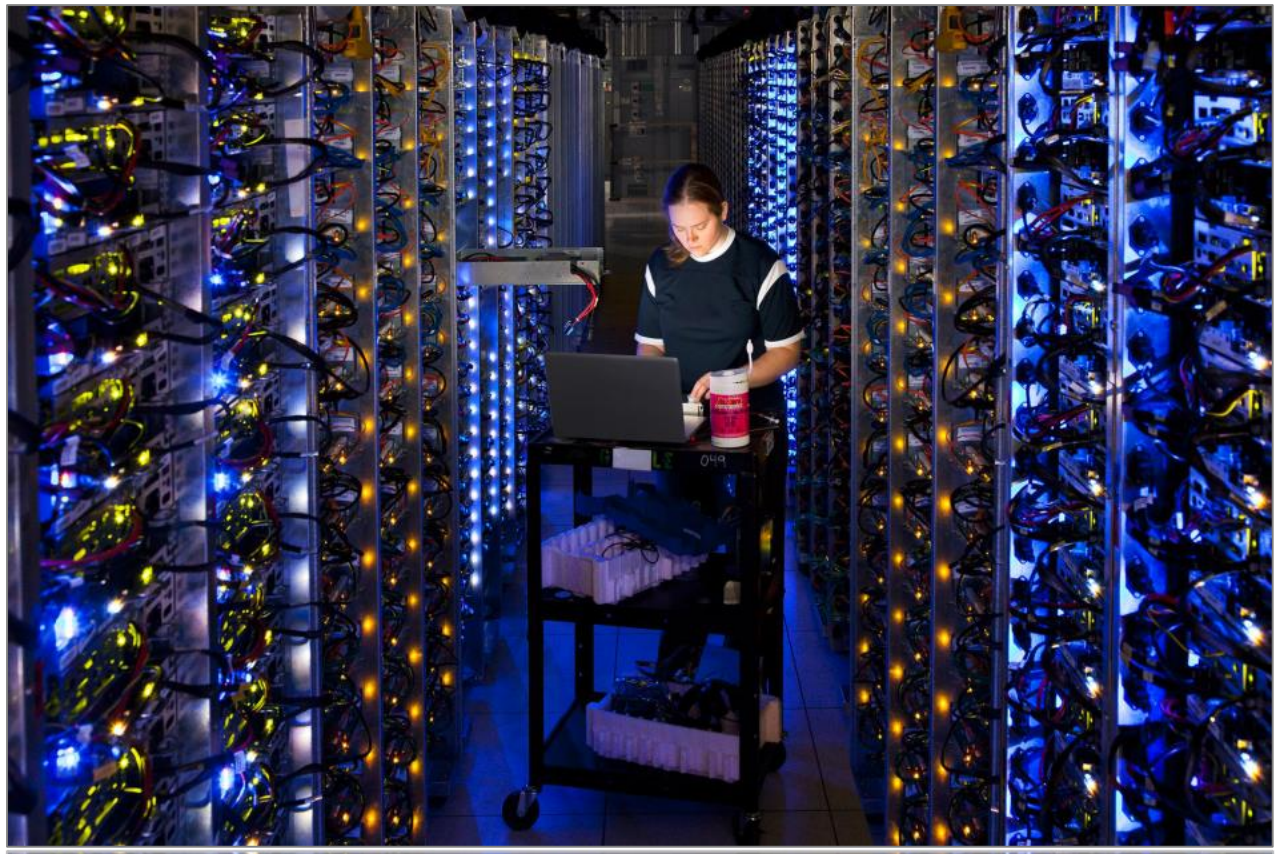
ЗАДАЧИ ОТДЕЛА ИБ

Контроль изменения конфигурационной информации

Контроль соответствия проводимых изменений политике безопасности предприятия

Контроль текущих конфигураций на наличие уязвимостей

ЗАДАЧИ ОТДЕЛА ИТ



Оперативная диагностика и восстановление после сбоев

Автоматизированное ведение базы данных конфигураций

Контроль проведения запланированных изменений

ГЕТЕРОГЕННАЯ ИТ-ИНФРАСТРУКТУРА

Сетевое оборудование

Виртуальные среды

Операционные системы

РЕШЕНИЕ

Network configuration and **change management** (**NCCM**)

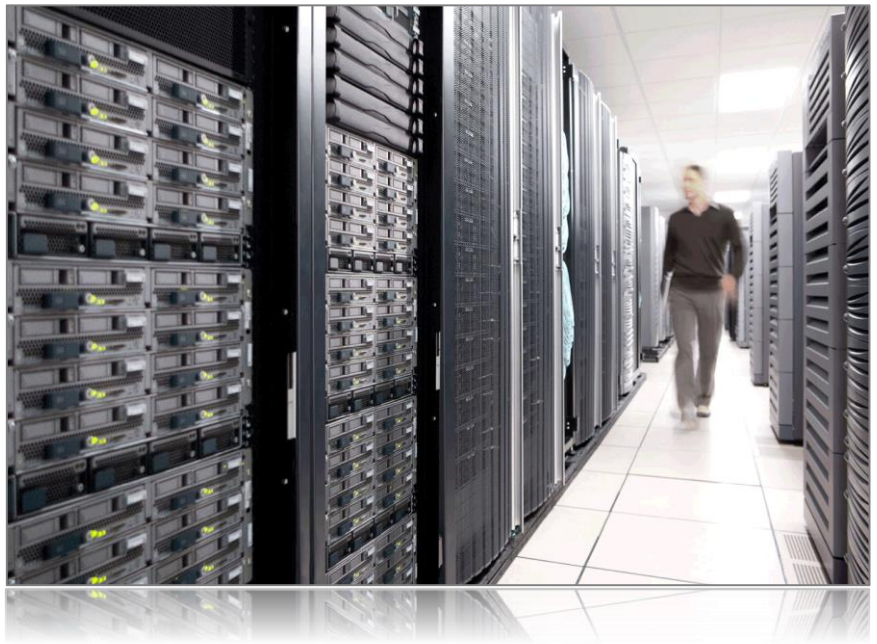
&

Vulnerability Assessment (VA)

РЕШАЕМЫЕ ЗАДАЧИ

ОТДЕЛ ИБ	ОТДЕЛ ИТ
Обнаружение уязвимостей ИТ-инфраструктуры	Инвентаризация объектов ИТ-инфраструктуры
Проверки соответствия отраслевым стандартам и аудит	Устранение уязвимостей объектов ИТ-инфраструктуры
Контроль целостности файлов серверных и десктопных операционных систем	Контроль обновлений, служб, пользователей серверных операционных систем
Контроль проведения запланированных изменений	
Контроль конфигураций сред виртуализации	
Контроль конфигураций и состояния рабочей среды сетевого оборудования	

СЕТЕВОЕ ОБОРУДОВАНИЕ И ИНВЕНТАРИЗАЦИЯ



- Контроль изменений конфигураций
- Анализ syslog сообщений
- Мультивендорная поддержка

- Поиск устройств сканером сети
- Автоматическое построение карты
- Работа с базой данных (CMDB)

УЯЗВИМОСТИ И ПРОВЕРКИ СООТВЕТСТВИЯ

- Обнаружение уязвимостей ПО и оборудования
- Рекомендации по устранению
- Обновление базы уязвимостей данными от вендоров и репозиторием OVAL

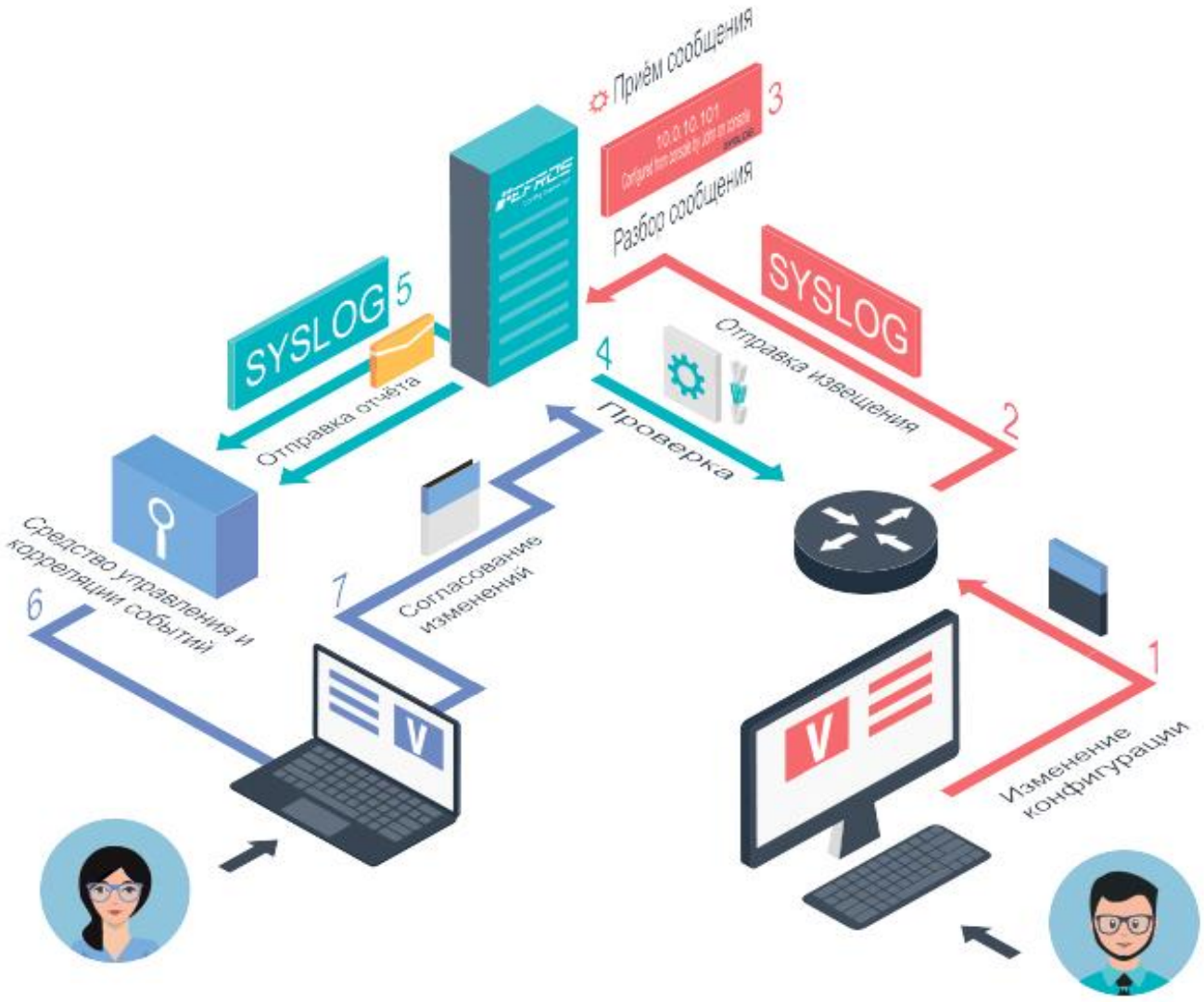
- Аудит безопасности объектов ИТ-инфраструктуры позволит оценить степень их защищенности

СЕРВЕРА И АРМ СОТРУДНИКОВ

- Контроль конфигураций платформ виртуализации
- Контроль дисковых хранилищ

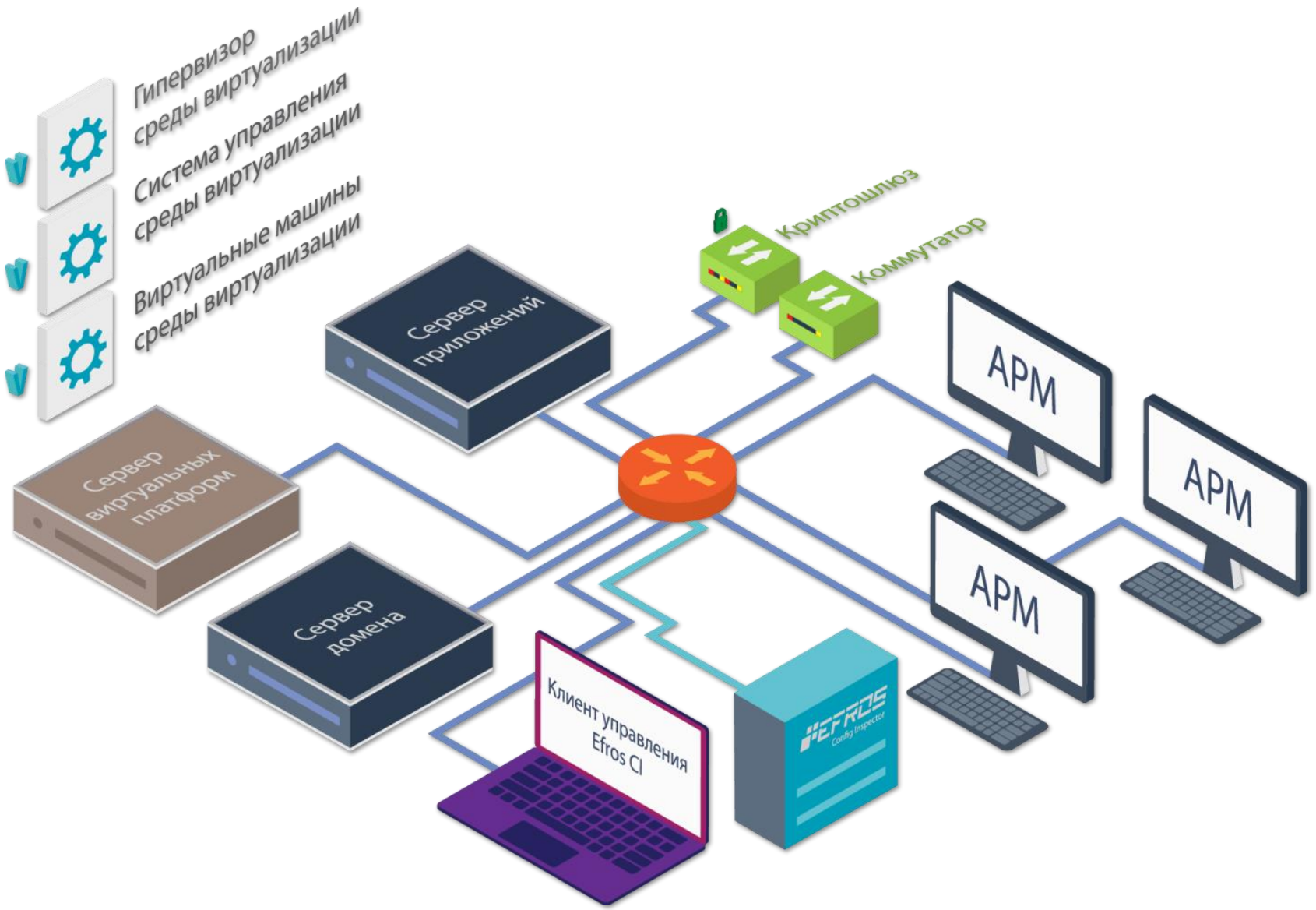
- Контроль изменений в Active Directory: службы, пользователи
- Контроль целостности локальных файлов
- Контроль обновлений, служб

СХЕМА РАБОТЫ

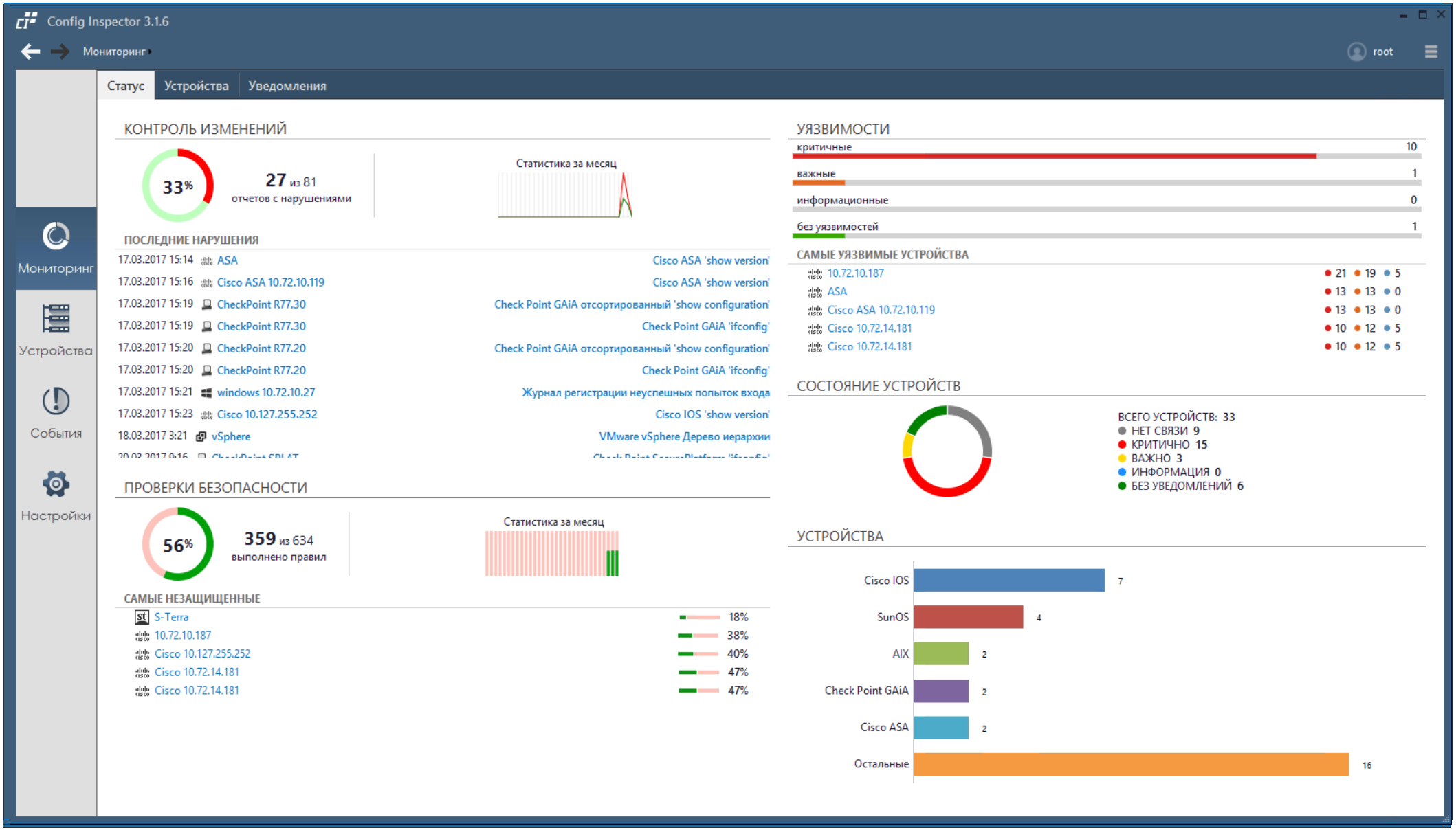


- Efros CI запускает проверки по расписанию, проводя полный анализ на соответствие заданным параметрам
- Efros CI принимает и анализирует syslog сообщения от устройств и по результатам анализа запускает проверку

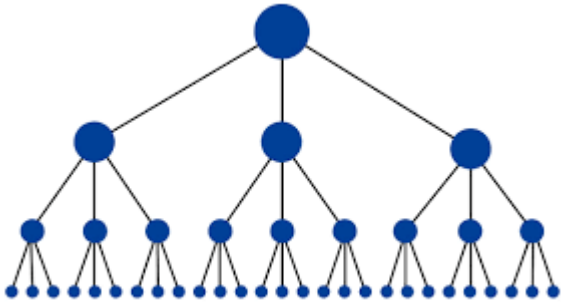
ТИПОВАЯ СХЕМА ПОДКЛЮЧЕНИЯ



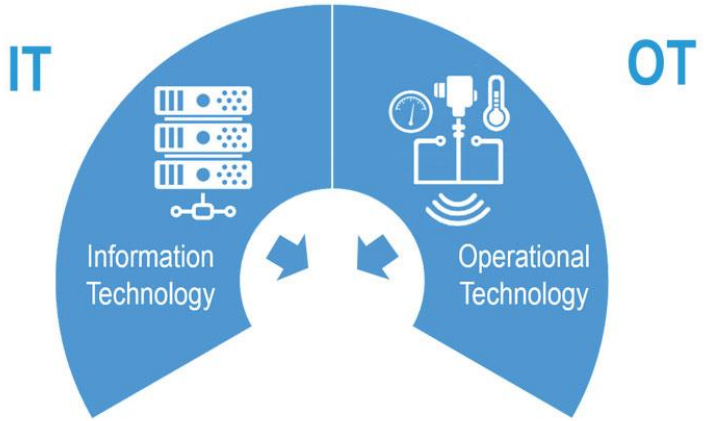
ИНТЕРФЕЙС


Config Inspector 3.1.6
Мониторинг
root
Статус
Устройства
Уведомления
Мониторинг
Устройства
События
Настройки
КОНТРОЛЬ ИЗМЕНЕНИЙ
33%
27 из 81
отчетов с нарушениями
Статистика за месяц
ПОСЛЕДНИЕ НАРУШЕНИЯ
17.03.2017 15:14 ASA Cisco ASA 'show version'
17.03.2017 15:16 Cisco ASA 10.72.10.119 Cisco ASA 'show version'
17.03.2017 15:19 CheckPoint R77.30 Check Point GAiA отсортированный 'show configuration'
17.03.2017 15:19 CheckPoint R77.30 Check Point GAiA 'ifconfig'
17.03.2017 15:20 CheckPoint R77.20 Check Point GAiA отсортированный 'show configuration'
17.03.2017 15:20 CheckPoint R77.20 Check Point GAiA 'ifconfig'
17.03.2017 15:21 windows 10.72.10.27 Журнал регистрации неуспешных попыток входа
17.03.2017 15:23 Cisco 10.127.255.252 Cisco IOS 'show version'
18.03.2017 3:21 vSphere VMware vSphere Дерево иерархии
ПРОВЕРКИ БЕЗОПАСНОСТИ
56%
359 из 634
выполнено правил
Статистика за месяц
САМЫЕ НЕЗАЩИЩЕННЫЕ
S-Terra 18%
10.72.10.187 38%
Cisco 10.127.255.252 40%
Cisco 10.72.14.181 47%
Cisco 10.72.14.181 47%
УЯЗВИМОСТИ
критичные 10
важные 1
информационные 0
без уязвимостей 1
САМЫЕ УЯЗВИМЫЕ УСТРОЙСТВА
10.72.10.187 21 19 5
ASA 13 13 0
Cisco ASA 10.72.10.119 13 13 0
Cisco 10.72.14.181 10 12 5
Cisco 10.72.14.181 10 12 5
СОСТОЯНИЕ УСТРОЙСТВ
ВСЕГО УСТРОЙСТВ: 33
НЕТ СВЯЗИ 9
КРИТИЧНО 15
ВАЖНО 3
ИНФОРМАЦИЯ 0
БЕЗ УВЕДОМЛЕНИЙ 6
УСТРОЙСТВА
Cisco IOS 7
SunOS 4
AIX 2
Check Point GAiA 2
Cisco ASA 2
Остальные 16

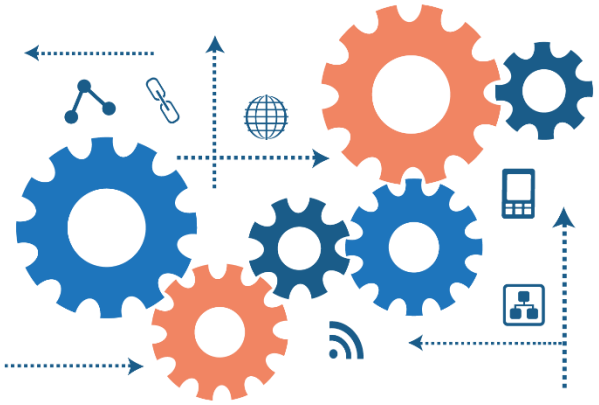
РАЗВИТИЕ ПРОДУКТА



РАЗВИТИЕ ИЕРАРХИЧНОЙ АРХИТЕКТУРЫ ПРОДУКТА



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АСУ ТП



ИНТЕГРАЦИЯ С СИСТЕМАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРЕИМУЩЕСТВА

1. Современные технологии, низкая стоимость владения
2. Широкие функциональные возможности, поддержка большого числа вендоров
3. Соответствие требованиям Оперативно-Аналитического центра
4. Оперативные доработки функциональных возможностей по запросам
5. Оперативная техническая поддержка

Требования Оперативно-Аналитического центра

Приказ №64 от 11 октября 2017 г.

№ п/п	Перечень требований к системе защиты информации, подлежащих включению в частное техническое задание или задание по безопасности на информационную систему
1.1	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
1.2	Обеспечение сбора, записи и хранения информации о событиях безопасности в течение установленного срока хранения, но не менее шести месяцев
1.3	Осуществление мониторинга (просмотра, анализа) событий безопасности уполномоченными субъектами информационной системы
1.4	Обеспечение мониторинга (просмотра, анализа) информации о сбоях в механизмах сбора информации и о достижении предела объема (емкости) памяти устройств хранения уполномоченными пользователями
3.1	Обеспечение идентификации объектов и закрепления за ними субъектов информационной системы
3.2	Обеспечение идентификации и аутентификации субъектов информационной системы
4.1	Обеспечение изменения атрибутов безопасности, установленных по умолчанию в соответствии с политикой информационной безопасности организации

Требования Оперативно-Аналитического центра

Приказ №64 от 11 октября 2017 г.

№ п/п	Перечень требований к системе защиты информации, подлежащих включению в частное техническое задание или задание по безопасности на информационную систему
4.3	Обеспечение защиты информации о событиях безопасности
4.4	Обеспечение контроля за установкой обновлений программного обеспечения средств защиты информации
6.2	Обеспечение идентификации и аутентификации субъектов информационной системы и объектов в виртуальной инфраструктуре
6.3	Обеспечение регистрации событий безопасности в виртуальной инфраструктуре
7.1	Наличие схемы информационной системы с указанием объектов, внешних подключений и информационных потоков
7.8	Обеспечение контроля за установкой обновлений программного обеспечения
7.9	Обеспечение контроля за работоспособностью, параметрами настройки и правильностью функционирования средств защиты информации

Efros Config Inspector

ПК Efros Config Inspector успешно прошел процедуру сертификации в РБ. 20.01.2018 г выдан сертификат соответствия, срок действия 5 лет.

Согласно серии стандартов ISO 27000, 27001 настоятельно рекомендуется вести контроль конфигураций

EFROS Config Inspector

Enterprise partner

Технологический партнер

INFOWATCH МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

GIS ГАЗИНФОРМСЕРВИС

WWW.CHECKER.GAZ-IS.RU

FSTEC Vulnerability checker

Тип продукта

Cisco ACS

Версия

5.8.0.9

Пример: 5.8.0.32

Проверить

7.5 Vulnerability in Java Deserialization Affecting Cisco Products

A vulnerability in the Java deserialization used by the Apache Commons Collections (ACC) library could allow an unauthenticated, remote attacker to execute arbitrary code.

cve CVE-2015-6420
cisco cisco-sa-20151209-java-deserialization

AV:N/AC:L/Au:N/C:P/I:P/A:P

4.3 Cisco Secure Acess Control System XML External Entitiy Vulnerability

A vulnerability in the web-based user interface of the Cisco Secure Access Control System (ACS) could allow an authenticated, remote attacker to have read access to part of the information stored in the affected system.

cve CVE-2017-3839
cisco cisco-sa-20170215-acs1

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

4.3 VMware ESXi, vCenter Server Appliance, Workstation and Fusion updates address multiple security vulnerabilities. ESXi Host Client stored cross-site scripting vulnerability

VMware ESXi, Workstation and Fusion updates address multiple security vulnerabilities The ESXi Host Client in VMware ESXi (6.5 before ESXi650-201712103-SG, 5.5 before ESXi600-201711103-SG and 5.5 before ESXi550-201709102-SG) contains a vulnerability that may allow for stored cross-site scripting (XSS). An attacker can exploit this vulnerability by injecting Javascript, which might get executed when other users access the Host Client.

cve CVE-2017-4940
vmware VMSA-2017-0021

AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS:3.0/CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

4.3 VMware product updates address multiple security issues. HTTP Header injection issue in vCenter Server and ESXi

VMware product updates address a DLL hijacking issue in Windows-based VMware Tools and an HTTP Header injection issue in vCenter Server and ESXi. CRLF injection vulnerability in VMware vCenter Server 6.0 before U2 and ESXi 6.0 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via unspecified vectors.

fstec 2017-02200
cve CVE-2016-5331
vmware VMSA-2016-0010.1

ДЕЙСТВУЙТЕ

1. Скачать демо-версию и попробовать все возможности ПК в течении 90 дней.
2. Получить информацию по оптимальному использованию ПК.
3. Оформить запрос на проведение пилотного решения.
4. Запросить коммерческое предложение.

СПАСИБО ЗА ВНИМАНИЕ

Ознакомьтесь с дополнительными материалами
и получите демо-версию на сайте www.gaz-is.ru

Дмитрий Успехов
Ведущий менеджер
ООО «Газинформсервис»
Uspehov-D@gaz-is.ru
+7 (911) 931-43-50