GIS ГАЗИНФОРМ СЕРВИС

Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4

Описание применения

Санкт-Петербург 2023

Аннотация

В документе приведены сведения о программном комплексе управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4 (далее по тексту ПК «Efros Config Inspector» v.4 или комплекс). Настоящий документ содержит описание назначения комплекса, описание функциональных возможностей, условий применения и решаемых комплексом задач, а также входные и выходные данные комплекса.

Содержание

1. Назначение ПК «Efros Config Inspector» v.4 4
1.1. Структура и основные характеристики комплекса 7
1.2. Функциональные возможности 12
1.2.1. Обработка отчетов 17
1.2.2. Проверки 20
1.2.3. Сбор, обработка событий 21
1.2.4. Поддержка операций управления устройствами 23
1.2.5. Резервирование сервера ПК 24
2. Условия применения 25
2.1. Требования к техническому и программному обеспечению 25
2.2. Условия эксплуатации 30
3. Описание решаемых комплексом задач 33
3.1. Контроль активного сетевого оборудования разных производителей 33
3.2. Запуск проверок по расписанию 34
3.3. Отправка писем администратору 34
3.4. Отправка извещений сторонним средствам мониторинга 34
3.5. Аудит конфигураций контролируемых устройств по политикам 34
3.6. Конфигурирование устройств и групп устройств 34
3.7. Восстановление конфигурации устройств 35
3.8. Ведение журнала действий пользователей 35
3.9. Возможность аутентификации по протоколу SSH при подключении к устройствам 35
3.10. Контроль файлов ОС 35
3.11. Формирование пользовательских стандартов и настройка требований проверок безопасности для устройств 36
3.12. Универсальный отчет правил межсетевых экранов 36
3.13. Зонный анализ на основе требований разрешения и запрета трафика 39
3.14. Формирование стандартов безопасности и контроль наличия/отсутствия политик и правил МЭ 39
3.15. Оптимизация правил межсетевых экранов 39
3.16. Сбор данных об уязвимостях контролируемого оборудования и ПО 40
3.17. Построение иерархии серверов 40
3.18. Резервирование серверов ПК 40
4. Входные и выходные данные 41
4.1. Входные данные 41
4.2. Выходные данные 42
Перечень сокращений 44
Термины и определения 45

1. Назначение ПК «Efros Config Inspector» v.4

ПК «Efros Config Inspector» v.4 предназначен для активного контроля сетевого оборудования, серверных и клиентских операционных систем (далее – ОС), систем управления базами данных (СУБД), автоматизированных систем управления технологическим процессом (АСУ ТП), виртуальных сред, а также анализа правил межсетевых экранов. Активный контроль контролируемого оборудования осуществляется с использованием протоколов, указанных в таблице 1, при установке серверной части ПК «Efros Config Inspector» v.4 на ЭВМ под управлением одной из следующих ОС:

- ОС специального назначения «Astra Linux Special Edition» v.1.6 (релиз «Смоленск»), v.1.7 (далее – ОС «Astra Linux SE»), сертификат соответствия № 2557 (выдан ФСТЭК России 27.01.2012 г.);
- ОС «РЕД ОС» Муром v.7.2, v.7.3 (далее – ОС «РЕД ОС»), сертификат соответствия № 4060 (выдан ФСТЭК России 12.01.2019 г.);
- ОС серии Windows (x64)[1].

Таблица 1 – Протоколы, используемые ПК «Efros Config Inspector» v.4 для контроля оборудования

Протокол	Где используется	Устройства/Функции	Поддерживаемые ОС
SSH*	Модули взаимодействия с сетевыми устройствами	Сетевые устройства	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
Telnet			
SCP, SFTP	Модуль управления устройствами, Модуль взаимодействия с устройствами Континент, Dionis, Docker	Копирование файлов конфигураций и шаблонов проверок безопасности	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
LDAP	Модуль взаимодействия с Active Directory	Active Directory	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
CPMI	Модуль взаимодействия с устройствами CheckPoint	CheckPoint SmartCenter	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
LEA			
XenAPI	Модуль взаимодействия с Citrix XenServer	Citrix XenServer	ОС серии Windows (x64)

[1] ОС серии Windows (x64) в таблице 1 – перечень версий ОС MS Windows, под управлением которых допускается работа серверной части комплекса (64-разрядные ОС) (полный перечень см. в п. 2.1)).

Протокол	Где используется	Устройства/Функции	Поддерживаемые ОС
Cisco Administrative XML (AXL)	Модуль взаимодействия с сетевыми устройствами Cisco UCM	Cisco UCM	ОС серии Windows (x64)
REST (HTTP/HTTPS)	Модули взаимодействия с устройствами Cisco, Check Point, Скала-Р, SCADA Cimplicity, UiPath, zVirt, Proxmox, Tionix, Primo RPA и Docker	Cisco ACS Cisco Firepower Cisco ACI CheckPoint R80 Check Point Domain Management Server Скала-Р SCADA Cimplicity UiPath zVirt Proxmox Tionix Primo RPA Docker	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
WMI	Модуль взаимодействия с Hyper-V	Загрузка настроек Hyper-V	ОС серии Windows (x64)
PowerShell (WinRM)		Выполнение проверок соответствия Hyper-V	ОС серии Windows (x64)
SMB	Модуль взаимодействия с Active Directory	Загрузка файлов групповых политик	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
	Модуль взаимодействия с Hyper-V	Загрузка файлов ВМ Hyper-V	ОС серии Windows (x64)
Microsoft RTC API	Модуль отправки сообщений через MS Lync	Отправка сообщений в Lync	ОС серии Windows (x64)
Microsoft Exchange Web Services Managed API	Модуль отправки сообщений через MS Exchange	Отправка писем через MS Exchange	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
SMTP	Модуль отправки писем по протоколу SMTP	Отправка писем SMTP	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
Syslog	Модуль отправки syslog-сообщений	Отправка Syslog-сообщений администраторам сети	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
	Модуль Syslog-сервер	Syslog-сервер приема сообщений	
SNMP	Сканер сети для последующего	Поиск устройств в сети (SNMP сканер)	ОС серии Windows (x64), ОС «Astra Linux SE»,

Протокол	Где используется	Устройства/Функции	Поддерживаемые ОС
	добавления найденных устройств в список устройств	Приём сообщений	ОС «РЕД ОС»
		Загрузка сведений по интерфейсам/маршрутам для сетевых устройств	
VIX API (SOAP, HTTPS)	Модуль взаимодействия с vCenter	vCenter, загрузка настроек	ОС серии Windows (x64)
HTTPS		vCenter, загрузка файлов ВМ	ОС серии Windows (x64)
Microsoft TDS	Модуль взаимодействия с MS SQL	СУБД MS SQL	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
Oracle .Net	Модуль взаимодействия с Oracle	СУБД Oracle	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
PostgreSQL Protocol	Модуль взаимодействия с PostgreSQL, Jatoba	СУБД PostgreSQL, Jatoba	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
Firebird Wire Protocol	Модуль взаимодействия с Firebird	СУБД Firebird	ОС серии Windows (x64) ОС «Astra Linux SE», ОС «РЕД ОС»
MySQL	Модуль взаимодействия с MySQL	СУБД MySQL	ОС серии Windows ОС «Astra Linux SE», ОС «РЕД ОС»
XML-RPC	Модуль взаимодействия с UserGate	UserGate	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
DioNIS Control Protocol (DCP)	Модуль взаимодействия с Dionis	Dionis LX	ОС серии Windows (x64)
Проприетарный на базе HTTPS	Windows-агент	Сбор данных с ОС Windows от агента	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
		Прием сообщений от Windows-агента	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
	Сервер	Подключение консоли к серверу	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
		Взаимодействие между серверами в иерархии	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
	Коллекторы	Приём-передача сообщений коллектору комплекса	ОС серии Windows (x64)

Протокол	Где используется	Устройства/Функции	Поддерживаемые ОС
* Используемая в комплексе ПК «Efros Config Inspector» v.4 библиотека libssh поддерживает следующие параметры подключения: – **Ciphers** – chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr,aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc; – **MACs** – hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1; – **KexAlgorithms** – diffie-hellman-group-exchange-sha1,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group18-sha512,diffie-hellman-group16-sha512,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1,ext-info-c; – **HostKeyAlgorithms** – ssh-ed25519,ecdsa-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha2-nistp256,rsa-sha2-512,rsa-sha2-256,ssh-rsa			

1.1. Структура и основные характеристики комплекса

ПК «Efros Config Inspector» v.4 построен на основе архитектуры «Клиент - Сервер» и состоит из:

1) Сервера ПК «Efros Config Inspector» v.4 (далее – сервер ПК):
   - серверной части – устанавливается на выделенной электронно-вычислительной машине (ЭВМ);
   - клиентской консоли – может быть установлена на сервере ПК либо на других рабочих станциях с подключением к серверу ПК по сети;
   - внешних модулей – устанавливаются вместе с серверной частью на сервере ПК, взаимодействуют с серверной частью на программном уровне;
2) Windows-агента – устанавливается на контролируемом компьютере с ОС Windows, подключается к серверной части[1] по сети;
3) Коллектора задач (далее – коллектор) – устанавливается на других ЭВМ, подключается к серверной части по сети.

Серверная часть ПК «Efros Config Inspector» v.4 обеспечивает выполнение функций ПК «Efros Config Inspector» v.4 по контролю сетевого оборудования, серверных и клиентских ОС, СУБД, АСУ ТП, виртуальных сред, а также анализу правил межсетевых экранов, и функций по настройке параметров работы комплекса:

- проверка/создание базы данных (БД) на сервере БД;
- подключение к контролируемым устройствам, Windows-агентам, коллекторам задач и серверам иерархии.

[1] При работе с сервером ПК «Efros Config Inspector» v.4 не поддерживается совместимость с windows-агентами более ранних версий, например, 3.0 и 3.1.

Клиентская консоль подключается к серверной части и предоставляет графический интерфейс для выполнения следующих функций:

1) Мониторинг статистики изменений конфигураций, проверок безопасности, выявления уязвимостей, состояния устройств с помощью встроенных и настраиваемых виджетов (области данных на странице) и уведомлений о событиях контроля и об ошибках выполнения заданий устройств в графическом и текстовом виде.

2) Работа с контролируемыми устройствами:
   - ведение списка устройств и групп устройств;
   - контроль текущих статусов контролируемых устройств (просмотр уведомлений о событиях, зафиксированных для устройств, операциях, выполненных с устройствами, и архива отчетов о событиях и операциях с возможностью выборки и фильтрации отчетов для устройств);
   - выполнение действий с устройствами (например, загрузка отчетов, проверка соединения, конфигурирование и восстановление конфигурации устройств);
   - обновление базы известных уязвимостей для устройств, скрытие/активация уязвимостей.

3) Формирование пользовательских отчетов для нескольких выбранных устройств на основе отчетов, загруженных с устройств, с возможностью сохранения параметров отчета в виде шаблона отчета.

4) Настройка сбора и обработки событий. Просмотр журнала событий с возможностью настройки журнала (фильтрация, построение отчетов).

5) Настройка ПК «Efros Config Inspector» v.4:

а) настройки сервера ПК:
   - задание триггеров для обработки событий системы и устройств, включение/выключение аудита изменений отчетов для привязки произведенных на устройствах изменений к пользователям (с возможностью подключения к Системе контроля действий поставщиков ИТ-услуг);
   - управление профилями для гибкой настройки параметров контроля устройств;
   - управление отчетами, проверками, контролем устройств и групп;
   - управление проверками устройств, настройка правил и исключений;
   - управление списком устройств в части: графического представления топологической карты локальной сети и установки параметров проверки доступности устройств;
   - настройка расписаний загрузки отчетов и выполнения операций с устройствами;
   - настройка скрытия/разрешений загрузок и контроля целостности, вычисляемых/получаемых с устройств отчетов;
   - экспорт и импорт настроек комплекса;
   - сканирование сети (поиск сетевых устройств в локальной сети);
   - настройка политики межсетевых экранов при создании пользовательских правил проверок безопасности;

б) администрирование комплекса:

- подключение, отключение и настройка внешних модулей для работы с контролируемыми устройствами;
- управление учетными записями пользователей комплекса;
- настройка иерархии серверов комплекса;
- настройка сроков хранения данных в БД комплекса;
- просмотр списка резервных серверов ПК;
- настройка коллекторов задач;
- настройка параметров обновления базы данных уязвимостей (БДУ) комплекса;
- настройка подключения комплекса к прокси-серверу БДУ;
- просмотр списка задач, выполняемых комплексом;
- управление лицензиями ПК «Efros Config Inspector» v.4.

6) Настройка параметров запуска внешних программ, используемых для работы с контролируемым оборудованием: SSH-соединений, Telnet-соединений, HTTP-соединений, HTTPs-соединений.

7) Работа с данными, полученными с сервера «Flow Server» (настройка правил формирования событий о зафиксированной сетевой активности, просмотр и анализ полученной информации), доступна только при активной лицензии, содержащей права на использование программного компонента «Flow».

Клиентская консоль подключается к серверу по протоколу HTTPS и TLS. Одновременно к серверу могут быть подключены несколько клиентских консолей.

Коллектор ПК «Efros Config Inspector» v.4 подключается к серверной части. При наличии большого количества задач серверной части (например, загрузка отчетов) часть задач передается на выполнение коллектору.

Внешние модули и windows-агент соединяют сервер программного комплекса с устройствами по различным коммуникационным протоколам. Управление контролируемыми устройствами, а также администрирование сервера ПК осуществляется из клиентской консоли.

ПК «Efros Config Inspector» v.4 обеспечивает активный контроль сетевого оборудования, серверных и клиентских ОС, АСУ ТП, виртуальных сред, а также анализ правил межсетевых экранов производства компаний:

- Cisco Systems, Inc. (полный перечень типов сетевого оборудования см. в пункте 1.2 «Функциональные возможности»);
- 3Com Corporation (3ComOS);
- ЗАО «Российская корпорация средств связи» (RSOS9000, RS7750, RSOA700, Onyx);
- С-Терра СиЭсПи (NME-RVPN, VPN Gate);
- VMware, Inc. (ESXi, vCenter);
- HP, Inc. (BladeSystem, Comware Switch, Procurve, Virtual Connect, UX, Aruba);
- Allied Telesis (Allied-Telesis AT-GS950);
- Lenovo (ENOS 8.4, Cumulus, FabricOS);

- КриптоПро (КриптоПро TLS шлюз);
- Blue Coat Systems, Inc., ранее Crossbeam Systems, Inc. (XOS v.9);
- Oracle Corporation (СУБД Oracle 10g, SunOS, СУБД MySQL);
- D-Link Corporation (DES, DGS, DGS 1210, DGS 3130/3630);
- ООО «СайберЛимфа» (DATAPK);
- Phoenix Contact (Phoenix contact);
- RAISECOM Technology (ISCOM);
- Korenix Technology Co., Ltd (JetNet);
- Kubernetes;
- ZyXEL Communications Corp. (ZyNOS);
- Zelax (Zelax M-1 Мега, Zelax ZES);
- Edge-core (ECS);
- ExtremeNetworks (Extreme 220 series, ExtremeXOS);
- Check Point Software Technologies, Inc. (R80 Management Server, SecurePlatform, GAiA, SmartCenter, GAiA Embedded, Domain Management Server, Maestro Orchestrator);
- ООО «Кьютек» (QSW);
- MikroTik (Mikrotik RouterOS);
- Moxa, Inc (EDS, MGate, NPort 5100 Series);
- Huawei Technologies Co., Ltd (Quidway);
- Citrix Systems, Inc (XenServer);
- ОАО «ИнфоТеКС» (VipNet Coordinator, VipNet xFirewall, VipNet Prime);
- H3C Technologies (H3C);
- НПП «Фактор-ТС» (Dionis LX и Dionis NX версии 1.1, 1.2 и 2.0);
- Juniper Networks, Inc (JUNOS);
- ООО «Предприятие «Элтекс» (Eltex ESR, ME, MES, MES2428, WLC, WOP/WEP);
- ООО «Бифорком Тек» (коммутаторы серии CS2100);
- ООО «Код Безопасности» (Код Безопасности Континент);
- ООО «ТИОНИКС» (TIONIX);
- Palo Alto Networks, Inc (PanOS 7, 9);
- ОАО НПП «Полигон» (Арлан, ИнЗер);
- UiPath Inc (Uipath Studio, Uipath Orchestrator, Uipath Robot);
- Primo RPA (Primo RPA Orchestrator);
- WatchGuard Technologies, Inc. (WatchGuard Fireware OS, WatchGuard Fireware XTM OS);
- Rockwell Automation, Inc (Rockwell Cisco IOS);
- TFortis (PSW);Siemens AG (Siemens Scalance X-300, X-400 series, Simatic WinCC);
- ОС Unix/Linux (полный перечень ОС см. в пункте 1.2 «Функциональные возможности»);
- ОС Microsoft Windows (полный перечень ОС см. в пункте 1.2 «Функциональные возможности»);
- Virtual Machine Manager, Hyper-V (полный перечень ПО см. в пункте 1.2 «Функциональные возможности»);

- ООО «Базальт СПО» (Альт Сервер Виртуализации 9.2 в PVE исполнении (PVE версия 6.3));
- СУБД Microsoft (MS SQL 2000, 2005, 2008, 2012, 2016);
- СУБД PostgreSQL;
- ООО «Газинформсервис» (СУБД «Jatoba»);
- Firebird Foundation (СУБД Firebird);
- Docker;
- Open Virtualization Alliance (KVM);
- Инфолэнд (zVirt);
- НАТЕКС (NetXpert);
- NSGate (NIS);
- Hirschmann (MAR);
- UserGate (UserGate UTM);
- AVAYA;
- Azimut (Marlin);
- AdAstrA Research Group, Ltd (SCADA TRACE MODE);
- Fortinet (Fortinet FortiGate, Fortinet FortiGate VDOM, Fortinet FortiWLC, Fortinet FortiSwitch);
- РЕД СОФТ (РЕД Виртуализация 7.3.0);
- НПФ «Система-Сервис» (Аргус);
- АО «ЭлеСи» (SCADA Infinity);
- Атомик Софт (SCADA Alpha.HMI);
- ООО «ИнСАТ» (MasterSCADA);
- ФГУП «ЭЗАН» (SCADA-система «Соната»);
- GE Digital (CIMPLICITY, iFix, GENESIS32);
- Schneider Electric (Vijeo Citect SCADA);
- Compressor Controls Corporation (CCC) (TrainTools, TrainView);
- ООО «Газприборавтоматика» (Zond2006, Zond2015);
- Emerson (SCADA DeltaV);
- Yokogawa Electric Corporation (CENTUM VP);
- НПО «Текон-Автоматика» (SCADA АСУД-248);
- ООО «НПА Вира Реалтайм» (ПК «Сириус-ИС»);
- Rubytech (СКАЛА-Р 1.91);
- Verano (RTAP A.08.10 (Windows), RTAP A.09.00 (Linux));
- Wonderware InTouch (7, 8, 10, 11);
- Weidmueller.(Weidmueller Advanced Line Managed Switches);
- АО «ТРЭИ» (ПЛК Trei (QNX 6.5));
- АО «ЭЗАН» (ПЛК Ezan (QNX 6.5)).

Список протоколов и модулей, с использованием которых на сервере ПК «Efros Config Inspector» v.4 может осуществляться активный аудит сетевого и серверного оборудования, может быть расширен за счет разработки и включения в программный комплекс соответствующих внешних модулей.

Данные ПК «Efros Config Inspector» v.4 хранятся во внешней СУБД. В качестве внешней СУБД поддерживаются:

– PostgreSQL: 11, 12, 13, 14, 15;
– Microsoft SQL Server: 2016, 2017, 2019 (только при условии установки серверной части ПК на ЭВМ под управлением ОС серии Windows);
– MySQL: 8.0;
– защищенная СУБД «Jatoba» (сертификат соответствия № 4327 от 19.11.2020, выдан ФСТЭК России).

Также поддерживаются новые версии указанных СУБД.
СУБД может быть установлена локально на сервере ПК либо на удаленном компьютере (далее – сервере БД) и подключена к серверу ПК по сети.

1.2. Функциональные возможности

ПК «Efros Config Inspector» v.4 реализует следующие функциональные возможности:

1) Контроль и разграничение доступа пользователей к функциям комплекса и к устройствам:
– ведение списка пользователей комплекса с возможностью управления пользователями (добавление пользователей, групп пользователей, блокирование, активация, удаление учетной записи пользователя, смена пароля пользователя);
– разграничение доступа пользователей комплекса к функционалу комплекса, к списку контролируемых устройств, включая операции по чтению, записи (удалению), разрешенные к выполнению пользователям при доступе к контролируемым устройствам и к операциям на подчиненных серверах;
– разделение полномочий пользователей и администраторов комплекса, с предоставлением прав и привилегий по доступу к параметрам настройки исключительно администратору;
– автоматическое блокирование идентификатора пользователя после заданного в параметрах периода (от 1 до 90 дней) его неиспользования;
– автоматическая проверка характеристик паролей при их создании, проверка сложности паролей, проверка паролей по истории паролей (запрет на использование пользователем любого из ранее использованных паролей или общеизвестных паролей при создании новых);
– ограничение времени действия паролей (максимальное и минимальное время);
– настройки правил использования паролей и удаленной работы пользователей комплекса с серверной частью комплекса;
– блокировка возможности подключений с IP-адреса на заданный в параметрах период (от 10 до 60 минут) в случае нескольких подряд попыток ввода неверной идентификационной информации пользователя (от 3 до 8 неуспешных попыток аутентификации).

2) Ведение списка контролируемых устройств:
– ведение списка контролируемых комплексом устройств и групп устройств;
– поиск устройств в сети (сканирование сети);

– расширение списка, поддерживаемого комплексом оборудования, за счет подключения к нему дополнительных модулей.

3) Идентификация и аутентификация пользователей и устройств:

– идентификация и аутентификация пользователей и устройств комплекса на сервере ПК с использованием идентификатора и паролей, защита ввода паролей;

– идентификация устройств на сервере ПК по логическим именам (имя устройства и (или) ID), логическим адресам (IP-адресам) или по комбинации имени и логического адреса устройства;

– аутентификация устройств в ПК с использованием соответствующих протоколов аутентификации (сертификатов или учетных данных пользователя с применением проприетарного протокола на основе HTTPS).

4) Управление устройствами:

– загрузка в комплекс текстовых конфигураций контролируемых устройств (текстовых файлов, выводов команд);

– загрузка и формирование отчетов по настройкам, локальным файлам и параметрам работы контролируемых устройств;

– выполнение проверок соответствия конфигурации контролируемых устройств требованиям безопасности (compliance проверки);

– выполнение конфигурирования устройств и групп устройств по запросу пользователя;

– выполнение восстановления конфигурации устройств по запросу пользователя;

– выполнение проверок устройств и групп устройств по расписанию.

5) Контроль работы устройств:

– мониторинг уведомлений о событиях контроля и об ошибках выполнения заданий устройств в графическом и текстовом виде;

– обеспечение проверки соответствия рабочей (running) и загрузочной (startup) конфигураций при загрузке контролируемого оборудования; установка эталонных конфигураций, ведение истории версий отчетов с конфигурациями контролируемого оборудования, осуществление сравнения текстов конфигураций;

– контроль текущих статусов контролируемых устройств и групп устройств (просмотр уведомлений о событиях, зафиксированных для устройств и групп устройств, операциях, выполненных с устройствами и группами, и архива отчетов о событиях и операциях);

– ведение архива текстовых конфигураций и отчетов;

– контроль изменений текстовых конфигураций и отчетов;

– экспорт данных контроля оборудования в файл.

6) Проверка наличия уязвимостей контролируемого оборудования:

– выполнение проверок наличия уязвимостей контролируемого оборудования, с формированием отчетов по результатам выполнения проверок устройств на наличие уязвимостей с описанием выявленных уязвимостей (с возможностью скрытия/активирования уязвимостей);

– использование БДУ для выявления уязвимостей, на основании данных вендоров, открытых баз уязвимостей;

– возможность настройки подключения к БДУ через прокси-сервер.

7) Сбор и обработка событий:

– сбор и обработка событий (сообщений) с контролируемых устройств;

– ведение журнала событий, включающего аудит действий пользователей комплекса, с возможностью настройки журнала (фильтрация, выборка, построение отчетов).

8) Настройка общих параметров работы комплекса:

– возможность настройки реакции комплекса (выполнение проверок, отправка писем и сообщений) на события (как принятые с устройств, так и события системы);

– отправка писем во внешние информационные системы;

– настройка параметров запуска внешних программ, используемых для работы с контролируемым оборудованием: SSH-соединений, Telnet-соединений, HTTP-соединений, HTTPs-соединений.

9) Контроль целостности программного обеспечения комплекса и функционирования оборудования:

– контроль целостности собственного программного обеспечения, а также прикладного и системного программного обеспечения (ПО), установленного на контроль, посредством периодической проверки контрольных сумм;

– инвентаризация контролируемого оборудования (технических средств и средств защиты информации) с помощью протокола ICMP и SNMP;

– контроль доступности серверного и телекоммуникационного оборудования;

– контроль выполняемых комплексом задач.

10) Формирование и просмотр пользовательских отчетов:

– создание пользовательских отчетов для выбранных устройств на основе отчетов, загруженных с устройств;

– создание на основе пользовательских отчетов шаблонов отчетов в зависимости от прав пользователя только личных (доступных только пользователю, создавшему шаблон) или также и общих (доступных всем пользователям комплекса).

11) Хранение и резервирование данных:

– хранение данных комплекса в реляционной БД с возможностью настройки сроков хранения оперативной информации;

– бэкапирование данных средствами СУБД с возможностью восстановления БД;

– резервирование серверов ПК.

Оборудование, поддерживаемое серверной частью «Efros Config Inspector» v.4, установленной на разные платформы (ОС «Astra Linux SE», ОС «РЕД ОС» и ОС серии Windows), представлено в таблице 2.

Таблица 2 – Перечень поддерживаемого оборудования серверной частью «Efros Config Inspector» v.4, установленной на различные платформы

Поддерживаемое оборудование	ОС «РЕД ОС»	ОС «Astra Linux SE»	ОС серии Windows
3Com OS	ДА	ДА	ДА
AD Domain	ДА	ДА	ДА
Allied-Telesis AT-GS950	ДА	ДА	ДА
Avaya	ДА	ДА	ДА
Cisco (ACS, ACI, ASA, AsyncOS, CatOS, FTD, FWSM Module, IOS, IOS XE, IOS XR, IPS, NX-OS, PIX, SMB, WAP, WLC, FMC 6.x (с поддержкой MDS), Firepower)	ДА	ДА	ДА
Cisco (UCM 10.0, UCM 8.5, Unified Phone 78xx, Unified Phone 88xx)	НЕТ	НЕТ	ДА
Check Point (GAiA, GAiA Embedded, R80 Management Server, SecurePlatform, SmartCenter, Domain Management Server, Maestro Orchestrator)	ДА	ДА	ДА
Crossbeam XOS v.9	ДА	ДА	ДА
DATAPK	ДА	ДА	ДА
Phoenix contact	ДА	ДА	ДА
H3C	ДА	ДА	ДА
Dionis NX (NX 1.1, NX 1.2, NX 2.0)	ДА	ДА	ДА
Dionis LX	НЕТ	НЕТ	ДА
D-Link (DES, DGS, DGS 1210, DGS 3130/3630)	ДА	ДА	ДА
Edge-Core ECS	ДА	ДА	ДА
Eltex (ESR, ME, MES2428, MES, WLC, WOP/WEP)	ДА	ДА	ДА
Extreme 220 series, ExtremeXOS	ДА	ДА	ДА
Fortinet FortiGate, Fortinet FortiGate VDOM, Fortinet FortiWLC, Fortinet FortiSwitch	ДА	ДА	ДА
Hirschmann MAR	ДА	ДА	ДА
HP (BladeSystem, Comware Switch, Procurve, Virtual Connect, UX, Aruba)	ДА	ДА	ДА
Huawei VRP	ДА	ДА	ДА
Juniper JunOS	ДА	ДА	ДА
Korenix JetNet	ДА	ДА	ДА
Kubernetes	ДА	ДА	ДА
Lenovo ENOS 8.4, Cumulus, FabricOS	ДА	ДА	ДА
Mikrotik RouterOS	ДА	ДА	ДА
Moxa (EDS, MGate, NPort 5100 Series)	ДА	ДА	ДА
MS SCVMM (Virtual Machine Manager 2008 R2, 2012 R2, 2016, 2019, SCVMM Group, Hyper-V 2008 (R2 VM, R2 хост, R2 хост с контролем целостности), Hyper-V 2012 (R2 VM, R2 хост, R2 хост с контролем целостности), Hyper-V 2016 (VM, хост, хост с контролем целостности), Hyper-V 2019 (VM, хост, хост с контролем целостности) Standalone Hyper-V (2008 R2, 2012 R2, 2016, 2019))	НЕТ	НЕТ	ДА
Альт Сервер Виртуализации 9.2 в PVE исполнении (PVE версия 6.3)	ДА	ДА	ДА
MS SQL 2000, 2005, 2008, 2012, 2016	ДА	ДА	ДА

Поддерживаемое оборудование	ОС «РЕД ОС»	ОС «Astra Linux SE»	ОС серии Windows
PostgreSQL	ДА	ДА	ДА
СУБД «Jatoba»	ДА	ДА	ДА
KVM (актуальные версии Linux)	ДА	ДА	ДА
Nateks (NX-3400, NX-5100, NXI-3030, NXI-3050)	ДА	ДА	ДА
КриптоПро TLS шлюз	ДА	ДА	ДА
NSGate NIS	ДА	ДА	ДА
Palo Alto Pan-OS 7, 9	ДА	ДА	ДА
PKCC (OmniAccess 700, OmniSwitch 6850, OmniSwitch 7710, OmniSwitch 7750, OmniSwitch 9000, Onyx)	ДА	ДА	ДА
QTech QSW	ДА	ДА	ДА
Raisecom ISCOM	ДА	ДА	ДА
Rockwell Cisco IOS	ДА	ДА	ДА
TFortis PSW	ДА	ДА	ДА
Azimut Marlin	ДА	ДА	ДА
Siemens Scalance X-300 series, X-400 series, Simatic WinCC	ДА	ДА	ДА
S-Terra VPN Gate	ДА	ДА	ДА
ViPNet Coordinator HW, ViPNet xFirewall, ViPNet Prime	ДА	ДА	ДА
TIONIX	ДА	ДА	ДА
Код безопасности Континент	ДА	ДА	ДА
Коммутаторы CS2100 (Бифорком Тек)	ДА	ДА	ДА
VMWare vCenter (vCenter (VCSA, Windows), Standalone ESXi с контролем файлов по HTTPS (SSH), VM (5.0, 5.1, 5.5, 6.0, 6.5, 7), Host, Host с контролем целостности файлов по SSH (HTTPS), Folder, Datacenter, vApp, Resource Pool, ESXi ОС с контролем файлов по HTTPS (SSH), Cluster)	НЕТ	НЕТ	ДА
ESXi ОС с контролем файлов по SSH	ДА	ДА	ДА
СКАЛА-Р 1.91	ДА	ДА	ДА
Uipath Studio, Uipath Orchestrator, Uipath Robot	ДА	ДА	ДА
Primo RPA Orchestrator	ДА	ДА	ДА
UserGate UTM 5, 6, 7	ДА	ДА	ДА
WatchGuard Fireware (OS, XTM OS)	ДА	ДА	ДА
ОС Unix/Linux (AIX, Oracle Oracle SunOS, HP-UX, AltLinux, Red Hat, Debian, Manjaro, Ubuntu, Mint, Fedora, FreeBSD, Red OS, Astra Linux)	ДА	ДА	ДА
ОС Windows (xp, vista, 7, 8, 10, 2000, 2003, 2008r2, 2012, 2012r2, 2016, 2019)	ДА	ДА	ДА
РЕД Виртуализация 7.3.0	ДА	ДА	ДА
СУБД Oracle 10g	ДА	ДА	ДА
СУБД MySQL 5.5.7 и выше	ДА	ДА	ДА
СУБД Firebird	ДА	ДА	ДА
Docker	ДА	ДА	ДА
Citrix XenServer	НЕТ	НЕТ	ДА
Zelax M-1-MEGA, Zelax ZES	ДА	ДА	ДА
ZyXEL ZyNOS	ДА	ДА	ДА

Поддерживаемое оборудование	ОС «РЕД ОС»	ОС «Astra Linux SE»	ОС серии Windows
zVirt 4.3.3.6-1.el7	ДА	ДА	ДА
Полигон (Арлан, ИнЗер)	ДА	ДА	ДА
SCADA Alpha.HMI	ДА	ДА	ДА
SCADA Infinity	ДА	ДА	ДА
SCADA- Аргус	ДА	ДА	ДА
MasterSCADA	ДА	ДА	ДА
SCADA-система «Соната»	ДА	ДА	ДА
SCADA ПК «Сириус-ИС»	ДА	ДА	ДА
SCADA DeltaV v. 6.3.2	ДА	ДА	ДА
SCADA TRACE MODE v. 5 и 6	ДА	ДА	ДА
GENESIS32	ДА	ДА	ДА
CENTUM VP	ДА	ДА	ДА
CIMPLICITY	ДА	ДА	ДА
iFix 3.5	ДА	ДА	ДА
TrainTools	ДА	ДА	ДА
TrainView	ДА	ДА	ДА
Vijeo Citect v 7.40	ДА	ДА	ДА
SCADA АСУД-248	ДА	ДА	ДА
SCADA RTAP A.08.10 (Windows), RTAP A.09.00 (Linux)	ДА	ДА	ДА
Zond2006	ДА	ДА	ДА
Zond2015	ДА	ДА	ДА
Wonderware InTouch (7, 8, 10, 11)	ДА	ДА	ДА
Weidmueller Advanced Line Managed Switches	ДА	ДА	ДА
ПЛК Trei (QNX 6.5)	ДА	ДА	ДА
ПЛК Ezan (QNX 6.5)	ДА	ДА	ДА

Отличие функций ПК «Efros Config Inspector» v.4, установленного на разные платформы (ОС «Astra Linux SE», ОС «РЕД ОС» и ОС серии Windows), представлено в таблице 3.

Таблица 3 – Функциональные различия ПК «Efros Config Inspector» v.4 при развертывании на различных платформах

Функции	ОС «РЕД ОС»	ОС «Astra Linux SE»	ОС серии Windows
Идентификация и аутентификация пользователей под доменной учетной записью	ДА	ДА	ДА
Наличие клиентской консоли, для локальной установки совместно с сервером, реализующей графический интерфейс для управления функциями комплекса	НЕТ (используется консоль, установленная на сервере под управлением ОС серии Windows)	НЕТ (используется консоль, установленная на сервере под управлением ОС серии Windows)	ДА

Резервирование серверов ПК доступно только при условии, что серверы ПК установлены на одинаковые платформы. Кроме того, не допускается миграция БД между разными типами ОС, поскольку после такой миграции станет невозможен запуск сервера ПК с подключением к БД на новой ОС.

Для успешного построения иерархии, все сервера ПК, включаемые в иерархию, должны иметь одинаковую версию (мажорную и минорную). Например, управляющий и подчиненный сервер ПК в иерархии должны быть версии 4.14.

1.2.1. Обработка отчетов

Отчеты формируются путем загрузки с устройств или через преобразование из существующих отчетов.

Отчеты позволяют:

- просматривать данные устройств;
- выполнять фильтрацию и выборки;
- отслеживать изменение настроек устройств, хранить архив изменений;
- контролировать целостность настроек;
- проверять корректность настроек, использовать дополнительные проверки.

Комплекс позволяет создавать отчеты типа *Фильтр* для загрузки с устройств, выбирая поля и записи из существующих отчетов. Такая возможность в комбинации с функциями контроля целостности создает новые сценарии использования комплекса. Например, пользователь может составить список допустимых процессов и проверять группу серверов на соответствие этому списку.

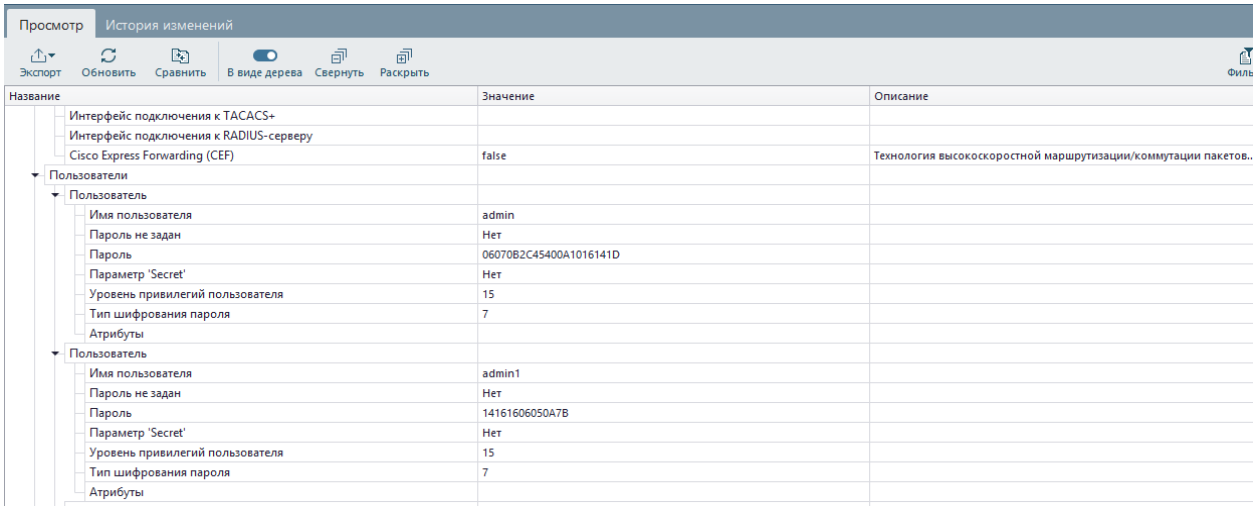
Для межсетевых экранов (МЭ) кроме встроенных отчетов пользователем при настройке проверок МЭ могут быть созданы стандарты безопасности, содержащие требования к политикам и правилам, заданным на МЭ, и назначены устройства, в списке отчетов которых будет доступен отчет по созданному стандарту безопасности

В ПК «Efros Config Inspector» v.4 поддерживаются следующие форматы отчетов:

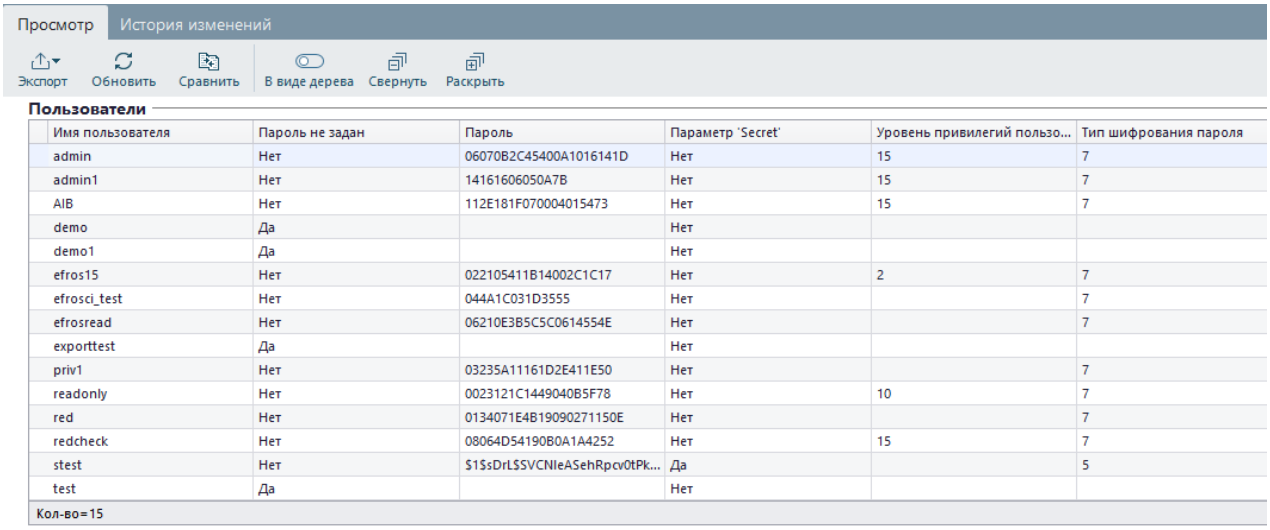
- отчеты о конфигурации, включающие текстовые и структурированные отчеты;
- отчеты о проверках (политик безопасности, наличия уязвимостей, синхронизации рабочей и загрузочной конфигураций).

На рисунке 1 (а, б) приведены примеры представлений отчета, содержащего список пользователей, извлеченный из конфигурационного файла Cisco IOS. Данные отчетов, загруженных с устройств, могут быть экспортированы в файл формата TXT (текстовые отчеты) и XML, HTML (структурированные отчеты).

Поддерживается также возможность создания на основе отчетов, загруженных с устройств, пользовательских отчетов для нескольких выбранных устройств.



а)



б)

Рисунок 1 – Примеры представлений отчета, содержащего список пользователей, извлеченный из конфигурационного файла Cisco IOS

Поддерживаются следующие типы пользовательских отчетов:

- ***Выборка*** – отчеты, содержащие последние загруженные с выбранных устройств версии отчета формата ***Конфигурации*** и ***Проверки*** выбранного типа в соответствии с заданными условиями фильтрации;
- ***Уязвимости устройств*** – отчеты, содержащие перечень уязвимостей для устройств заданных типов. Поддерживается возможность скрытия/активации уязвимостей для выбранных устройств;
- ***История изменений*** – отчеты, содержащие данные об отчетах с изменениями для выбранных типов отчетов (всех форматов) выбранных устройств за выбранный период времени;
- ***Бюллетени НКЦКИ*** – отчеты, содержащие перечень уязвимостей из бюллетеней Национального координационного центра по компьютерным инцидентам (НКЦКИ) для устройств заданных типов за выбранный период времени;

- ***Правила межсетевых экранов*** – отчеты, содержащие все правила на разных устройствах, соответствующие заданным критериям;
- ***Оптимизация правил МЭ*** – отчеты, содержащие перечень обнаруженных теневых, избыточных, а также неиспользуемых правил МЭ и правил с нулевым Hit Count (число случаев выполнения правила) для устройств заданных типов.

Параметры формирования пользовательских отчетов могут быть сохранены в виде шаблона отчета и повторно использоваться для формирования отчета. Шаблоны отчетов могут быть двух типов ***Личные*** (доступные только пользователю) и ***Общие*** (доступные всем пользователям).

1.2.2. Проверки

Проверки добавляются на сервер ПК вместе с подключением внешних модулей работы с устройствами, для которых они предназначены.

Проверки могут иметь различные назначения:
– **проверка доступности**. Например, проверка доступности по ICMP ping либо проверка подключения к устройству по выбранному протоколу;
– **сервисные проверки**. Например, проверка синхронизации running и startup конфигураций Cisco IOS;
– **проверка безопасности (Compliance)**. Например, проверка аудита конфигурации Cisco IOS по правилам CIS или соответствие корпоративному стандарту;
– **проверка уязвимостей**. Например, вывод текущих уязвимостей для Cisco IOS по стандарту OVAL (https://oval.mitre.org/).

Для настройки проверок под нужды пользователя поддерживаются:
– возможность отключения проверки;
– возможность исключения одного или нескольких правил из проверки;
– возможность задания исключений для правил (например, исключение пользователя из правила ***Необходимо шифровать пароли пользователей***);
– возможность создавать собственные правила и стандарты с помощью регулярных выражений. Описание регулярных выражений стандарта PCRE, допустимых к применению в ПК «Efros Config Inspector» v.4, приведено в Приложении 1 документа 643.72410666.00082-01 95 01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 2. Настройки контроля».

Данные отчетов о результатах проверки могут быть экспортированы в файл формата HTML (по выбору пользователя экспортируются данные всех проверок, только нарушенных или только пройденных успешно). Пример отчета о результате проверки приведен на рисунке 2.

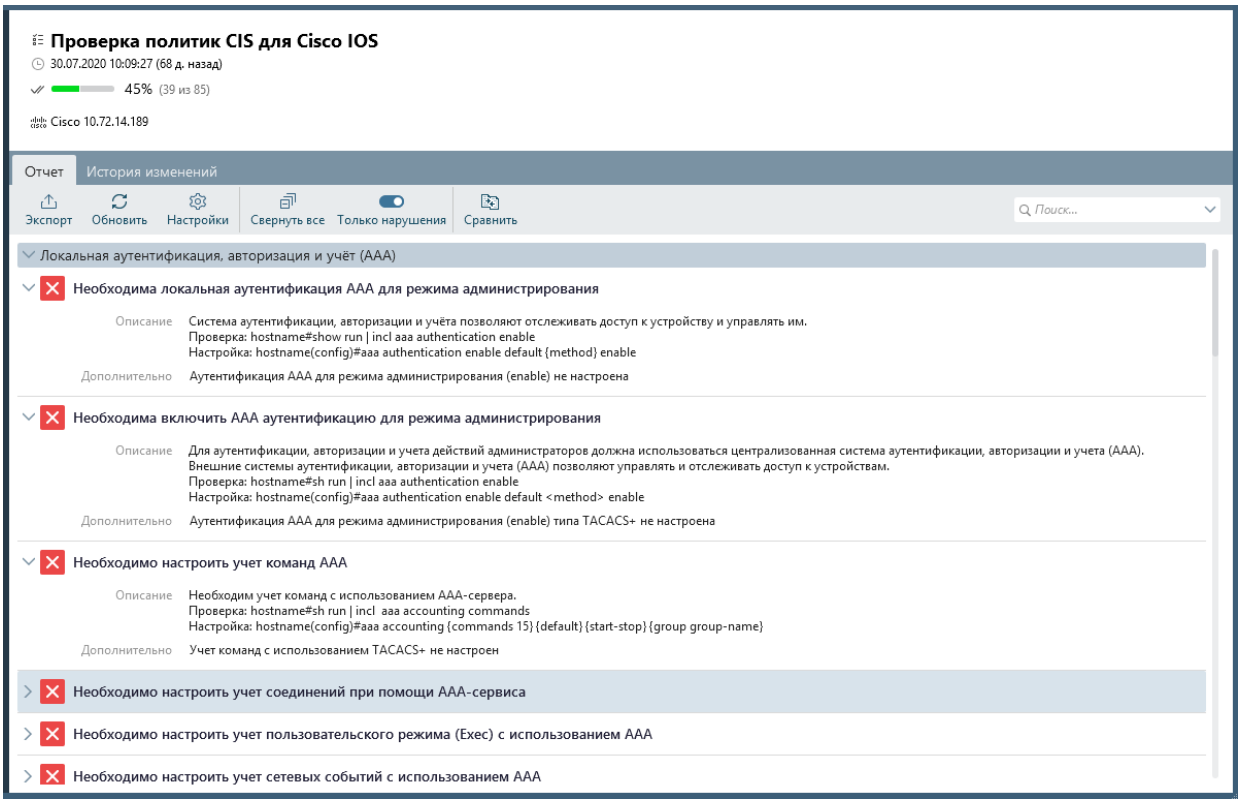


Рисунок 2 – Отчет о результате проверки

1.2.3. Сбор, обработка событий

ПК «Efros Config Inspector» v.4 поддерживает сбор и хранение событий, произошедших на сервере ПК или на контролируемом оборудовании.

События могут регистрироваться как самим ПК «Efros Config Inspector» v.4 (например, при загрузке отчета), так и внешними модулями (например, Syslog-сообщения).

При этом комплекс поддерживает динамическое добавление новых типов событий. Помимо типа события также добавляются поля, которые содержит событие. Например, модуль Syslog-сервера регистрирует тип события Syslog-сообщение с полями *Facility*, *Severity*, *Address*, *Message*.

Перечень событий по умолчанию (до подключения внешних модулей):

- аудит;
- восстановление конфигурации;
- выполнение конфигурирования;
- выполнение операции;
- загрузка отчета;
- запуск действий по триггеру;
- запуск задания по расписанию;
- изменение доступности;
- изменение отчета.
- изменение результата проверки;
- контроль целостности компонентов;

- нарушение целостности;
- обновление словаря уязвимостей;
- переключение основного сервера;
- экспорт отчетов;
- ошибка сервера.

Примечание – К ошибкам сервера могут относиться:

- ошибки выполнения реакций на события (отправка почты/syslog, экспорт событий);
- ошибки запуска модулей (например, занят порт Syslog-сервера);
- критические ошибки при обработке результата загрузки отчета или при выполнении операции;
- ошибки при выполнении связанных действий при commit/rollback транзакций;
- другие ошибки, которые могут быть важны пользователю, например, *Переполнение очереди syslog сообщений, часть сообщений пропущена.*

В дальнейшем, данные, содержащиеся в полях событий, могут использоваться для задания условий, как при фильтрации (рис. 3), так и при настройке обработчиков событий (триггеров) (рис. 4). Возможность создания триггеров доступна пользователям ПК «Efros Config Inspector» v.4 с правами *Управление* категории *Настройки контроля*.

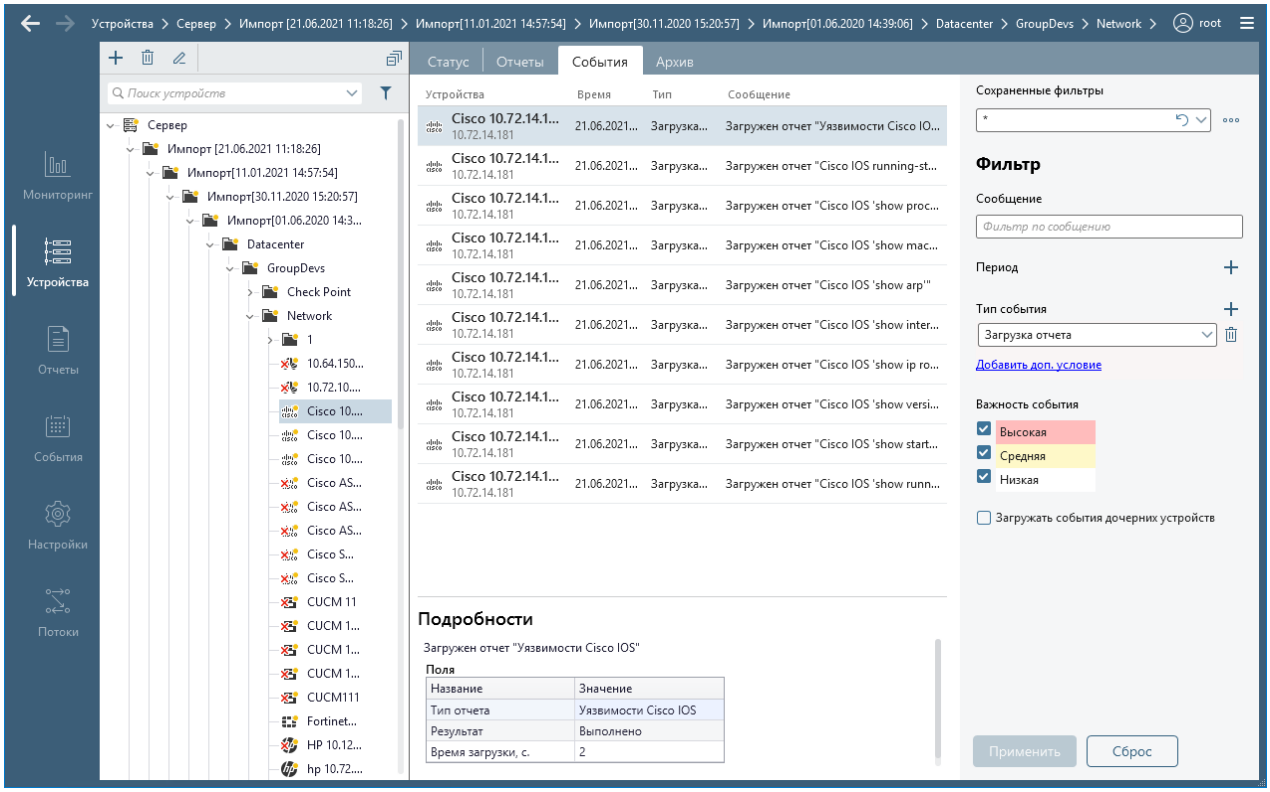


Рисунок 3 – Фильтрация событий

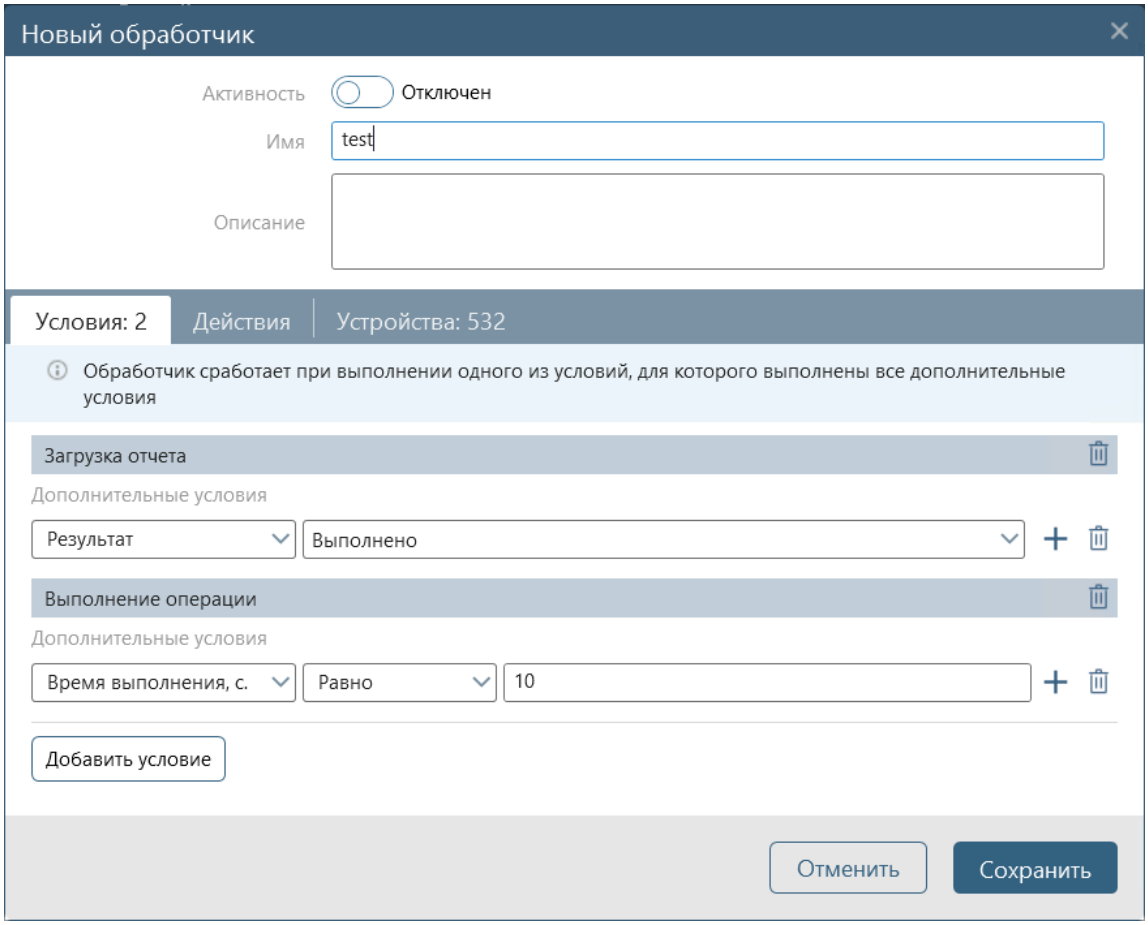


Рисунок 4 – Задание условий при настройке обработчика событий

При создании триггеров пользователь может выбирать типы событий и задавать условия к их полям. При этом в качестве реакции системы возможны следующие варианты, например:

- создание уведомления в системе;
- проверка соединения;
- запуск загрузки отчетов;
- экспорт событий;
- отправка писем, syslog сообщений с деталями события.

1.2.4. Поддержка операций управления устройствами

ПК «Efros Config Inspector» v.4 поддерживает выполнение операций с устройствами (например, операция копирования рабочей конфигурации в конфигурацию запуска для устройств Cisco IOS, изменение загрузочной конфигурации отдельных типов устройств, восстановление конфигураций сетевых устройств Eltex MES, Eltex ESR, Cisco ASA, Cisco IOS, Cisco SMB, HP Comware, Huawei VRP, Marlin (Azimut), Dionis NX и Mikrotik (RouterOS) с использованием сохраненных в архиве загрузочных конфигураций).

Операции управления устройствами добавляются на сервер ПК путем установки модуля управления. Управление устройством доступно только при наличии модуля управления и модуля соответствующего устройства.

С сервера ПК операции управления устройствами могут выполняться:

- по запросу пользователя;
- по расписанию;
- как результат обработки событий (по триггеру).

1.2.5. Резервирование сервера ПК

В ПК «Efros Config Inspector» v.4 доступна настройка резервирования сервера ПК (поддерживается только для серверов ПК, установленных на однотипных ОС).

Резервирование сервера ПК осуществляется в случае выхода из строя основного сервера ПК. При этом все функции основного сервера ПК принимает на себя резервный.

Для функционирования резервного сервера ПК необходимо выполнить его настройку. Порядок настройки режима резервирования сервера ПК описан в п. 6.5 «Настройка режима резервирования сервера ПК» руководства администратора.

Режим резервирования будет доступен при наличии одного и более резервных серверов ПК.

Примечание – Резервирование используемой СУБД средствами ПК «Efros Config Inspector» v.4 не выполняется, но может быть выполнено за рамками ПК «Efros Config Inspector» v.4 встроенными средствами СУБД.

При наличии нескольких серверов ПК основным считается тот, который был подключен к БД комплекса первым.

В случае нарушения работы основного сервера ПК через заданный в БД комплекса промежуток времени (по умолчанию составляет 10 минут) произойдет автоматическое переключение на резервный сервер ПК. При наличии более одного резервного сервера ПК, переключение происходит на тот, который был раньше других подключен к БД комплекса.

Вышедший из строя сервер ПК и все остальные серверы ПК остаются в статусе резервных.

2. Условия применения

2.1. Требования к техническому и программному обеспечению

Рекомендуемый состав технических средств электронно-вычислительной машины (ЭВМ)[1] для установки серверной части и внешних модулей ПК «Efros Config Inspector» v.4 рассчитывается на основе данных приведенных в таблицах 4 - 6.

Рекомендуемые параметры для полосы пропускания для организации иерархии контролируемой сервером ПК сети размером от «До 50 ОЗ» до «До 2000 ОЗ»:

- минимальный канал для функционирования серверов в иерархии в режиме передачи уведомлений – 512 кбит\с. Низкая скорость отклика системы;
- рекомендуемая скорость от 2 Мбит\с и выше.

Для сетей от 2000 объектов защиты (ОЗ) параметры рассчитываются индивидуально. Необходимо обращение в техподдержку.

Таблица 4 – Рекомендуемые требования к производительности ЭВМ установки сервера ПК

Размер контроли-руемой сети сервером ПК[1)]	**Аппаратные требования**					
	CPU	**RAM**	**ROM[2)]**	**Сетевые порты**	**Рекомендованный объем дискового пространства[3)] для хранения данных на срок до**	
					90 дней[4)], Гбайт	**180 дней[5)], Гбайт**
До 50 ОЗ	От 2 Ghz CPU, Cores: 4	8 GB	SAS 10K и выше	1 порт 100 Мбит/с	Не менее 50	Не менее 100
До 150 ОЗ	от 2 Ghz CPU, Cores: 4	8 GB	SAS 10K и выше	1 порт 100 Мбит/с	Не менее 150	Не менее 300
До 300 ОЗ	от 2 Ghz CPU, Cores: 8	16 GB	SAS 10K и выше	1 порт 100 Мбит/с	Не менее 200	Не менее 400
До 500 ОЗ	от 2 Ghz CPU, Cores: 12	16 GB	SAS 15K и выше	1 порт 1 Гбит/с	Не менее 300	Не менее 600
До 1000 ОЗ	от 2 Ghz CPU, Cores: 16	32 GB	SSD	1 порт 1 Гбит/с	Не менее 600	Не менее 1200
До 2000 ОЗ	от 2 Ghz CPU, Cores: 16	32 GB	SSD	1 порт 1 Гбит/с	Не менее 1200	Не менее 2400
От 2000 ОЗ	Рассчитывается индивидуально. Необходимо обращение в техподдержку					

[1] Под ЭВМ понимается электронно-вычислительная машина, совместимая с архитектурой Intel x86_64.

Размер контроли-руемой сети сервером ПК[1)]	Аппаратные требования					
	CPU	RAM	ROM[2)]	Сетевые порты	Рекомендованный объем дискового пространства[3)] для хранения данных на срок до	
					90 дней[4)], Гбайт	180 дней[5)], Гбайт
1) Для оценки количества ОЗ сервера необходимо учитывать непосредственно подключенные ОЗ и ОЗ на подчиненных серверах, если сервер включен в иерархию. При этом ОЗ подчиненных серверов учитываются с коэффициентом 0,35. Итоговое количество ОЗ контролируемой сети определять по формуле: $(n+(0,35\sum(ni))$, где ni –количество ОЗ на подчинённых серверах; n – количество ОЗ непосредственно подключенных к серверу						
2) Для повышения отказоустойчивости функционирования решения в составе аппаратной платформы рекомендуется выделить системный раздел, рекомендуемый объем системного раздела – не менее 240 Гбайт						
3) Для снижения вероятности потери данных рекомендуется организация RAID-массива в конфигурации RAID1 + 1 диск Hot Spare. Возможно применение RAID-массивов, обладающих более высокой степенью надежности, в соответствии с условиями применения решения и/или требованиями заказчика						
4) Объем дискового пространства рекомендован для хранения данных (события, промежуточные версии конфигураций ОЗ) не менее 90 дней при указанной емкости контролируемой сети. При необходимости хранения больше чем 90 дней, рекомендуется использовать регулярную выгрузку на сторонние носители или рассчитывать объем хранилища по формуле ниже в примечании						
5) Объем дискового пространства рекомендован для хранения данных (события, промежуточные версии конфигураций ОЗ) не менее 180 дней при указанной емкости контролируемой сети. При необходимости хранения больше чем 180 дней, рекомендуется использовать регулярную выгрузку на сторонние носители или рассчитывать объем хранилища по формуле ниже в примечании						

Таблица 5 – Средние показатели параметров загрузки отчетов по типам устройств

Тип устройства	Среднее время загрузки, t (сек.)	Увеличение объема данных, V (Mb\час)
Network	120	0,05
ESXi	30	0,05
Unix	120	0,45
Windows	460	0,6

Таблица 6 – Средние значения коэффициента производительности сервера ПК

Размер контролируемой сети	Значение коэффициента (k)
Малая	0,25
Средняя	0,15
Большая	0,1

Примечание – В таблицах 5 и 6, для расчета минимального периода опроса контролируемых устройств и минимального объема свободного дискового пространства, приведены ориентировочные (приблизительные) значения параметров, которые могут изменяться в зависимости от технических характеристик используемой ЭВМ.

Для приблизительного расчета минимального периода загрузки отчетов с контролируемых на сервере ПК устройств можно воспользоваться следующей формулой:

$$(\sum t_n \cdot n) \cdot k,$$

где t_n – среднее время загрузки отчетов с контролируемого типа устройств (берется из таблицы 5);
n – количество контролируемых на сервере ПК устройств одного типа;
k – коэффициент производительности сервера ПК (берется из таблицы 6).

Например, для небольшой сети, в которой находится 15 сетевых устройств, 20 Unix-систем и 10 рабочих станций с ОС Windows, приблизительное время необходимое для загрузки отчетов на сервер ПК со всех контролируемых устройств составит:

$$(120 \cdot 15 + 120 \cdot 20 + 460 \cdot 10) \cdot 0{,}25 = 2200 \text{ сек} = 37 \text{ мин}$$

Для определения оптимальной периодичности автоматического выполнения операций с устройствами (загрузки отчетов по расписанию) необходимо:

1) После настройки комплекса и добавления всех контролируемых устройств на сервер ПК выполнить операцию загрузки отчетов со всех устройств.
2) Зафиксировать время, затраченное на загрузку отчетов со всех устройств.
3) К полученному времени добавить 20 процентов. Полученное значение установить в качестве периода времени между запусками расписания.
4) При добавлении на сервер ПК дополнительных устройств необходимо повторить п.1-3, корректируя установленную периодичность запуска расписания.

Свободное дисковое пространство ЭВМ, необходимое для установки только серверной части комплекса и внешних модулей, составляет 10 Гб.

При установке серверной части комплекса и сервера БД на одну ЭВМ минимальный объем свободного дискового пространства рассчитывается на основе данных, приведенных в таблице 5 и заданного при настройке параметров работы сервера ПК периода очистки БД (Т).

Для расчета необходимого минимального объема свободного дискового пространства для хранения данных комплекса в используемой БД нужно воспользоваться следующей формулой:

$$(\sum V_n \cdot n) \cdot T \cdot 24,$$

где V_n – среднее увеличение объема используемой БД в час в зависимости от типа контролируемых устройств (берется из таблицы 5);

n – количество контролируемых на сервере ПК устройств одного типа;
T – период очистки БД (устанавливается при настройке программного комплекса в клиентской консоли).

Например, для контролируемых на сервере ПК 15 сетевых устройств, 20 Unix-систем и 10 рабочих станций с ОС Windows и периода очистки БД в 30 дней, минимальный объем свободного дискового пространства составит приблизительно:

$$(0,05 \cdot 15 + 0,45 \cdot 20 + 0,6 \cdot 10) \cdot 720 = 11340\ Mb$$

Допускается установка серверной части ПК «Efros Config Inspector» v.4 на ЭВМ, функционирующие под управлением операционных систем:

- ОС специального назначения «Astra Linux Special Edition» v.1.6 (релиз «Смоленск»), v.1.7, сертификат соответствия № 2557 (выдан ФСТЭК России 27.01.2012 г.);
- ОС «РЕД ОС» Муром v.7.2, v.7.3, сертификат соответствия № 4060 (выдан ФСТЭК России 12.01.2019 г.);
- ОС серии Windows 64-разрядные (далее - ОС Windows (x64)):
  - Windows Server 2008R2 Foundation Edition SP1;
  - Windows Server 2008R2 Standard Edition SP1;
  - Windows Server 2008R2 Enterprise Edition SP1;
  - Windows Server 2008R2 Datacenter Edition SP1;
  - Windows Server 2012/2012R2 Foundation;
  - Windows Server 2012/2012R2 Essentials;
  - Windows Server 2012/2012R2 Standard;
  - Windows Server 2012/2012R2 Datacenter;
  - Windows Server 2016 Standard;
  - Windows Server 2016 Datacenter;
  - Windows Server 2016 Essentials;
  - Windows Server 2019 Standard;
  - Windows Server 2019 Datacenter;
  - Windows Server 2019 Essentials;
  - Windows Server 2022 Standard;
  - Windows Server 2022 Datacenter;
  - Windows Server 2022 Essentials;
  - Windows 7 Professional SP1;
  - Windows 7 Enterprise SP1;
  - Windows 7 Ultimate SP1;
  - Windows 8.1 Core;
  - Windows 8.1 Professional;
  - Windows 8.1 Enterprise;
  - Windows 10 Home;
  - Windows 10 Pro;
  - Windows 10 Enterprise;
  - Windows 11 Home;

- Windows 11 Pro;
- Windows 11 Enterprise.

Дополнительно на ЭВМ, с серверной частью ПК «Efros Config Inspector» v.4, под управлением ОС серии Windows должны быть установлены следующие программные средства:

- .NET Framework версии 4.7;
- СУБД (одна из, также поддерживаются новые версии указанных СУБД):
  - PostgreSQL: 11, 12, 13, 14, 15;
  - Microsoft SQL Server: 2016, 2017, 2019;
  - MySQL: 8.0;
  - защищенная СУБД «Jatoba» (сертификат соответствия № 4327 от 19.11.2020, выдан ФСТЭК России);
- SQL Server Native Client – при использовании СУБД MS SQL Server 2017, установленной на отдельном сервере баз данных;
- ПО Java (JRE) версия 1.8.0.

Для установки серверной части и внешних модулей ПК «Efros Config Inspector» v.4, на ЭВМ под управлением ОС «Astra Linux SE» и ОС «РЕД ОС», необходим следующий минимальный состав программных средств:

- СУБД (одна из, также поддерживаются новые версии указанных СУБД):
  - PostgreSQL: 11, 12, 13, 14, 15;
  - MySQL: 8.0;
  - защищенная СУБД «Jatoba» (сертификат соответствия № 4327 от 19.11.2020, выдан ФСТЭК России);
- ПО Java (JRE) версия 1.8.0;
- systemd (вер. 232 для ОС «Astra Linux SE», вер. 219 для ОС «РЕД ОС») - подсистема инициализации Linux для запуска служб и управления ими в процессе работы системы.

Перед установкой серверной части комплекса на англоязычные ОС следует установить Русский язык в качестве Языка системы для программ, не поддерживающих Юникод.

Для обеспечения взаимодействия контролируемых ОС Windows с сервером ПК в используемом брандмауэре должны быть открыты TCP-порты: на сервере ПК – 20002, а на контролируемых ОС – 20001.

СУБД может быть установлена локально на сервере ПК либо на удаленном компьютере и подключена к серверу ПК по сети. При подключении удаленной СУБД MySQL для обеспечения корректной работы необходимо, чтобы значение переменной max_allowed_packet сервера MySQL было не менее 512 Мб.

Для установки клиентской консоли ПК «Efros Config Inspector» v.4 ЭВМ должна иметь следующий минимальный состав технических и программных средств:

1. Аппаратное обеспечение:
   - процессор 2 CPU с тактовой частотой от 2,2 ГГц;
   - оперативная память 8 Гб;
   - свободное дисковое пространство 2 Гб;
   - сетевая карта 100/1000 Мбит/с Ethernet.
2. Программное обеспечение:
   - одна из ОС: ОС серии Windows x64 (аналогично серверной части (см. выше)) или ОС серии Windows x86 (перечень ОС аналогичен перечню ОС серии Windows x64 для серверной части (см. выше));
   - .NET Framework 4.7.

Для сетевого взаимодействия клиентской консоли с сервером программного комплекса на рабочих станциях с установленной клиентской консолью должен быть открыт 20000 TCP-порт.

Windows-агент ПК «Efros Config Inspector» v.4 функционирует под управлением 64-разрядных ОС серии Windows (перечень ОС аналогичен перечню ОС для серверной части). Дополнительно, в состав изделия входят портативные версии, не требующие установки, поддерживающие работу со следующими ОС:

- ОС серии Windows x86 (перечень ОС аналогичен перечню ОС серии Windows x64 для серверной части (см. выше));
- ОС Windows XP, Windows Vista, Windows 2003, Windows 2003 R2 x86;
- ОС Windows 2000 x86.

Минимальные требования к производительности рабочей станции:

- процессор с тактовой частотой 1,6 ГГц;
- ОЗУ объемом 1 Гб (1,5 Гб для работы на виртуальной машине);
- 100 Мб доступного пространства на жестком диске;
- сетевая карта Ethernet.

ВНИМАНИЕ: Корректная работа сервера ПК «Efros Config Inspector» v.4 обеспечивается только с версиями windows-агента 4.x, совместимость для более ранних версий windows-агента (например, 3.0 и 3.1) не поддерживается!

2.2. Условия эксплуатации

2.2.1. Перед эксплуатацией ПК «Efros Config Inspector» v.4 необходимо внимательно ознакомиться с комплектом эксплуатационной документации на него.

2.2.2. Установка компонентов комплекса должна осуществляться на ЭВМ защищаемой локальной вычислительной сети, расположенные в контролируемой зоне.

2.2.3. Установка компонентов комплекса должна выполняться в соответствии с руководством администратора.

2.2.4. Установка и эксплуатация комплекса должны выполняться только с действующей лицензией на использование, входящей в комплект поставки. Не допускается эксплуатация ПК «Efros Config Inspector» v.4 после истечения срока действия лицензии на использование. Изделие не выполняет функции защиты после истечения срока действия лицензии на использование.

2.2.5. Настройка параметров комплекса должна осуществляться в соответствии с документами:

– 643.72410666.00082-01 96 01-01. Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование»;

– 643.72410666.00082-01 96 01-02. Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 2. Настройки контроля»;

– 643.72410666.00082-01 96 01-03. Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 3. Работа с устройствами».

2.2.6. Администратор безопасности должен периодически проверять наличие обновлений ОС на официальном сайте разработчика и устанавливать их на эксплуатируемую ЭВМ.

2.2.7. После завершения установки и настройки комплекса должны быть приняты организационно-технические меры, исключающие бесконтрольный доступ к комплексу и техническим средствам ЭВМ.

2.2.8. Для корректного функционирования компонентов ПК «Efros Config Inspector» v.4, установленных на ЭВМ под управлением ОС серии Windows, при взаимодействии с установленным антивирусным ПО необходимо добавить в список исключений в настройках антивирусного ПО следующие программные модули комплекса:

– службу сервера (C:\Program Files\EFROS Config Inspector 4\Server\CIService.exe);

– клиентскую консоль (C:\Program Files (x86)\EFROS Config Inspector 4\Console\CIWPF.exe) либо (C:\Program Files\EFROS Config Inspector 4\Console\CIWPF.exe) в зависимости от разрядности используемого модуля и операционной системы;

– службу Windows-агента (C:\Program Files\EFROS Config Inspector 4\Agent\WAService.exe);

– службу коллектора задач (C:\Program Files\EFROS Config Inspector 4\Collector\CollectorService.exe).

2.2.9. Порядок настройки сетевого и серверного оборудования (в зависимости от производителя оборудования) для подключения его к серверу ПК по используемым протоколам указан в файле справки *Описание модулей.zip* (*Описание модулей.chm*), расположенном на дистрибутивном диске программного комплекса.

2.2.10. Должны быть установлены все актуальные обновления безопасности среды функционирования ПК «Efros Config Inspector» v.4. При эксплуатации комплекса в среде ОС Windows 7/2008R2/2012 обязательна установка расширенных обновлений безопасности в рамках программы технической поддержки Extended Security Updates Microsoft.

3. Описание решаемых комплексом задач

Активный аудит сетевого и серверного оборудования достигается в ПК «Efros Config Inspector» v.4 за счет решения следующих задач:

- контроль активного сетевого оборудования разных производителей;
- проверка серверных ОС (Windows, Unix-like);
- мониторинг состояния объектов виртуальных инфраструктур;
- запуск проверок по расписанию;
- отправка писем и уведомлений администратору комплекса;
- отправка извещений сторонним средствам мониторинга;
- прием и хранение Syslog-сообщений;
- аудит конфигураций контролируемых устройств по заданным профилям;
- конфигурирование устройств и групп устройств;
- восстановление конфигурации устройств;
- ведение журнала действий пользователей;
- возможность аутентификации на устройствах по протоколу SSH;
- контроль файлов ОС;
- создание стандартов и настройка требований проверок безопасности для устройств;
- создание стандартов и настройка требований проверок безопасности межсетевых экранов;
- сбор данных об уязвимостях контролируемого оборудования и ПО;
- построение иерархии серверов и настройка подключения подчиненных серверов;
- резервирование серверов.

Прежде чем решать ту или иную задачу, администратору безопасности необходимо выполнить настройку комплекса.

3.1. Контроль активного сетевого оборудования разных производителей

Для контроля устройств необходимо при помощи клиентской консоли выполнить операцию ***Загрузить***. Данная операция запускается из меню устройства в ***Панели списка устройств***.

Полный список действий при выполнении данной операции включает:

1) Загрузку на сервер ПК текстовых конфигураций контролируемых устройств (текстовых файлов, выводов команд).
2) Загрузку и формирование отчетов по настройкам, локальным файлам и параметрам работы контролируемых устройств.
3) Выполнение проверок наличия уязвимостей контролируемого оборудования.
4) Выполнение проверок соответствия конфигурации контролируемых устройств требованиям безопасности (compliance проверки).

3.2. Запуск проверок по расписанию

Решение данной задачи заключается в настройке расписания проверки контролируемого оборудования. Расписание проверки задается в ***Форме настройки расписаний загрузки отчетов*** раздела **Настройки** клиентской консоли.

После выполнения настройки контроль устройств будет осуществляться строго по указанному расписанию.

3.3. Отправка писем администратору

В ПК «Efros Config Inspector» v.4 поддерживается отправка писем администратору с сообщениями о произошедших на сервере ПК и контролируемых устройствах событиях по протоколу *SMTP*.

Решение задачи отправки писем заключается в настройке параметров отправки писем. Настройка выполняется в ***Форме подключения, отключения и настройки внешних модулей*** раздела **Настройки** клиентской консоли для модуля ***Отправка писем по протоколу SMTP***.

3.4. Отправка извещений сторонним средствам мониторинга

В ПК «Efros Config Inspector» v.4 поддерживается отправка уведомлений на внешний сервер по протоколу *Syslog*.

3.5. Аудит конфигураций контролируемых устройств по политикам

В ПК «Efros Config Inspector» v.4 поддерживается аудит контроля конфигураций по заданным профилям.

Решение данной задачи заключается в:

- создании профилей политик контроля;
- проверке рабочей конфигурации устройств при загрузке на выполнение правил;
- анализе выполненных и невыполненных условий.

Операции выполняются администратором комплекса в ***Форме управления профилями***, далее автоматически при загрузке отчетов.

3.6. Конфигурирование устройств и групп устройств

ПК «Efros Config Inspector» v.4 поддерживает функцию конфигурирования устройств типов Eltex MES, Eltex ESR, Cisco ASA, Cisco IOS, Cisco SMB, HP Comware, Huawei VRP, Marlin (Azimut), Dionis NX и Mikrotik (RouterOS).

Задача решается предоставлением пользователям доступа к конфигурированию отдельных устройств, поддерживающих данную функцию, в соответствии с установленными правами доступа. Пользователи получают возможность внесения изменений в конфигурацию контролируемых устройств путем выдачи команд

конфигурирования. Поддерживается сохранение/изменение/удаление списков команд конфигурирования, а также возможность автоматической генерации скрипта аутентификации (AAA) после ввода параметров аутентификации в отдельном диалоговом окне.

Примечание – Возможность генерации шаблона набора команд в окне ввода параметров в версии 4.14.100 ПК «Efros Config Inspector» v.4 поддерживается для следующих типов устройств: Eltex MES, Eltex ESR, Cisco ASA, Cisco IOS, Huawei VRP.

Операция может выполняться как для одного устройства, так и для группы устройств.

Операция выполняется администратором с полным доступом или пользователями с доступом для выполнения операций на корневой группе устройств.

3.7. Восстановление конфигурации устройств

В ПК «Efros Config Inspector» v.4 для типов устройств Eltex MES, Eltex ESR, Cisco ASA, Cisco IOS, Cisco SMB, HP Comware, Huawei VRP, Marlin (Azimut), Dionis NX и Mikrotik (RouterOS) решена задача восстановления конфигурации путем загрузки ранее сохраненных файлов конфигураций (эталонов) из архива ПК «Efros Config Inspector» v.4. В ходе восстановления возможно сравнение эталонной и текущей конфигурации устройства. Запуск восстановления конфигурации реализован на вкладке ***Статус*** раздела **Устройства**.

3.8. Ведение журнала действий пользователей

В ПК «Efros Config Inspector» v.4 поддерживается фильтрация журнала событий по действиям различных пользователей комплекса.

Решение задачи просмотра журнала действий пользователя заключается в настройке фильтра. Настройка выполняется в разделе **События** путем фильтрации событий по типу события ***Аудит*** по условию ***Пользователь***.

3.9. Возможность аутентификации по протоколу SSH при подключении к устройствам

В ПК «Efros Config Inspector» v.4 при подключении к устройствам поддерживается протокол SSH версии 2.0.

Данная настройка доступна для ряда устройств – в свойствах контролируемого устройства есть возможность указать необходимый протокол взаимодействия.

3.10. Контроль файлов ОС

В ПК «Efros Config Inspector» v.4 поддерживается функция контроля целостности файлов операционной системы контролируемых устройств по требованию пользователя.

Данная функциональная возможность реализована во вкладке ***Конфигурации*** формы настройки профилей раздела **Настройки** и настраивается путем создания пользовательских отчетов для операционной системы контролируемого оборудования, в которых перечислены полные пути к контролируемым файлам или указаны маски для типов контролируемых объектов. Пользователь может как вручную выбрать контролируемые файлы, так и для некоторых ОС воспользоваться встроенными шаблонами ПК «Efros Config Inspector» v.4.

3.11. Формирование пользовательских стандартов и настройка требований проверок безопасности для устройств

В ПК «Efros Config Inspector» v.4 реализована возможность формирования пользовательских стандартов проверок безопасности на основании базы проверок CIS, существующих пользовательских проверок (включая проверки с помощью регулярных выражений), а также путем копирования и последующего редактирования проверок, в том числе задания и редактирования исключений. При добавлении пользовательских стандартов возможен импорт настроек и требований пользовательского стандарта проверки безопасности из файла формата XML, а также добавление нового стандарта путем выбора требований из базы требований, формируемой из предустановленных требований при подключении внешних модулей оборудования или путем копирования из ранее добавленных стандартов.

Данная функциональная возможность реализована во вкладке **Проверки безопасности** раздела **Настройки.**

3.12. Универсальный отчет правил межсетевых экранов

В ПК «Efros Config Inspector» v.4 для межсетевых экранов реализована возможность формирования универсального отчета «Правила МЭ», содержащего установленные на МЭ различных типов правила в удобном для пользователя виде. Отчет для различных типов МЭ выводится в едином стиле. В таблице 7 приведен перечень столбцов отчета с указанием для поддерживаемых типов МЭ наличие данных в столбце. В таблице 8 приведен перечень отображаемых для различных типов МЭ данных в столбце «Additional».

В таблицах использованы следующие условные обозначения:

- **«-»** – не поддерживается устройством;
- «нет» – не реализовано;
- «да»' – реализовано.

Таблица 7 – Возможности отчета «Правила МЭ»

Устройство	Number	Name	Protocol	Source	Source Port	Destination	Destination Port	Service	Description (remark)	Hit Count	Статус (enable/disable)	Additional
Cisco ASA	нет	-	да	да	да	да	да	-	да	да	да	да
Cisco ASA Context	нет	-	да	да	да	да	да	-	да	да	да	да
Cisco PIX	нет	нет	да	да	да	да	да	-	да	да	да	да
Cisco Firepower Device	да	да	-	да	да	да	да	-	да	да	да	да
Cisco FTD с контролем файлов по SSH	да	да	-	да	да	да	да	-	да	да	да	да
Cisco IOS	нет	-	да	да	да	да	да	-	да	нет	-	да
Huawei VRP	-	-	да	да	да	да	да	-	-	-	-	да
Eltex ME	нет	нет	нет	нет	нет	нет	нет	нет	нет	нет	нет	нет
Eltex MES	-	-	да	да	да	да	да	-	-	да	-	да
Eltex ESR	-	-	да	да	да	да	да	-	-	нет	да	да
Dionis NX 1.1	-	-	да	да	да	да	да	-	да	нет	да	да
Dionis NX 1.2	-	-	да	да	да	да	да	-	да	нет	да	да
Dionis-NX 2.0	-	-	да	да	да	да	да	-	да	нет	да	да
Fortinet FortiGate	да	да	-	да	-	да	-	да		да	да	да
Fortinet FortiGate VDOM	да	да	-	да	-	да	-	да		да	да	да
UserGate UTM 5	да	да	-	да	-	да	-	да	-		да	да
UserGate UTM 6	да	да	-	да	-	да	-	да	-		да	да
ViPNet Coordinator HW	да	да	-	да	-	да	-	да	да	-	да	да
ViPNet xFirewall	кда	да	-	да	-	да	-	да	да	-	да	да
Marlin	да	да	-	да	-	да	-	да	-	-	да	да
S-Terra VPN Gate	-	-	да	да	да	да	да	-	да	-	-	да
Check Point Gateway	да	да	-	да	-	да	-	да	да	да	да	да
Check Point GAiA с контролем файлов по SSH	да	да	-	да	-	да	-	да	да	да	да	да
Check Point GAiA Embedded с контролем файлов по SSH	да	да	-	да	-	да	-	да	да	да	да	да
Полигон Арлан												
Полигон ИнЗер												
Mikrotik RouterOS												
HP												
Linux												

Таблица 8 – Возможности колонки «Additional»

Устройство	Inbound Interface	Outbound Interface	Application	User	Last change	Time Range	Logging
Cisco ASA	-	-		Да	Да	Да	
Cisco ASA Context	-	-		Да	Да	Да	
Cisco PIX	-	-					
Cisco Firepower Device	-	-	Да				
Cisco FTD с контролем файлов по SSH	-	-	Да				
Cisco IOS	-	-					
Huawei VRP	-	-					
Eltex ME	нет	нет					
Eltex MES	-	-					
Eltex ESR	-	-					
Dionis NX 1.1	-	-					
Dionis NX 1.2	-	-					
Dionis-NX 2.0	-	-					
Fortinet FortiGate	да	да		Да	Да	Да	
Fortinet FortiGate VDOM	да	да		Да	Да	Да	
UserGate UTM 5	да	да					
UserGate UTM 6	да	да					
ViPNet Coordinator HW	-	-					
ViPNet xFirewall	-	-					
Marlin	да	да					
S-Terra VPN Gate	-	-					
Check Point Gateway	-	-		Да	Да	Да	
Check Point GAiA с контролем файлов по SSH	-	-		Да	Да	Да	
Check Point GAiA Embedded с контролем файлов по SSH	-	-		Да	Да	Да	
Полигон Арлан							
Полигон ИнЗер							
Mikrotik RouterOS							
HP							
Linux							
SNR						Да	

3.13. Зонный анализ на основе требований разрешения и запрета трафика

Для межсетевых экранов типов CheckPoint, Dionis NX, Cisco ASA, Cisco FMC, Cisco PIX, Cisco IOS, Eltex MES, Huawei VRP, Fortinet FortiGate, Usergate и Marlin (Azimut) реализована возможность анализа движения трафика по зонам (подсетям). Анализ фильтрации трафика выполняется на основании заданных пользователем подсетей (источник, адресат), портов, протоколов и исключений. В результате формируется отчет, демонстрирующий запрещенные и разрешенные протоколы.

Данная функциональная возможность реализована во вкладке **Проверки межсетевых экранов** раздела **Настройки.**

3.14. Формирование стандартов безопасности и контроль наличия/отсутствия политик и правил МЭ

В ПК «Efros Config Inspector» v.4 реализована возможность формирования стандартов безопасности для контроля наличия/отсутствия политик и правил МЭ путем создания списков требований стандартов вручную, копированием имеющихся требований, выбора требований из базы требований существующих стандартов.

Проверка МЭ в соответствии с требованиями выполняется по параметрам: тип проверки (*Содержит*, *Не содержит*), тип учитываемых действий в правиле (*Не учитывать*, *Permit*, *Deny*), учитываемые протоколы и порты (*Не учитывать, Any, Значение*), учитываемые адреса источников и адреса назначения (*Не учитывать, Any, Зона, Подсеть (*для параметра *Подсеть* может быть установлен флаг *Адрес устройства)*), учитываемые приложения (*Не учитывать, Значение*) наличие/отсутствие комментария.

После активации стандарта безопасности путем разрешения его использования на устройствах, для устройств в разделе **Устройства** становится доступен отчет по политикам и правилам, удовлетворяющим заданным в требованиях стандарта параметрам.

Данная функциональная возможность реализована во вкладке ***Проверки межсетевых экранов*** раздела **Настройки.**

3.15. Оптимизация правил межсетевых экранов

Механизм анализа правил межсетевых экранов ПК «Efros Config Inspector» v.4 выявляет избыточные и «теневые» правила МЭ типов CheckPoint, Dionis NX, Cisco ASA, Cisco FMC, Cisco PIX, Cisco IOS, Eltex MES, Huawei VRP, Fortinet FortiGate, Usergate и Marlin (Azimut). Избыточными считаются полностью или частично дублированные правила. «Теневые» правила не выполняются в силу вышестоящих правил с обратным действием, несут потенциальную угрозу безопасности. Итоговые отчеты содержат рекомендации по оптимизации правил МЭ.

Для устройств, поддерживающих подсчет Hit Count (число случаев выполнения правил МЭ) в отчете по оптимизации правил учитываются также «Неиспользуемые» правила – правила, Hit Count которых не изменялся в течении заданного в

настройках отчета периода, и «Нулевые» правила – правила, значения Hit Count для которых равен «0».

3.16. Сбор данных об уязвимостях контролируемого оборудования и ПО

В ПК «Efros Config Inspector» v.4 реализовано обновление базы уязвимостей путем обмена через программный интерфейс с сервером, содержащим БДУ, об известных уязвимостях в формализованном унифицированном виде. Полученные сведения об уязвимостях представляются по устройствам и программному обеспечению в виде отчета об уязвимостях, а также по типам устройств на вкладке ***База уязвимостей*** раздела **Настройки**.

В отчетах по уязвимостям устройств раздела **Устройства** и в пользовательских отчетах типа ***Уязвимости устройств*** раздела **Отчеты** реализована возможность скрытия/активирования уязвимостей для одного устройства или группы устройств.

3.17. Построение иерархии серверов

В ПК «Efros Config Inspector» v.4 реализована функция построения иерархии серверов ПК, добавление новых серверов, настройка режима работы подчиненных серверов и доступа пользователей к ним. Для успешного построения иерархии, все сервера ПК, включаемые в иерархию, должны иметь одинаковую версию (мажорную и минорную). Например, управляющий и подчиненный сервер ПК в иерархии должны быть версии 4.14.

Также в **форме настройки иерархии** (открывается при переходе по ссылке **Иерархия** в разделе **Настройка**), при добавлении нового сервера ПК, возможна настройка ограничения скорости при работе с подчиненными серверами. В разделе **Устройства** одновременно могут отображаться данные не более чем с трех одновременно подключенных серверов ПК (по выбору пользователя).

3.18. Резервирование серверов ПК

В случае выхода из строя основного сервера ПК предусмотрено переключение выполнения всех функций резервным сервером ПК. Для работы системы резервирования необходимо наличие в лицензии ПК «Efros Config Inspector» v.4 модуля **Поддержка резервирования**. Для настройки резервирования серверная часть ПК «Efros Config Inspector» v.4 устанавливается на новый компьютер (под управлением ОС того же типа, что и для основного сервера ПК), выполняется настройка подключения сервера ПК к используемой БД комплекса. Список резервных серверов доступен для просмотра из раздела **Настройки** клиентской консоли комплекса.

В случае сбоя основного сервера ПК, модули и настройки серверной части будут доступны на резервном сервере ПК.

4. Входные и выходные данные

4.1. Входные данные

Входными данными для ПК «Efros Config Inspector» v.4 являются:

1) ***настройки:***

– сетевых устройств, серверов, виртуальных инфраструктур и групп данных объектов;

– ПК «Efros Config Inspector» v.4 (настройки работы служб, сервера баз данных, отправки писем и извещений и др.);

2) ***данные (состав принимаемых данных зависит от состава включенных при настройке комплекса внешних модулей):***

– принятые по протоколу Telnet, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc854);

– принятые по протоколу SSH, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc4251);

– принятые по протоколу SCP;

– принятые по протоколу HTTPS, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc2818);

– принятые по протоколу TLS, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc2246);

– принятые Syslog сообщения, формат данных в соответствии со спецификацией (https://tools.ietf.org/html/rfc3164);

– принятые по протоколу SNMP, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc1155);

– принятые по протоколу VIX API (при работе с VMWare vCenter), формат данных в соответствии со спецификацией для протокола (https://www.vmware.com/support/developer/vix-api/guestOps50_technote.pdf);

– принятые по протоколу WMI (при работе с Hyper-V), формат данных в соответствии со спецификацией для протокола (https://docs.microsoft.com/ru-ru/windows/win32/wmisdk/wmi-start-page);

– принятые по протоколу WinRM (при работе с Hyper-V), формат данных в соответствии со спецификацией для протокола (https://docs.microsoft.com/en-us/windows/win32/winrm/portal);

– принятые по протоколу SMB (при работе с Hyper-V), формат данных в соответствии со спецификацией для протокола (https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-SMB2/%5bMS-SMB2%5d.pdf);

– принятые по протоколу AXL API (при работе с CISCO UCM), формат данных в соответствии со спецификацией для протокола (https://developer.cisco.com/docs/axl/#!what-is-axl/what-is-administrative-xml);

– принятые по протоколу CPMI (при работе с устройствами CheckPoint), формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc3862);

– принятые по протоколу REST (при работе с устройствами Cisco ACS, Cisco Firepower, CheckPoint R80, Скала-Р);

– принятые по протоколу XenAPI (при работе с устройствами Citrix XenServer), формат данных в соответствии со спецификацией для протокола (https://xapi-project.github.io/xen-api/basics.html);

– принятые по протоколу LDAP (при контроле ActiveDirectory), формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc4510);

– принятые по протоколу SNMP (при сканировании сети), формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc1155);

– принятые по протоколу Microsoft TDS;

– принятые по протоколу Oracle .Net;

– принятые по протоколу PostgreSQL protocol;

– принятые по протоколу Firebird Wire Protocol;

– принятые по протоколу MySQL;

– принятые по протоколу XML-RPC;

– принятые по протоколу DioNIS Control Protocol (DCP).

4.2. Выходные данные

Выходными данными для ПК «Efros Config Inspector» v.4 являются:

1) ***сохраненные в базе данных отчеты о конфигурации и состоянии контролируемых устройств;***

2) ***данные (состав выходных данных зависит от состава включенных при настройке комплекса внешних модулей):***

– переданные по протоколу Telnet, формат данных в соответствии со спецификацией для протокола (https://courses.cs.washington.edu/courses/cse461/14sp/homework/rfc854-modified.html);

– переданные по протоколу SSH, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc4251);

– переданные по протоколу SCP;

– принятые по протоколу HTTPS, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc2818);

– переданные по протоколу TLS формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc2246);

– переданные по протоколу SMTP, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc5321);

– переданные по протоколу Microsoft Exchange Web Services Managed API (при отправке через MS Exchange), формат данных в соответствии со спецификацией для протокола (https://docs.microsoft.com/ru-ru/exchange/client-developer/exchange-web-services/explore-the-ews-managed-api-ews-and-web-services-in-exchange);

– переданные по протоколу Microsoft Unified Communications Managed API (при отправке сообщений в MS Lync), формат данных в соответствии со спецификацией для протокола (https://docs.microsoft.com/en-us/skype-sdk/ucma/ucma-5-0-general-reference);

– переданные по протоколу Syslog, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc3164);

– переданные по протоколу SNMP, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc1155);

– переданные по протоколу VIX API (при работе с VMWare vCenter), формат данных в соответствии со спецификацией для протокола (https://pubs.vmware.com/vi-sdk/visdk250/ReferenceGuide/);

– переданные по протоколу WMI (при работе с Hyper-V), формат данных в соответствии со спецификацией для протокола (https://docs.microsoft.com/ru-ru/windows/win32/wmisdk/wmi-start-page);

– переданные по протоколу WinRM (при работе с Hyper-V), формат данных в соответствии со спецификацией для протокола (https://docs.microsoft.com/en-us/windows/win32/winrm/portal);

– переданные по протоколу AXL API (при работе с CISCO UCM), формат данных в соответствии со спецификацией для протокола (https://developer.cisco.com/docs/axl/#!what-is-axl/what-is-administrative-xml);

– переданные по протоколу CPMI (при работе с устройствами CheckPoint), формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc3862);

– переданные по протоколу XenAPI (при работе с устройствами Citrix XenServer), формат данных в соответствии со спецификацией для протокола (https://xapi-project.github.io/xen-api/basics.html);

– переданные по протоколу LDAP (при контроле ActiveDirectory), формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc4510);

– переданные по протоколу REST (при работе с устройствами Cisco ACS, Cisco Firepower, CheckPoint R80, Скала-Р);

– переданные по протоколу Microsoft TDS;

– переданные по протоколу Oracle .Net;

– переданные по протоколу PostgreSQL protocol;

– переданные по протоколу Firebird Wire Protocol;

– переданные по протоколу MySQL;

– переданные по протоколу XML-RPC;

– переданные по протоколу DioNIS Control Protocol (DCP).

Перечень сокращений

HTTP (HyperText Transfer Protocol)	–	протокол прикладного уровня передачи данных. Основой HTTP является технология «клиент-сервер»
HTTPs (HyperText Transfer Protocol Secure)	–	расширение протокола HTTP
Syslog	–	стандарт отправки сообщений о происходящих в системе событиях
SSH (Secure Shell)	–	сетевой протокол прикладного уровня
SSL (Secure Socket Layer)	–	протокол, обеспечивающий безопасную связь
TELNET (TELecommunication NETwork)	–	сетевой протокол для реализации текстового интерфейса по сети, в качестве транспорта используется TCP
TLS (Transport Layer Security)	–	протокол, обеспечивающий защищенную передачу данных в сети
АСУ ТП	–	автоматизированная система управления технологическим процессом
БД	–	база данных
БДУ	–	база данных уязвимостей
МЭ	–	межсетевой экран
ОЗ	–	объект защиты
ОС	–	операционная система
ПК	–	программный комплекс
ПО	–	программное обеспечение
СУБД	–	система управления базами данных
ЭВМ	–	электронно-вычислительная машина

Термины и определения

Отчет – загружаемые с устройств данные, а также результаты обработки загруженных данных, являются отчетами типа ***Отчет***, ***Текстовый отчет***. Результат проверки данных на соответствие заданным правилам – отчет типа ***Отчет о проверке***

Проверка – отчет, сформированный ПК «Efros Config Inspector» v.4 по результатам проверки загруженных или выбранных данных на соответствие заданным правилам

Профиль – поименованная совокупность настроек параметров контроля устройств, отчетов и проверок, доступных для устройств

Событие – зафиксированное в журнале программы действие сервера ПК или пользователей программы

Статус – интерфейс, на котором отображены важные оповещения по ситуации и выведены основные операции с контролируемыми устройствами