



КОД  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ

# КАК КОНТРОЛИРОВАТЬ СЕТЕВУЮ ИНФРАСТРУКТУРУ И ВЫПОЛНЯТЬ ТРЕБОВАНИЯ КИИ

Штубов Никита  
Газинформсервис

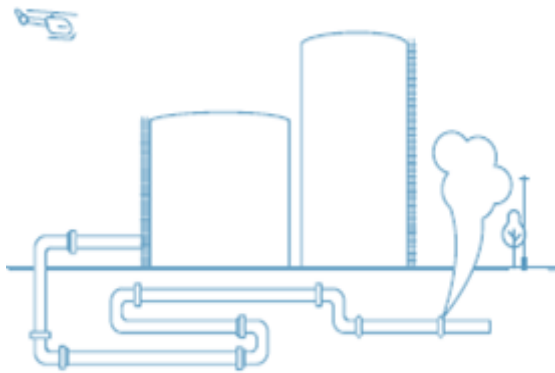
# Почему так важно защищать КИИ

↓  Взрыв сибирского нефтепровода был спровоцирован ЦРУ

↓  Слив миллиона литров сточных вод в реку

↓  Атака сократила добычу нефти с 3 млн. до 370 тыс. баррелей в сутки

↓  Кибер-атака оставила без электроэнергии свыше 600 000 жителей Украины



1982

2000

2002

2015

Нефтепровод (СССР)


Maroochy Water System (Австралия)

PDVSA (Венесуэла)

Украина

## Соотношение требований 239 приказа с другими приказами ФСТЭК России



<b>V. Аудит безопасности (АУД)</b>				
		КЗ 3	КЗ 2	КЗ 1
АУД.1	Инвентаризация информационных ресурсов	+	+	+
АУД.2	Анализ уязвимостей и их устранение	+	+	+
АУД.4	Регистрация событий безопасности	+	+	+
АУД.6	Защита информации о событиях безопасности	+	+	+
АУД.7	Мониторинг безопасности	+	+	+
<b>IX. Обеспечение доступности (ОДТ)</b>				
ОДТ.3	Контроль безотказного функционирования средств и систем		+	+
<b>XII. Реагирование на компьютерные инциденты (ИНЦ)</b>				
ИНЦ.1	Выявление компьютерных инцидентов	+	+	+
ИНЦ.2	Информирование о компьютерных инцидентах	+	+	+
ИНЦ.4	Устранение последствий компьютерных инцидентов	+	+	+
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	+	+	+

  - Требования появившиеся лишь в 239 приказе

XIII. Управление конфигурацией (УКФ)				
		КЗ 3	КЗ 2	КЗ 1
УКФ.2	Управление изменениями	+	+	+
XVI. Обеспечение действий в нештатных ситуациях (ДНС)				
ДНС.3	Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций		+	+
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	+	+	+



Проверка соответствия  
отраслевым стандартам и  
аудит



Обнаружение и устранение  
уязвимостей



Контроль конфигураций  
 сетевого оборудования



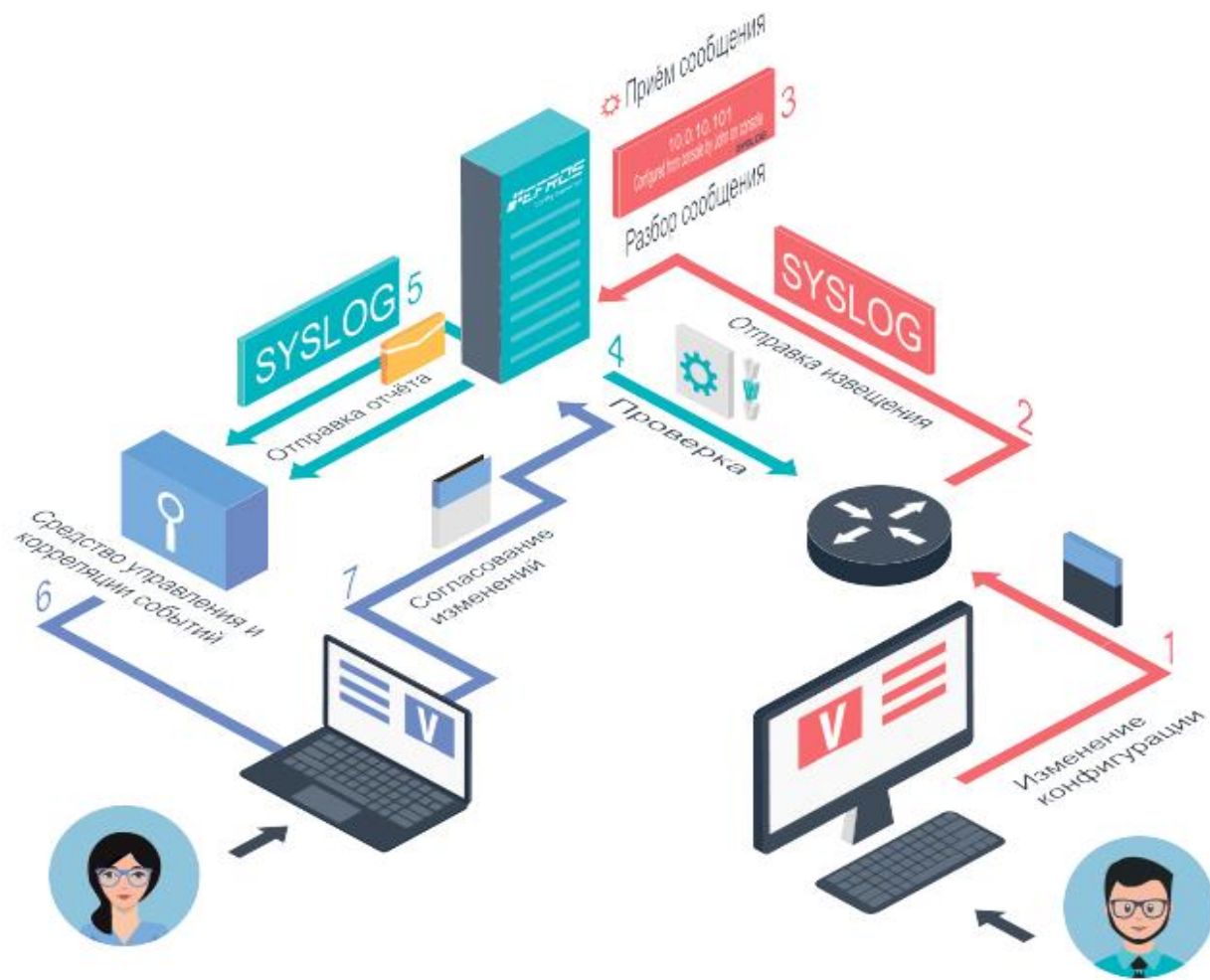
Контроль конфигураций сред  
виртуализации



Контроль целостности  
файлов ОС



# СХЕМА РАБОТЫ



Efos CI запускает проверки по расписанию, проводя полный анализ на соответствие заданным параметрам.

Efos CI принимает и анализирует syslog сообщения от устройств и по результатам анализа запускает проверку.

Для крупных объектов (более 500 сетевых устройств, серверов и т.п.) используются коллекторы – службы балансировки нагрузки и иерархия серверов.

## ЗАДАЧИ РУКОВОДСТВА



Снижение стоимости процессов эксплуатации и обеспечения информационной безопасности ИТ-инфраструктуры предприятия

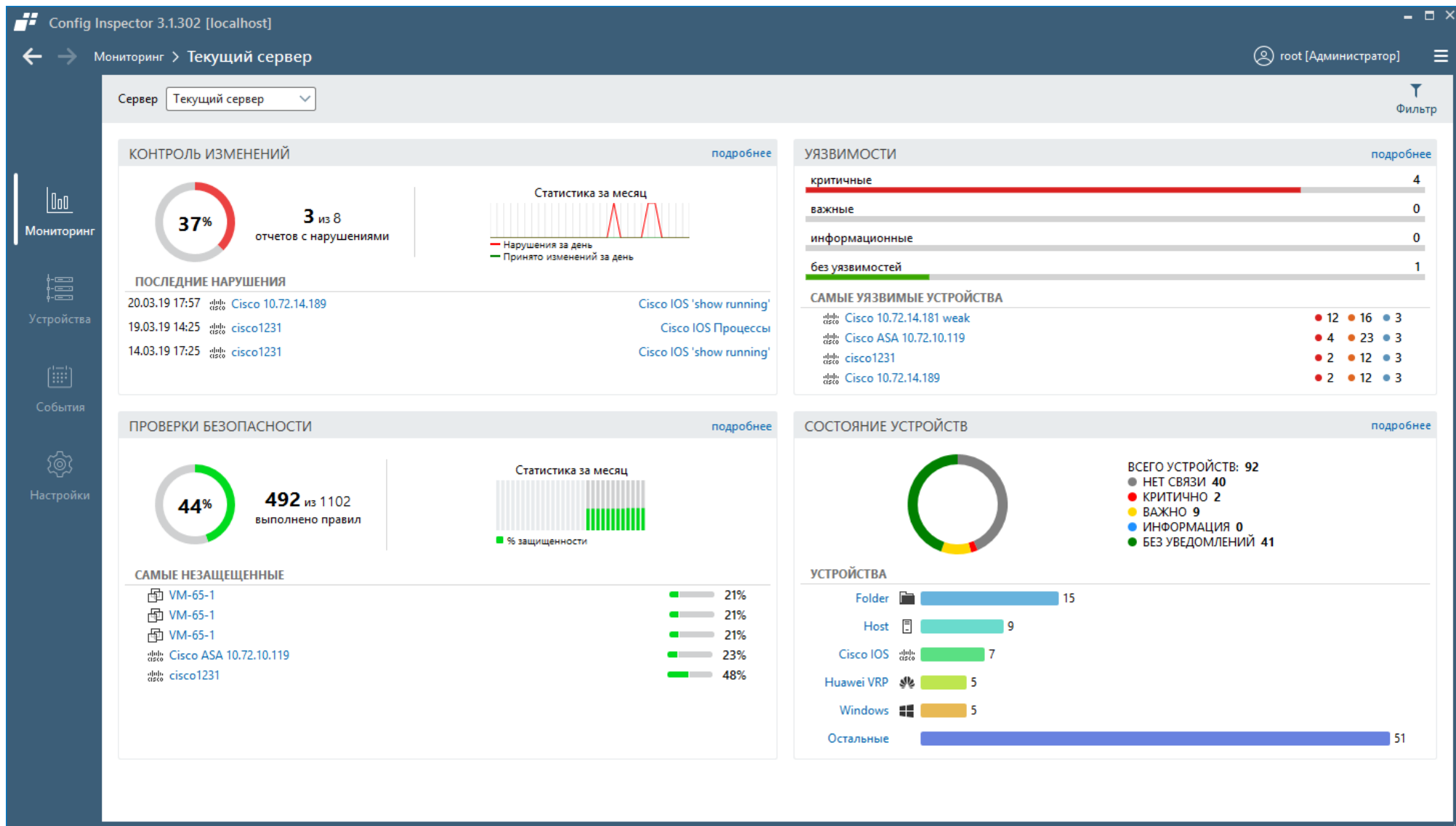


Повышение устойчивости бизнес-процессов, опирающихся на ИТ-инфраструктуру предприятия



Оптимизация кадрового состава компании





## ЗАДАЧИ ИБ



Предотвращение несанкционированного изменения конфигурационной информации



Контроль соответствия проводимых изменений политике безопасности предприятия



Контроль текущих конфигураций на наличие уязвимостей



Организация ролевой модели доступа

Config Inspector 3.1.302 [localhost]

← → Мониторинг > Текущий сервер

root [Администратор]

Фильтр

## УСТРОЙСТВА

### СОСТОЯНИЯ УСТРОЙСТВ

ВЕСЕГО УСТРОЙСТВ: 92

- НЕТ СВЯЗИ 40
- КРИТИЧНО 2
- ВАЖНО 9
- ИНФОРМАЦИЯ 0
- БЕЗ УВЕДОМЛЕНИЙ 41

### СТАТИСТИКА ЗА МЕСЯЦ

### КОЛИЧЕСТВО УСТРОЙСТВ В СИСТЕМЕ

Тип устройства	Количество
Folder	15
Host	9
Cisco IOS	7
Huawei VRP	5
Windows	5
Cisco UCM 8.5	4

### Список устройств

Устройство	Состояние
Cisco ASA 10.72.10.119	● Нет связи
Cisco 10.127.255.251	● Нет связи
CUCM	● Нет связи
10.72.10.173	● Нет связи
Cisco SMB 302 ENABLE	● Нет связи
10.72.14.184	● Нет связи
Cisco SMB 302	● Нет связи
Eltex	● Нет связи
Check Point SmartCenter	● Нет связи
Solaris 10.10.8.12	● Нет связи
Cisco 10.72.14.180	● Нет связи
Cisco 10.127.255.252	● Нет связи
CheckPoint R77.30	● Нет связи
CheckPoint SPLAT	● Нет связи
HP 10.127.255.249	● Нет связи
CUCM 1111	● Нет связи
Solaris 10.10.8.6	● Нет связи
10.72.11.161	● Нет связи
debian	● Нет связи
CUCM 11.5	● Нет связи
CUCM 11	● Нет связи
Nateks	● Нет связи
sterra	● Нет связи
askdjhasfg	● Нет связи
AIX AIX 10.10.1.136	● Нет связи
Solaris 10.10.8.5	● Нет связи
Suse 10.72.10.132	● Нет связи
PKCC	● Нет связи
Check Point SmartCenter 10.72.10.240	● Нет связи

Config Inspector 3.1.302 [localhost] root [Администратор]

← → Устройства > Сервер > cisco1231

Поиск устройств

- Hosts
  - VSAN-Cluster
    - 10.10.65.60
    - 10.10.65.61
    - 10.10.65.62
  - Virtual Machines
    - Discovered virtual mact
- Ядро сети
  - Cisco 10.127.255.251
  - Cisco 10.127.255.252
- 234
- asd
  - askdjhasfg
  - cisco1231**
  - Huawei
- 10.72.10.27
  - 234
  - asd
    - Test
      - Datacenter
      - Virtual Machines
        - Discovered virtual machine
          - VM-65-1
      - askdjhasfg
      - cisco1231
      - Huawei

Статус | Отчеты | События | Архив

**Безопасность**

- Проверка политик CIS для Cisco IOS пройдено 48%  
14.03.19 17:25
- Уязвимости Cisco IOS 2 12 3  
14.03.19 17:26

Уведомления: 3

- Нарушение целостности** ✓  
14.03.19 17:25  
Cisco IOS 'show running'
- Рабочая и загрузочная конфигурации не синхронизированы**  
14.03.19 17:12  
Рабочая и загрузочная конфигурации не синхронизированы
- Нарушение целостности** ✓  
19.03.19 14:25  
Cisco IOS Процессы

**Описание**

- имя: cisco1231
- тип: Cisco IOS
- профиль: По умолчанию
- описание:
- адрес: 10.72.14.189
- серийный номер: FAB0541P0PZ
- модель: WS-C2950-24
- версия:

Действия с устройством

- Загрузить
- Проверить соединение
- Скопировать running в startup

Другие действия ▾

Расписания | Обработчики событий 3

Название	Время следующего выполнения	Описание

Config Inspector 3.1.302 [localhost]

← → Устройства > 10.72.10.27 > cisco1231 root [Администратор]

Отчет Уязвимости Cisco IOS

Устройство cisco1231

Результат 2 12 3

Дата обновления 27.02.19 11:14 (27 д. назад) Текущий отчет

Экспорт | Свернуть | Раскрыть Поиск...

- 7.4 Cisco IOS and IOS XE Software Cluster Management Protocol Denial of Service Vulnerability

A vulnerability in the implementation of the cluster feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to trigger a denial of service (DoS) condition on an affected device.

*Версия совпадает с указанной компанией Cisco. 12.1(22)EA13*

fstec 2018-01628  
cve CVE-2018-0475  
cisco cisco-sa-20180926-cmp

> AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
- 7.1 Cisco IOS Software Multicast NTP Denial of Service Vulnerability
- 6.4 Network Time Protocol Information Disclosure of Origin Timestamp

A vulnerability in the standard and the special Network Time Protocol query program (ntpq and ntpdc) could allow an unauthenticated, remote attacker to obtain the value of the origin timestamp expected in the next peer response.

*Версия совпадает с указанной компанией Cisco. 12.1(22)EA13*

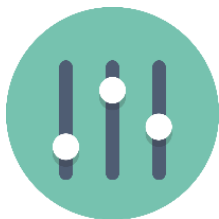
cve CVE-2015-8139  
cisco cisco-sa-20160127-ntp  
cisco cisco-sa-20160127-ntp

> AV:N/AC:L/Au:N/C:P/I:P/A:N
- 6.4 Network Time Protocol Zero Origin Timestamp Bypass
- 5.8 Network Time Protocol Off-Path Broadcast Mode Denial of Service
- 5.4 Standard Network Time Protocol Query Program Replay Attack
- 5.0 Network Time Protocol Replay Attack on Authenticated Broadcast Mode Vulnerability
- 4.3 Cisco IOS and IOS XE Software VLAN Trunking Protocol Denial of Service Vulnerability
- 4.2 Network Time Protocol Daemon redlist NULL Pointer Dereference Denial of Service Vulnerability

## ЗАДАЧИ ИТ



Оперативная диагностика и восстановление после сбоев



Автоматизированное ведение базы данных конфигураций



Контроль проведения запланированных изменений



Удобные механизмы поиска и сравнения

# События на устройстве

Config Inspector 3.1.302 [localhost]

← → Устройства > Сервер > Datacenter > GroupDevs > Network > Cisco 10.72.14.189

root [Администратор]

Статус | Отчеты | **События** | Архив

Перетяните сюда мышкой заголовок колонки для группировки данных по ней

Поиск устройств

Мониторинг

Устройства

События

Настройки

Время	Тип	Сообщение
22.03.2019 16:49:16	Загрузка отчета	Загружен отчет "Cisco IOS 'show running'"
22.03.2019 16:49:16	Нарушение целостности	Отчет "Cisco IOS 'show running'" не соответствует эталону, повторное нарушение
22.03.2019 16:49:16	Изменение отчета	Отчет "Cisco IOS 'show running'" изменен и помещен в архив
22.03.2019 16:49:16	Изменение отчета	Отчет "Проверка политик CIS для Cisco IOS" изменен и помещен в архив
22.03.2019 16:49:16	Запуск действий по триггеру	Запуск действий по триггеру "Изменения контролируемых отчетов"
22.03.2019 16:49:16	Изменение отчета	Отчет "Cisco IOS Конфигурация" изменен и помещен в архив
22.03.2019 16:49:03	Аудит	Загрузка отчета "Cisco IOS 'show running'" устройства "Cisco 10.72.14.189"(тип Cisco IOS), пользователь 'root'
21.03.2019 9:55:57	Загрузка отчета	Загружен отчет "Уязвимости Cisco IOS"
21.03.2019 9:55:30	Загрузка отчета	Загружен отчет "Cisco IOS running-startup difference"
21.03.2019 9:55:23	Загрузка отчета	Загружен отчет "Cisco IOS 'show processes cpu'"
21.03.2019 9:55:17	Загрузка отчета	Загружен отчет "Cisco IOS 'show mac"

**Дополнительно:**  
Загружен отчет "Cisco IOS 'show running'"

**Поля**

Название	Значение
Тип отчета	Cisco IOS 'show running'
Результат	Выполнено
Время загрузки, с.	13

Обновить

Сбросить фильтр

**Фильтр**

По времени

с [ ]

по [ ]

По типу события

Добавить

По важности события

Высокая

Средняя

Низкая

Загружать события дочерних устройств

Применить

Отменить

Группы | Профили

Config Inspector 3.1.302 [localhost]

← → Устройства > Сервер > cisco1231

root [Администратор]

Статус | Отчеты | События | **Архив**

Выборка

Отчет	Время	Тип отчета	Дополнительно
Сегодня			
Проверка политик CIS для Cisco IOS	11:12	Отчет о проверке	Текущий
Cisco IOS Конфигурация	11:12	Отчет	Текущий
Cisco IOS 'show running'	11:12	Текстовый отчет	Текущий
21 марта 2019			
Cisco IOS Процессы	9:52	Отчет	Текущий
19 марта 2019			
Cisco IOS Процессы	14:25	Отчет	
18 марта 2019			
123	13:42	Текстовый отчет	Текущий
14 марта 2019			
Проверка политик CIS для Cisco IOS	17:25	Отчет о проверке	
Cisco IOS Конфигурация	17:25	Отчет	
Cisco IOS 'show running'	17:25	Текстовый отчет	
Уязвимости Cisco IOS	17:12	Отчет о проверке	Текущий
Рабочая и загрузочная конфигурации не с	17:12	Отчет о проверке	Текущий
Cisco IOS 'show startup'	17:11	Текстовый отчет	14.03.2019 17:11:29 Текущий
Проверка политик CIS для Cisco IOS	17:11	Отчет о проверке	
Cisco IOS Конфигурация	17:11	Отчет	
Cisco IOS 'show running'	17:11	Текстовый отчет	14.03.2019 17:11:23

Группы | Профили



Config Inspector 3.1.302 [localhost]

← → Устройства > Сервер > Datacenter > GroupDevs > Network > Cisco 10.72.14.189

root [Администратор]

Отчет Cisco IOS 'show running'  
 Устройство Cisco 10.72.14.189  
 Исходный 20.03.19 17:57 (6 д. назад)

Итоговый 22.03.19 16:49 (4 д. назад) Текущий

Сравнение отчетов

Экспорт  Только отличия Предыдущее Следующее

Исходный	Текущий
1 Building configuration...	1 Building configuration...
2	2
3 Current configuration : 7816 bytes	3 Current configuration : 7832 bytes
4 !	4 !
5 version 12.1	5 version 12.1
6 no service pad	6 no service pad
7 service tcp-keepalives-in	7 service tcp-keepalives-in
8 service tcp-keepalives-out	8 service tcp-keepalives-out
9 service timestamps debug datetime msec localtime show-timezone	9 service timestamps debug datetime msec localtime show-timezone
10 service timestamps log datetime msec show-timezone	10 service timestamps log datetime msec show-timezone
11 service password-encryption	11 service password-encryption
12 !	12 !
13 hostname C2950	13 hostname C2950
14 !	14 !
15 no logging console	15 no logging console
16 no logging monitor	16 no logging monitor
17 aaa new-model	17 aaa new-model
18 aaa authentication login default local	18 aaa authentication login default local
19 aaa authentication enable default enable	19 aaa authentication enable default enable
20 aaa authorization exec default local	20 aaa authorization exec default local
21 aaa authorization commands 14 default group tacacs+	21 aaa authorization commands 14 default group tacacs+
22 aaa authorization commands 15 default group tacacs+ local	22 aaa authorization commands 15 default group tacacs+ local
23 enable secret 5 \$1\$PIu4\$ddcIv3XlQaTx7Bja6SsqF/	23 enable secret 5 \$1\$PIu4\$ddcIv3XlQaTx7Bja6SsqF/
24 enable password 7 06070B2C45400A1016141D	24 enable password 7 06070B2C45400A1016141D
25 !	25 !
26 username admin privilege 15 password 7 06070B2C45400A1016141D	26 username admin privilege 15 password 7 06070B2C45400A1016141D
27 username admin1 privilege 15 password 7 14161606050A7B	27 username admin1 privilege 15 password 7 14161606050A7B
28 username priv1 password 7 03235A11161D2E411E50	28 username priv1 password 7 03235A11161D2E411E50
29 username red password 7 0134071E4B19090271150E	29 username red password 7 0134071E4B19090271150E
30 username redcheck privilege 15 password 7 08064D54190B0A1A4252	30 username redcheck privilege 15 password 7 08064D54190B0A1A4252
31 username readonly privilege 10 password 7 0023121C1449040B5F78	31 username readonly privilege 10 password 7 0023121C1449040B5F78
32 username efrosread password 7 06210E3B5C5C0614554E	32 username efrosread password 7 06210E3B5C5C0614554E
33 username efros15 privilege 2 password 7 022105411B14002C1C17	33 username efros15 privilege 2 password 7 022105411B14002C1C17
34 username user3 privilege 3 password 7 09595D0C0B56	34 username user3 privilege 3 password 7 09595D0C0B56
35 username test1	35 username test1
36 username hacker	36 username hacker
37 username http privilege 15 password 7 04531F121F	37 username http privilege 15 password 7 04531F121F
38 username hacker2 privilege 15 password 7 0520715315E1104495C	38 username hacker2 privilege 15 password 7 0520715315E1104495C

Config Inspector 3.1.302 [localhost]

Настройки > Карта сети

root [Администратор]

Обновить | Фильтр  Нетранзитные сети | Адрес подсети  /  | Группа  | Применить

Мониторинг  
Устройства  
События  
Настройки

```

    graph TD
      A[192.168.100.0 / 24] --- B[Cisco 10.72.14.181 weak]
      B --- C[10.72.14.0 / 24]
      C --- D[cisco1231]
      C --- E[Huawei]
      C --- F[Cisco 10.72.14.189]
      G[Cisco ASA 10.72.10.119] --- H[10.72.10.0 / 24]
  
```

Перейти | Загрузить все

**Cisco 10.72.14.189**  
10.72.14.189

● Устройство доступно

модель, версия  
WS-C2950-24, 12.1(22)EA13

профиль  
По умолчанию

Защищенность  48%

Уязвимости ! 2 ! 12 i 3

Контроль изменений нарушений: 1

Уведомления ! 1 ! 2

## Уникальные преимущества



Сертифицированное ФСТЭК средство для защиты ИТ-инфраструктуры



Развитие продукта в контексте требований рынка и государственных регуляторов



Регулярное обновление данных об угрозах информационной безопасности



Поддержка большого списка отечественных и зарубежных производителей



Техническая поддержка 24/7 на русском языке

Реестр
Заявления
Документы
Помощь

Личный кабинет
🔍

Главная / Реестр / "EFROS Config Inspector"

## "EFROS Config Inspector"

**Сведения о правообладателях программного обеспечения**

**российская коммерческая организация**

Название организации

**ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ГАЗИНФОРМСЕРВИС"**

ИНН 7838017968

**Альтернативные наименования:**

"Efros Config Inspector"

"ЭФРОС Config Inspector"

**Класс ПО:**

Системы мониторинга и управления, Средства обеспечения информационной безопасности



Efros CI включен в Единый реестр российских программ для электронных вычислительных машин и баз данных



Efros CI в 2018г. успешно прошёл процедуру сертификации по требованиям руководящих документов ФСТЭК, НДВ 4

**СИСТЕМА СЕРТИФИКАЦИИ  
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ  
№ РОСС RU.0001.01БИ00

---

**СЕРТИФИКАТ СООТВЕТСТВИЯ  
№ 3977**

Выдан 1 августа 2018 г.  
Действителен до 1 августа 2021 г.

Настоящий сертификат удостоверяет, что **программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.3.1**, разработанный и производимый ООО «Газинформсервис», является программным средством контроля защищенности информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» (Гостехкомиссия России, 1999) — по 4 уровню контроля, технических условий ТУ 5015-048-72410666-2015 при выполнении указаний по эксплуатации, приведенных в формуляре 643.72410666.00048-01 30 01.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией АО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ» (аттестат аккредитации от 15.09.2016 № СЗИ RU.0001.01БИ00.Б010) - техническое заключение от 20.02.2018, экспертного заключения от 27.06.2018 органа по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: ООО «Газинформсервис» (ИНН 7838017968)  
Адрес: 198096, г. Санкт-Петербург, ул. Кронштадтская, дом 10, литер А  
Телефон: (812) 677-2050

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям руководящего документа и технических условий, указанных в настоящем сертификате, осуществляется испытательной лабораторией, аккредитованной ФСТЭК России.

---

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 1 августа 2018 г.

**#CODEIB**

**СПАСИБО ЗА ВНИМАНИЕ**

**Shtubov-N@gaz-is.ru**

**+7 921 414 66 99**

**gaz-is.ru**

**Facebook.com/nikita.shtubov**



**КОД  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ**