ГАЗИНФОРМ СЕРВИС

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

Руководство пользователя
Часть 3

Работа с устройствами

Санкт-Петербург 2023

Аннотация

В документе приведены сведения с описанием режимов работы программного комплекса управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4 (далее по тексту – ПК «Efros Config Inspector» v.4 или комплекс), принципов безопасной работы комплекса, функций и интерфейсов функций комплекса, параметров (настроек) безопасности комплекса, доступных пользователям, и их безопасных значений, типов событий безопасности, связанных с доступными пользователю функциями комплекса, а также действий пользователей после сбоев и ошибок.

Настоящее руководство предназначено для всех пользователей ПК «Efros Config Inspector» v.4.

Содержание

1. Назначение программного комплекса

ПК «Efros Config Inspector» v.4 предназначен для активного контроля сетевого оборудования, серверных и клиентских операционных систем (ОС), систем управления базами данных (СУБД), автоматизированных систем управления технологическим процессом (АСУ ТП), виртуальных сред, а также анализа правил межсетевых экранов производства компаний:

- Cisco Systems, Inc. (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, UCM 10.0, UCM 8.5, Unified Phone 78xx, Unified Phone 88xx);
- 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);
- 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 (AIX, SunOS, HP-UX, CentOS, AltLinux, Red Hat, Debian, Manjaro, Ubuntu, Mint, Fedora, FreeBSD, Red OS, Astra Linux, RHEL);
- ОС Microsoft Windows (xp, vista, 7, 8, 10, 2000, 2003, 2008r2, 2012, 2012r2, 2016, 2019);
- Virtual Machine Manager, Hyper-V (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));
- 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 5, 6, 7);
- 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 компаний, оборудование которых может быть подключено для контроля к комплексу, может быть расширен за счет разработки и включения в ПК «Efros Config Inspector» v.4 соответствующего внешнего модуля.

Программный комплекс обеспечивает выполнение следующих функций:

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 базы данных уязвимостей (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, включающий 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 сервером ПК задач.

10) Формирование и просмотр пользовательских отчетов:

– создание пользовательских отчетов для нескольких выбранных устройств на основе отчетов, загруженных с этих 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 базе данных (БД) с возможностью настройки сроков хранения оперативной информации;

– бэкапирование данных средствами СУБД с возможностью восстановления БД;

– резервирование серверов.

В рамках выполнения функций комплекс решает следующие задачи:

- контроль активного сетевого оборудования разных производителей;
- проверка серверных операционных систем (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 целостности 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.

1.1. Структура и режимы работы 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.

[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

Сервер ПК обеспечивает выполнение основных функций ПК по контролю сетевого оборудования, серверных и клиентских ОС, АСУ ТП, виртуальных сред, а также анализу правил межсетевых экранов и функций по настройке комплекса:

- проверка/создание БД на сервере БД;
- подключение к контролируемым устройствам, windows-агентам, коллекторам задач и серверам иерархии.

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

- 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):
  - 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.

Клиентская консоль подключается к серверу ПК по протоколу TLS и может работать одновременно на нескольких компьютерах. Допускается установка клиентской консоли ПК «Efros Config Inspector» v.4 на ЭВМ, функционирующие под управлением ОС серии Windows.

Клиентская консоль предоставляет графический интерфейс для управления комплексом при выполнении 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 списков устройств и групп устройств;
   - контроль текущих статусов устройств (просмотр уведомлений о событиях, зафиксированных для устройств, операциях, выполненных с устройствами, и архива отчетов о событиях и операциях);
   - 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 этих устройств, с возможностью сохранения параметров отчета в виде шаблона отчета.

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

5) Настройка комплекса:

а) настройки серверной части комплекса:
   - задание триггеров для обработки событий системы и устройств;
   - 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: 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».

Внешние модули и windows-агент соединяют сервер с устройствами по различным коммуникационным протоколам.

Коллектор задач (далее по тексту – коллектор) ПК «Efros Config Inspector» v.4 подключается к серверной части программного комплекса. При наличии большого количества задач сервера ПК (например, загрузка отчетов), часть задач передается на выполнение коллектору.

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.

Подробные сведения о технических и программных средствах, обеспечивающих выполнение программы приведены в документе 643.72410666.00082-01 95 01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство администратора».

1.1.1. Обработка отчетов

Отчеты в ПК «Efros Config Inspector» v.4 формируются путем загрузки с контролируемых 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.

ПК «Efros Config Inspector» v.4 позволяет создавать для загрузки с устройств пользовательские отчеты и отчеты типа *Фильтр*, 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 с правами *Управление* в категории ***Настройки контроля*** при настройке проверок МЭ могут быть созданы стандарты безопасности, содержащие требования для контроля наличия/отсутствия правил МЭ по заданным параметрам, и назначены устройства, в списке отчетов которых в разделе **Устройства** будет доступен отчет по созданному стандарту безопасности.

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

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

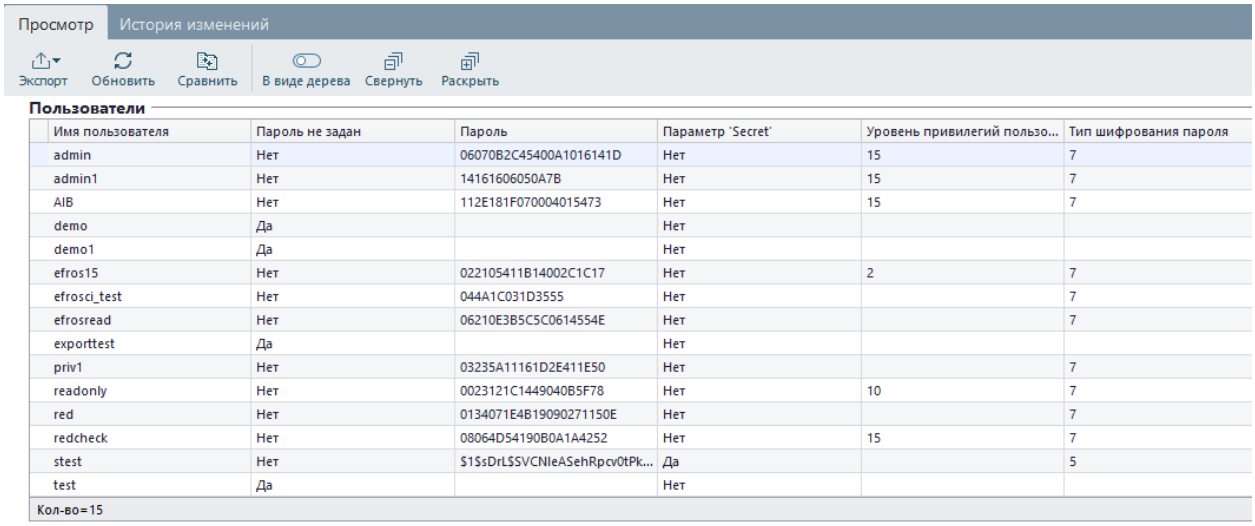
Данные отчетов, загруженных с устройств, могут быть экспортированы в файл формата TXT (текстовые отчеты) и XML, HTML (структурированные отчеты).

На рисунке 1 приведены примеры представлений отчета, содержащего список пользователей, извлеченных из конфигурационного файла Cisco IOS.

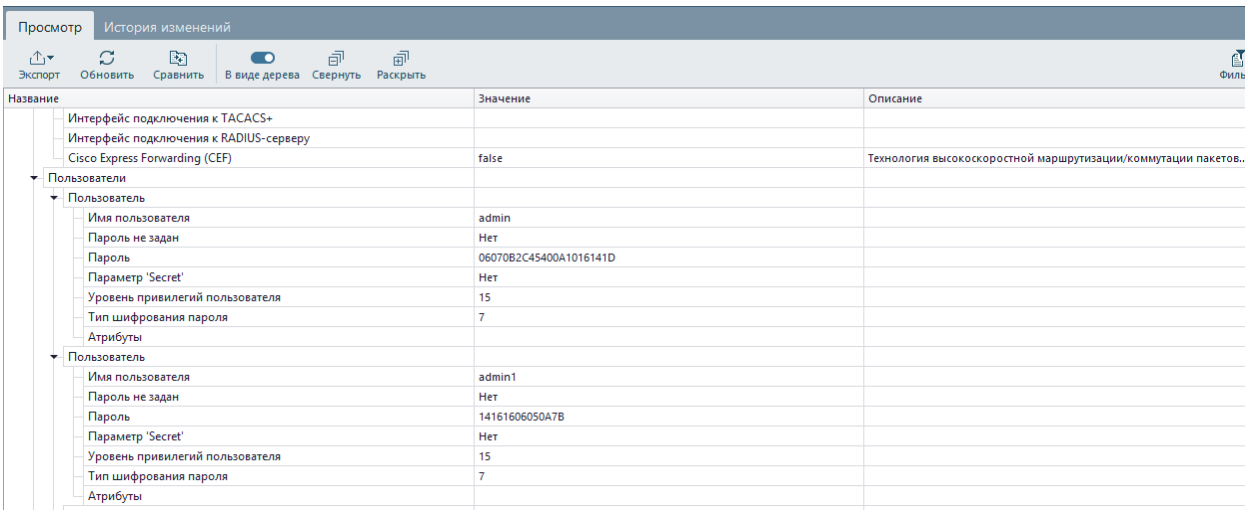
Поддерживается также возможность создания на основе отчетов, загруженных с устройств, пользовательских отчетов в разделе **Отчеты** для нескольких выбранных устройств. Поддерживаются следующие типы пользовательских отчетов:

- ***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 и нулевых правил МЭ для устройств заданных типов.



а)



б)

Рисунок 1 – Примеры представлений отчета

Примечание – Избыточными считаются полностью или частично дублированные правила. «Теневые» правила не выполняются в силу вышестоящих правил с обратным действием, несут потенциальную угрозу безопасности. «Неиспользуемые» правила – правила, Hit Count (число случаев выполнения правила) которых не

изменялся в течении заданного в параметрах отчета периода. «Нулевые» правила – правила, значения Hit Count для которых равен «0».

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

1.1.2. Проверки

Проверки добавляются в комплекс вместе с подключением внешних модулей работы с устройствами, для которых они предназначены. При добавлении проверки задаются: описание проверки и преобразование для формирования отчета о проверке из базовых отчетов.

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.

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.

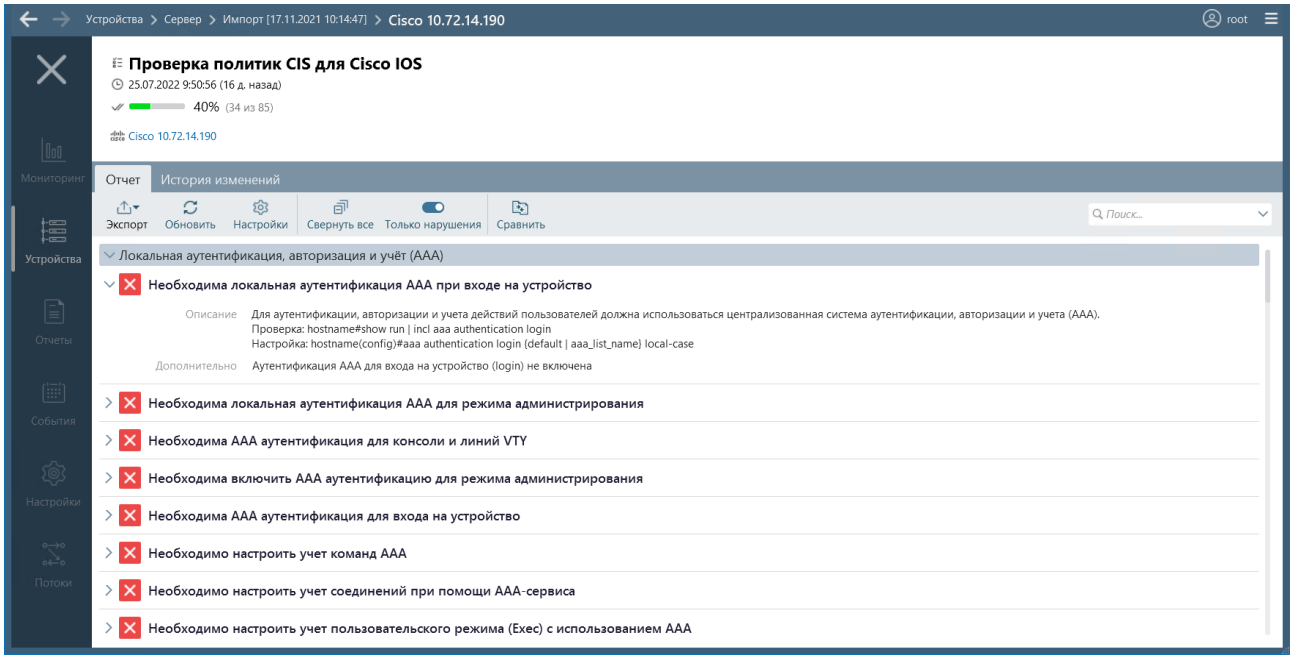


Рисунок 2 – Отчет о результате проверки

1.1.3. Сбор, обработка событий

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

События могут регистрироваться как самим комплексом (например, при загрузке отчета), так и внешними модулями (например, Syslog-сообщения).

При этом комплекс поддерживает динамическое добавление новых типов событий. При добавлении новых типов событий указываются поля. 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 отчёта 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 о полях событий могут использоваться для задания условий как при фильтрации (рис. 3), так и при настройке обработчиков событий (триггеров) (рис. 4).

Пользователи ПК «Efros Config Inspector» v.4 с правами *Управление* категории *Настройки контроля* (см. п. 1.2 «Пользователи ПК «Efros Config Inspector» v.4») имеют возможность создания обработчиков событий (триггеров).

Для задания условий при настройке обработчика событий пользователь может выбирать типы событий и задавать условия к их полям. При задании реакций поддерживаются следующие действия:

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

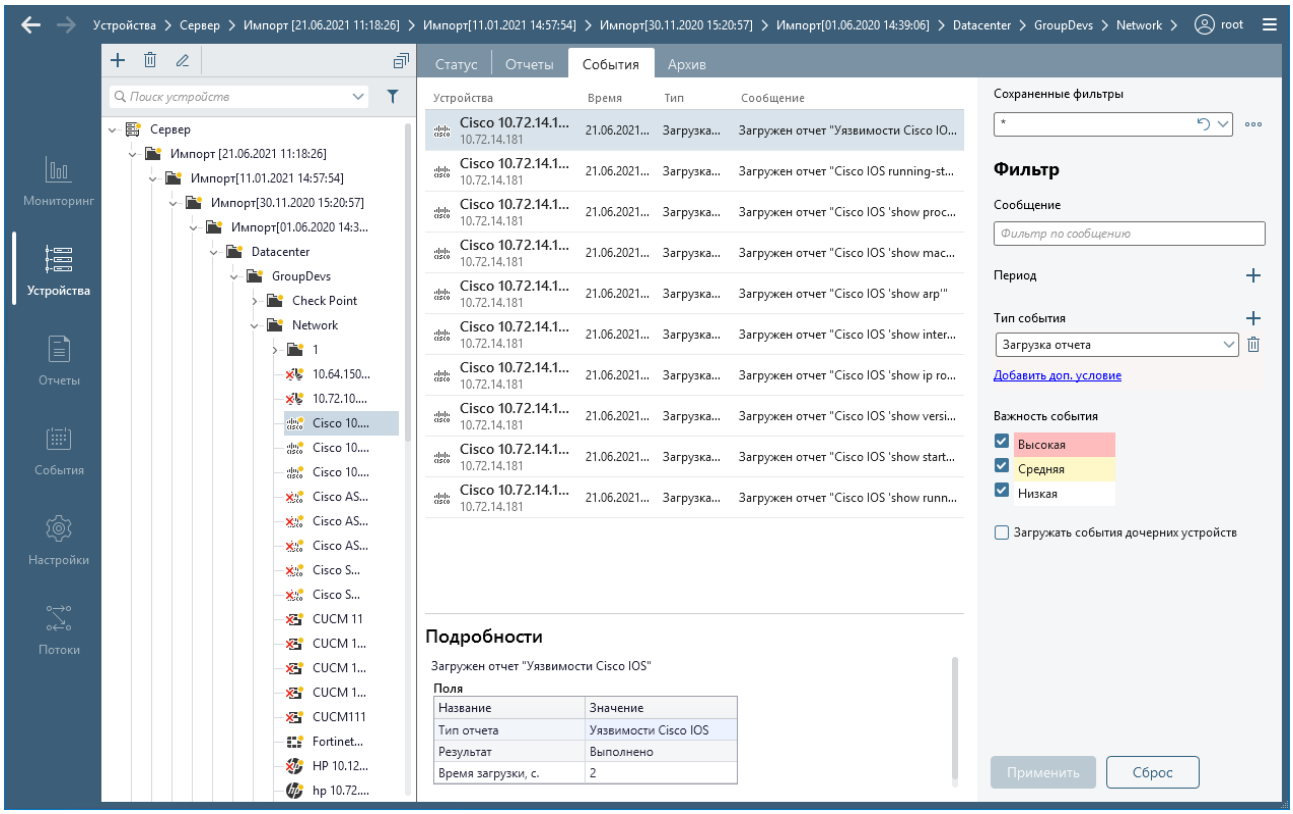


Рисунок 3 – Фильтрация событий

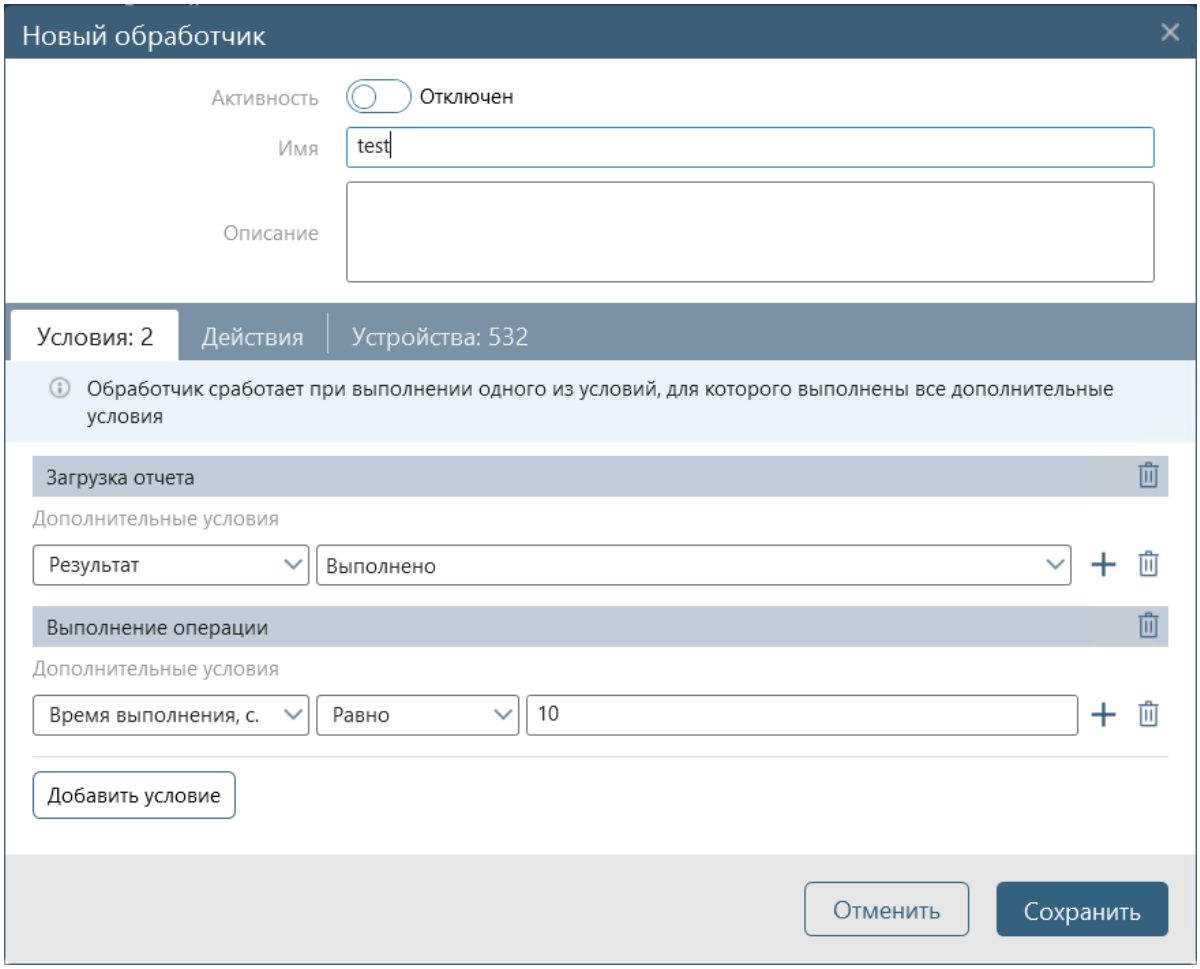


Рисунок 4 – Задание условий при настройке обработчика событий

1.1.4. 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).

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

Операции управления устройствами в ПК «Efros Config Inspector» v.4 могут выполняться:

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

1.1.5. Конфигурирование устройств/групп устройств и восстановление конфигурации устройств

ПК «Efros Config Inspector» v.4 поддерживает функцию конфигурирования устройств. В комплексе пользователям предоставляется доступ 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. Операция может выполняться как для одного устройства, так и для группы устройств.

Для устройств типов Eltex MES, Eltex ESR, Cisco ASA, Cisco IOS и Huawei VRP пользователям предоставляется возможность генерации шаблона набора команд (скрипта для настройки AAA) в окне ввода параметров конфигурирования. Скрипт доступен пользователю для корректировки, сохранения в шаблон и выполнения.

В ПК «Efros Config Inspector» v.4 для отдельных типов устройств доступно восстановление конфигурации путем загрузки ранее сохраненных файлов конфигураций (эталонов) из архива комплекса. В ходе восстановления возможно сравнение эталонной и текущей конфигурации устройства.

Операции конфигурирования/восстановления конфигурации выполняются пользователями с доступом для выполнения операций на корневой группе устройств.

1.2. Пользователи ПК «Efros Config Inspector» v.4

Пользователями ПК «Efros Config Inspector» v.4 являются должностные лица с правами настройки и контроля сетевого и серверного оборудования организации, эксплуатирующей комплекс.

Разграничение доступа пользователей к функциональным возможностям настройки ПК «Efros Config Inspector» v.4 обеспечивается назначением в учетных записях пользователей прав доступа к функциям комплекса двух категорий:

1) ***Настройки контроля*** – включает:
   - настройка обработчиков событий;
   - настройка профилей (параметров контроля устройств);
   - действия с устройствами (просмотр карты сети, настройка доступности устройств);
   - настройка расписаний;
   - настройка профилей подключений (учетных записей подключения к устройствам);
   - настройка стандартов проверок безопасности;
   - экспорт настроек системы;
   - импорт настроек системы;
   - сканирование сети;
   - настройка стандартов безопасности межсетевых экранов.
2) ***Администрирование*** – администрирование сервера ПК, включает:
   - управление лицензиями;
   - изменение и управление списком внешних модулей;
   - управление учетными записями пользователей и группами пользователей;
   - задание параметров хранения отчетов и событий;
   - просмотр списка резервных серверов ПК;

- просмотр списка задач ПК «Efros Config Inspector» v.4;
- управление распределением нагрузки (подключение коллекторов);
- настройка иерархии серверов ПК;
- настройка параметров подключения к базе данных уязвимостей (БДУ) и обновление БДУ;
- настройка подключения к БДУ через прокси-сервер;
- настройка и проверка подключения к серверу «Efros Security Center Flow Server»

Пользователи, которым назначены права:

- *Нет доступа* – не имеют доступа к страницам соответствующих функций комплекса;
- *Просмотр* – имеют доступ к страницам для просмотра данных без возможности внесения изменений;
- *Управление* – имеют полный доступ к данным соответствующих страниц.

Все пользователи комплекса (с правами доступа к администрированию и настройкам контроля и без них) имеют доступ к функциям комплекса по работе с устройствами и по формированию и просмотру пользовательских отчетов (на основе личных шаблонов отчетов).

Доступ пользователей к конкретным устройствам зависит от назначенных им администратором комплекса прав доступа. Перечень и описание назначаемых пользователям прав доступа приведен в таблице 1.

Таблица 1 – Перечень и описание прав доступа пользователей к устройствам

Право доступа	**Описание**
Нет доступа	– полное отсутствие доступа пользователя к устройству
Чтение (просмотр, загрузка отчетов)	– доступ к устройству, просмотр настроек; – просмотр уведомлений; – просмотр отчетов; – просмотр событий; – загрузка и обновление отчетов[1)] (отключаемая опция на уровне настроек пользователей); – проверка подключения (доступности)
Полный доступ (изменение настроек)[2)]	– добавление устройств; – изменение параметров устройств; – изменение настроек контроля устройств; – выполнение операций с устройствами. Например, операции: добавить пользователя или скопировать running в startup для устройств Cisco IOS, конфигурировать, восстановить конфигурацию

[1)] Загрузка и обновление отчетов доступны пользователям с правами *Чтение* – только при отключенном режиме *Запретить загрузку конфигураций для пользователей с правами «чтение»* (режим настраивается администратором в соответствии с документом 643.72410666.00082-01 96 01-01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование»).

[2)] Пользователям с правами доступа к устройствам *Полный доступ*, не имеющим прав

Право доступа	Описание
доступа *Управление* в категории *Настройки доступа*, не доступны для изменения настройки устройств, влияющие на общесистемные параметры контроля устройств. Например, таким пользователям недоступны операции добавления, изменения и клонирования отчетов на сервере ПК, но доступна для изменения настройка использования отчетов для устройств	

Функции управления устройствами доступны пользователям в ПК «Efros Config Inspector» v.4 только после включения модуля ***Управление устройствами*** (при его наличии в лицензии). Права на управление устройствами назначаются каждому пользователю отдельно в карточке пользователя. Действует назначенная привилегия на управление только на устройства, для которых пользователю назначены права *Полный доступ*.

Вне зависимости от прав доступа к настройкам и администрированию комплекса и к устройствам пользователь может менять локальные настройки клиентской консоли комплекса (см. п. 2.1.2).

Для доступа к функциональным возможностям комплекса предусмотрена обязательная аутентификация пользователя при запуске клиентской консоли комплекса. Идентификация пользователя осуществляется посредством ввода логина и пароля в соответствующие поля окна клиентской консоли.

В процессе аутентификации проверяется соответствие введенного пользователем логина и пароля одной из учетных записей из списка пользователей.

2. Выполнение функций

Для централизованного контроля и анализа конфигураций сетевого и серверного оборудования компании сетевому администратору необходимо:

1) Определить список контролируемого комплексом сетевого и серверного оборудования, а также рабочих станций, с установленными операционными системами семейства Windows или Linux.

2) Установить на рабочие станции с установленной ОС Windows Windows-агент ПК «Efros Config Inspector» v.4 (подробнее об установке Windows-агента см. документ 643.72410666.00082-01 95 01 «ПК «Efros Config Inspector» v.4. Руководство администратора).

3) Установить на ЭВМ установки серверной части комплекса и подключить внешние модули для работы с контролируемым оборудованием (подробнее об установке, подключении и настройке параметров работы внешних модулей см. документ 643.72410666.00082-01 96 01-01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование».

4) Добавить в список устройств комплекса контролируемое оборудование (подробнее о добавлении контролируемого оборудования, настройке его параметров см. п. 2.5 «Формирование списка контролируемых устройств»).

5) Настроить для контролируемого оборудования режим использования отчетов, расписание их автоматической загрузки и реакцию комплекса в ответ на произошедшие на сервере и/или контролируемом оборудовании события (обработчики событий) (подробнее о настройках контроля оборудования см. документ 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»).

В результате выполненных действий появится возможность загрузки в БД комплекса конфигураций контролируемого оборудования для их анализа и контроля.

2.1. Запуск и настройка клиентской консоли

2.1.1. Запуск и общее описание клиентской консоли

Производить запуск консоли клиентской части комплекса имеют право все пользователи комплекса. При инсталляции серверной части комплекса, для возможности первоначальной авторизации, автоматически создается встроенный пользователь (с логином **root** и паролем **root**).

Запуск клиентской консоли осуществляется из меню ***Пуск*** на панели задач. Для этого следует выбрать ***Пуск →Все программы →Efros Config Inspector 4 →Efros Config Inspector 4***.

Запустить консоль клиентской части также можно при помощи ярлыка вызова программы, который расположен на рабочем столе. В этом случае для запуска

программы необходимо дважды щелкнуть левой кнопкой манипулятора типа «мышь» (далее – «мышь») по пиктограмме ярлыка на рабочем столе.

При запуске консоли клиентской части ПК «Efros Config Inspector» v.4 откроется окно подключения консоли к серверной части комплекса (рис. 5), в котором следует:

1) В поле ***Сервер*** ввести IP-адрес сервера комплекса или его DNS-имя.

Если серверная и клиентская часть комплекса установлены на один компьютер, то можно указать один из зарезервированных для локального подключения IP-адресов, например, *127.0.0.1* или зарезервированное для локального подключения имя, например, *localhost*.

2) В поля **Логин** и **Пароль** ввести соответственно логин и пароль пользователя комплекса.

В поле ***Пароль*** отображается информационная пиктограмма с обозначением активной в текущий момент времени раскладки клавиатуры. Значение пиктограммы необходимо учитывать при вводе пароля пользователя.

Если осуществляется подключение к комплексу от имени пользователя, вошедшего в ОС, необходимо установить отметку у параметра ***Вход под текущим пользователем*** – поля ***Логин*** и ***Пароль*** станут недоступными для ввода, а идентификационные данные пользователя будут взяты из текущей сессии Windows, при этом в поле ***Логин*** отобразится имя учетной записи текущего пользователя ОС Windows.

3) Для подключения клиентской консоли к серверной части комплекса по умолчанию используется TCP-порт 20000. Если это значение в серверной консоли программного комплекса было изменено, то необходимо указать новое значение. Для этого необходимо в поле ***Порт*** ввести корректный номер TCP-порта для соединения клиентской консоли с серверной частью комплекса.

4) Нажать кнопку ***Подключиться***.

При первом запуске консоли локальным пользователем (в том числе встроенным пользователем) после создания учетной записи пользователя в списке пользователей ПК «Efros Config Inspector» v.4, при истечении срока действия пароля или при смене пароля текущего пользователя другим пользователем (с правами Управление в категории Администрирование) откроется окно принудительной смены пароля и пользователю необходимо выполнить смену пароля в соответствии с пунктом 2.1.4

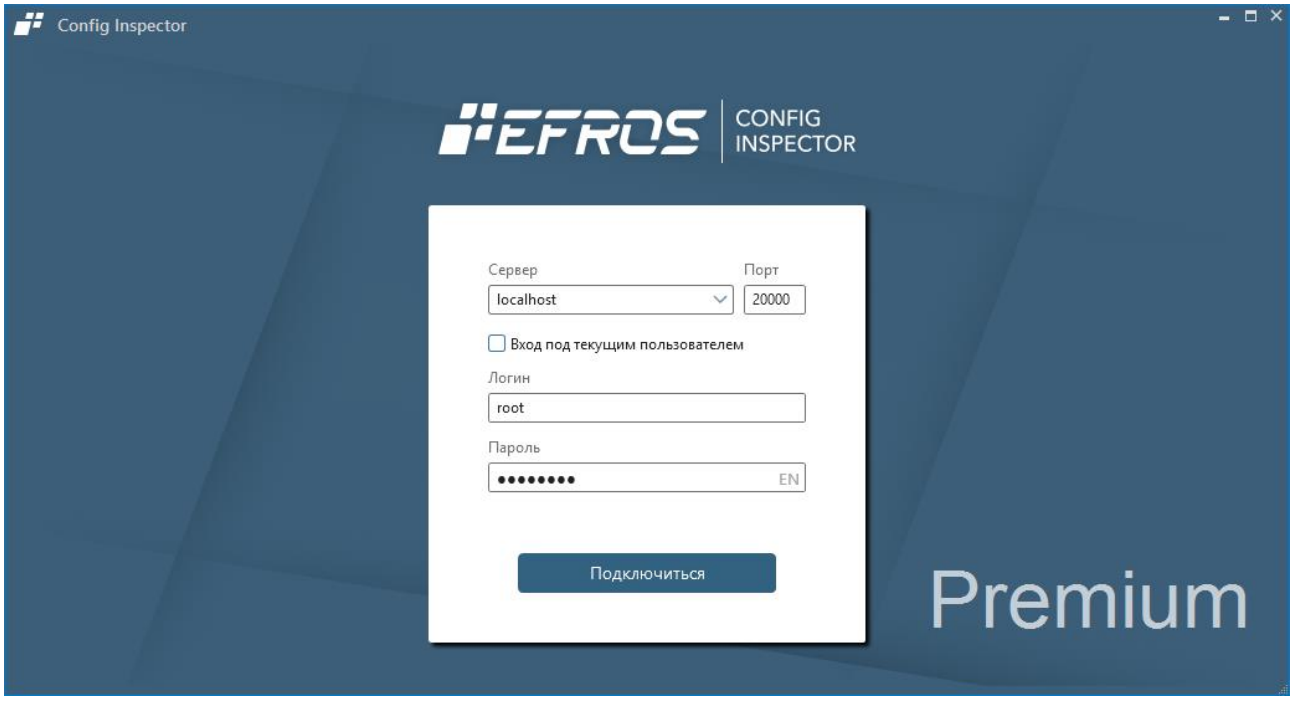


Рисунок 5 – Окно ***Подключение***

После успешного завершения аутентификации пользователя на сервере ПК «Efros Config Inspector» v.4 откроется окно клиентской консоли. По умолчанию открывается раздел консоли по работе с устройствами (рис. 6).

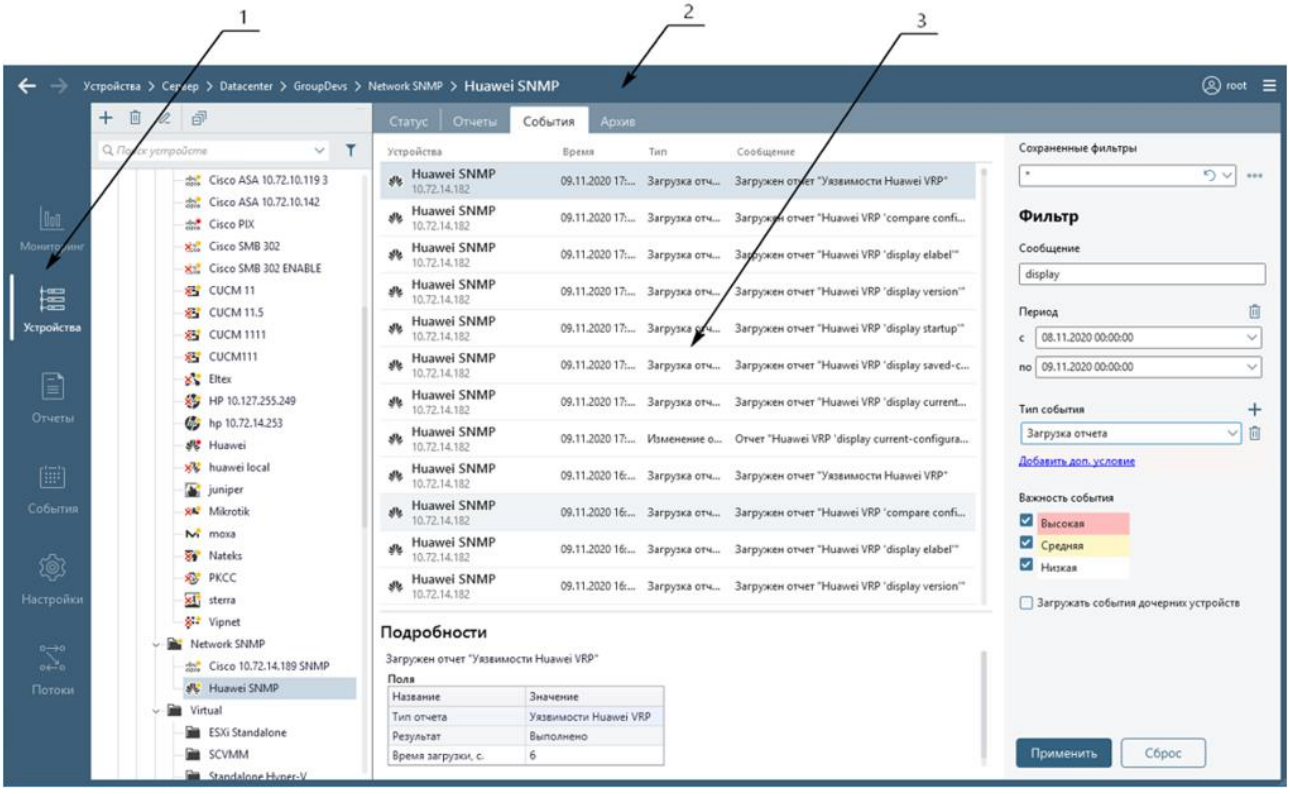


Рисунок 6 – Клиентская консоль. Раздел **Устройства**

Консоль разделена на:

1) Панель выбора раздела консоли (см. рис. 6, поз. 1), в которой расположены кнопки выбора разделов:

а) **Мониторинг** – здесь предоставляется обобщенная информация о состоянии всех устройств, подключенных к комплексу, в графическом виде (круговые диаграммы) и в виде списка уведомлений;

б) **Устройства** – раздел предназначен для работы с устройствами: ведения списка устройств, загрузки отчетов устройств, просмотра уведомлений, последних и архивных отчетов и событий устройств;

в) **Отчеты** – раздел предназначен для создания шаблонов и формирования на их основе пользовательских отчетов для выбранных устройств, по выбранным отчетам и за выбранный период;

г) **События** – в разделе отображены события, произошедшие на всех, контролируемых текущей серверной частью комплекса устройствах, а также действия пользователей клиентской консоли;

д) **Настройки** – раздел предназначен для доступа к настройкам текущей серверной части комплекса (подробнее описание раздела см. в п. 2.3 «Настройка комплекса»).

е) **Потоки** – раздел предназначен для доступа к функционалу работы с данными, полученными с сервера «Flow Server» (задание триггеров с правилами формирования событий о зафиксированной сетевой активности, просмотр и анализ информации). Функции программного компонента «Flow» комплекса доступны при активной лицензии, содержащей права на его использование.

Примечание – Описание последовательности действий при выполнении пользователями функций раздела **Потоки** приведено в документе «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector». Программный компонент «Flow». Руководство пользователя».

2) Заголовок (см. рис. 6, поз. 2), содержащий:

а) наименование и номер версии программного комплекса, имя (IP-адрес) сервера, к которому выполнено подключение (соответствует значению, введенному в поле ***Сервер*** окна подключения консоли к серверу ПК);

б) стандартные кнопки управления окном;

в) строку навигации по разделам и вкладкам консоли;

г) логин пользователя. При нажатии на имя пользователя открывается меню (рис. 7), описание пунктов которого приведено в таблице 2;

д) кнопку раскрытия меню «☰» (рис. 8), описание пунктов которого приведено в таблице 3.

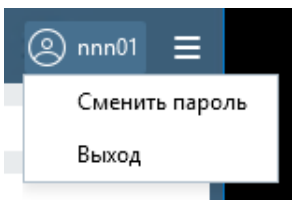


Рисунок 7 – Меню пользователя в клиентской консоли

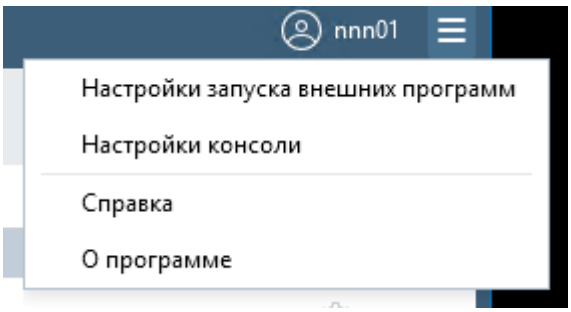


Рисунок 8 – Заголовок клиентской консоли с раскрытым меню

Таблица 2 – Состав и описание пунктов меню пользователя в клиентской консоли

Пункт	Описание/Назначение
Сменить пароль	Для перехода в окно смены пароля текущего пользователя (подробнее см. п. 2.1.4)
Выход	Осуществляется выход пользователя из консоли клиентской части комплекса. Консоль не закрывается, происходит возврат к окну авторизации пользователя.

Таблица 3 – Состав и описание пунктов меню заголовка клиентской консоли

Пункт	Описание/Назначение
Настройки запуска внешних программ	Для перехода в режим настройки параметров запуска внешних программ. При выборе пункта открывается окно **Настройки запуска внешних программ** (подробнее см. п. 2.1.3)
Настройки консоли	Переход в режим настройки параметров отображения в консоли всплывающих подсказок и уведомлений, а также параметров запроса комментариев к архивным версиям отчетов. При выборе пункта открывается окно **Настройки консоли** (подробнее см. п. 2.1.2)
Справка	Запуск файла справки по работе клиентской консоли
О программе	Позволяет получить сведения об установленной версии (рис. 9) клиентской консоли и сервера ПК, а также содержит ссылки: – *Техническая поддержка* – для перехода на страницу создания заявки в техподдержку комплекса; – *http://www.gaz-is.ru/* – для перехода на сайт компании-разработчика комплекса; – *Логи сервера* – для скачивания логов сервера ПК в виде архива (ссылка доступна для пользователей комплекса с правами *Просмотр* или *Управление* категории *Администрирование*); – *Сведения о системе* – для просмотра характеристик комплекса, с возможностью копирования текста для дальнейшей передачи в техподдержку компании-разработчика ПК «Efros Config Inspector» v.4 (ссылка доступна только для пользователей комплекса с правами *Управление* категории *Администрирование*)

Рисунок 9 – Окно просмотра сведений о программе

3) Рабочую область (см. рис. 6, поз. 3), в которой отображаются данные выбранной вкладки активного в текущий момент времени раздела консоли. Если при настройке консоли (см. пункт 2.1.2 «Настройка параметров работы клиентской консоли») включен режим отображения уведомлений, то при фиксировании текущей серверной частью комплекса событий: загрузка отчетов, принятие эталона, запуск действий по триггеру, обнаружение нарушения целостности для подключенных устройств или компонентов комплекса и т.д. – в рабочей области будут отображаться всплывающие окна с уведомлениями о зафиксированном событии.

2.1.2. Настройка параметров работы клиентской консоли

При выборе пункта меню ***Настройки консоли*** открывается окно настройки параметров работы клиентской консоли (рис. 10).

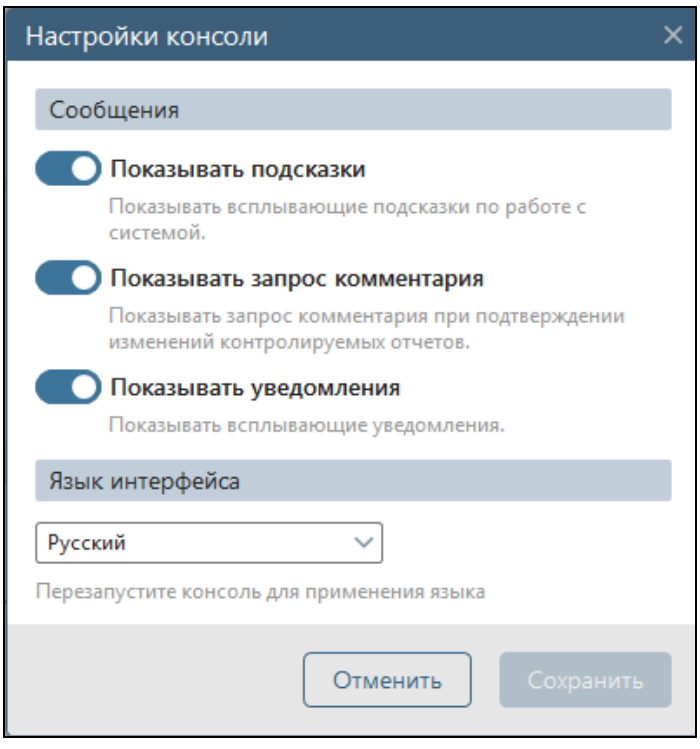


Рисунок 10 – Окно настройки параметров работы клиентской консоли

В окне **Настройки консоли** пользователю доступны для изменения следующие параметры:

- ***Показывать подсказки*** – управление отображением всплывающих подсказок по работе с клиентской консолью;
- ***Показывать запрос комментария*** – управление необходимостью ввода комментариев при подтверждении изменений отчетов, загруженных с устройств;
- ***Показывать уведомления*** – управление отображением всплывающих уведомлений о зафиксированных текущей серверной частью комплекса на событиях: загрузка отчетов, принятие эталона, запуск действий по триггеру, обнаружение нарушения целостности и т.д;
- ***Язык интерфейса*** – выбор языка интерфейса *(русский, английский)*.

2.1.3. Настройки запуска внешних программ

Для настройки запуска внешних программ пользователю необходимо выполнить следующие действия:

1) Нажать кнопку раскрытия меню в заголовке консоли и выбрать пункт меню ***Настройки запуска внешних программ***.

2) В открывшемся окне настройки параметров запуска внешних программ (рис. 11), разрешить запуск внешних программ для соединения клиентской консоли с контролируемым оборудованием, установив флаг в соответствующем поле.

3) Ввести в соответствующие поля путь к исполняемому файлу внешней программы и параметры запуска программы, если они отличаются от указанных по умолчанию.

4) Нажать кнопку ***Сохранить.*** Внесенные изменения будут сохранены, окно настройки параметров запуска внешних программ закроется.

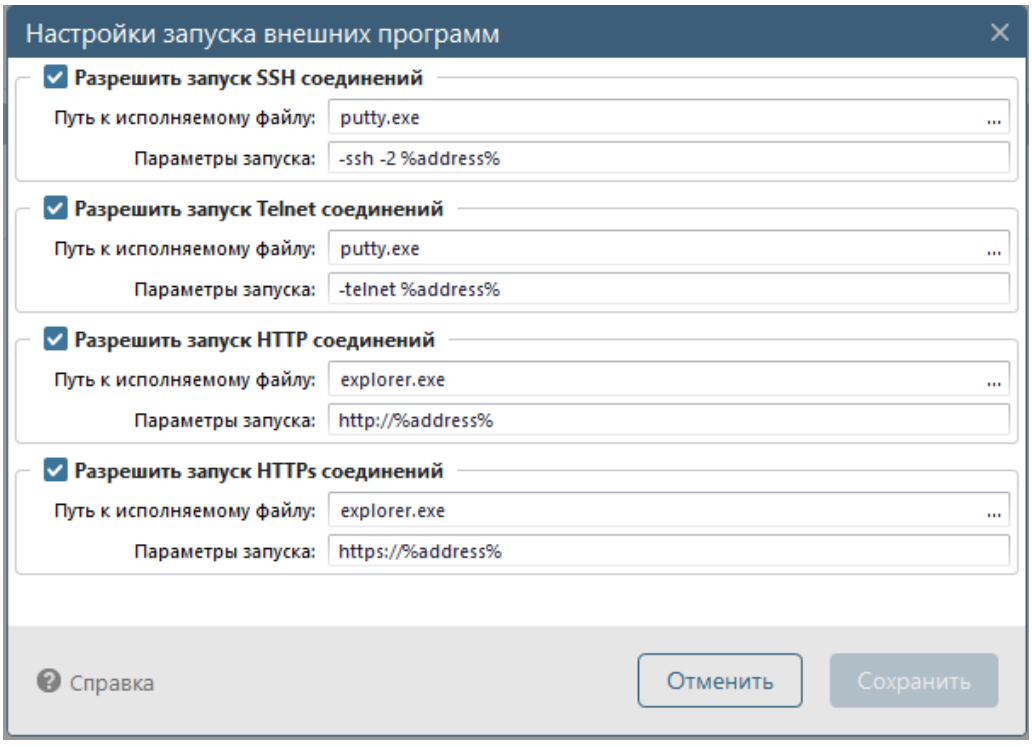


Рисунок 11 – Окно **Настройки запуска внешних программ**

2.1.4. Смена пароля пользователя

Операция смены пароля пользователя программного комплекса из клиентской консоли комплекса доступна только для локальных пользователей комплекса. При необходимости смены пароля доменного пользователя необходимо использовать средства ОС Windows.

Смена пароля пользователя может быть выполнена из общего списка пользователей ПК «Efros Config Inspector» v.4 (ведется в клиентской консоли) пользователем с правами *Управление* категории *Администрирование* или самим пользователем по решению пользователя при работе с клиентской консолью и в принудительном порядке в следующих случаях:

- при первом запуске клиентской консоли после создания учетной записи пользователя в списке пользователей ПК «Efros Config Inspector» v.4;
- при истечении срока действия пароля (срок действия пароля в ПК «Efros Config Inspector» v.4 настраивается и может быть от 1 до 365 дней);
- после смены пароля пользователя в списке пользователей ПК «Efros Config Inspector» v.4 другим пользователем.

Если требуется смена пароля в принудительном порядке, то после ввода данных пользователя в окне подключения к серверу и нажатия кнопки ***Подключиться*** откроется окно смены пароля (рис. 12). Пользователю необходимо ввести дважды новый пароль и нажать кнопку ***Сохранить***. Окно смены пароля пользователя закроется, пароль пользователя будет изменен.

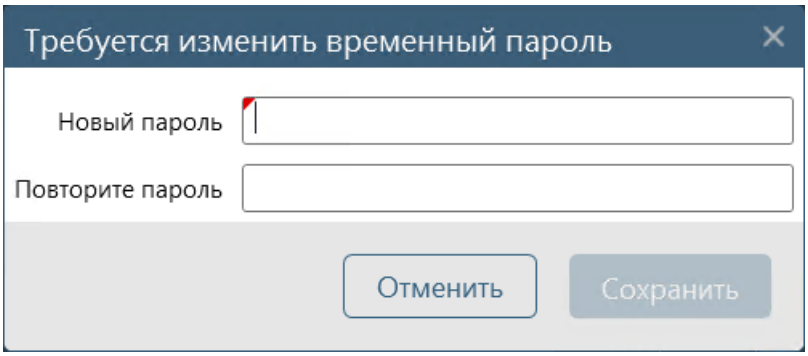


Рисунок 12 – Окно принудительной смены пароля пользователя

Для смены пароля ***текущего пользователя*** по решению пользователя необходимо выполнить следующие действия:

1) В заголовке клиентской консоли нажать на имя работающего с консолью пользователя.
2) Выбрать в открывшемся меню пункт ***Сменить пароль***.
3) В открывшемся окне заполнить поля данными старого и нового пароля.
4) Нажать кнопку ***Сохранить.*** Окно смены пароля пользователя закроется, пароль пользователя будет изменен.

При смене пароля могут возникать ошибки, перечень и правила исправления которых приведены в пункте 3.4.2.

2.2. Просмотр мониторинговой информации и настройка интерфейса раздела Мониторинг

Раздел **Мониторинг** (рис. 13) доступен всем пользователям комплекса и предназначен для предоставления пользователю обобщенной информации о состоянии всех доступных ему устройств, подключенных к текущему серверу ПК.

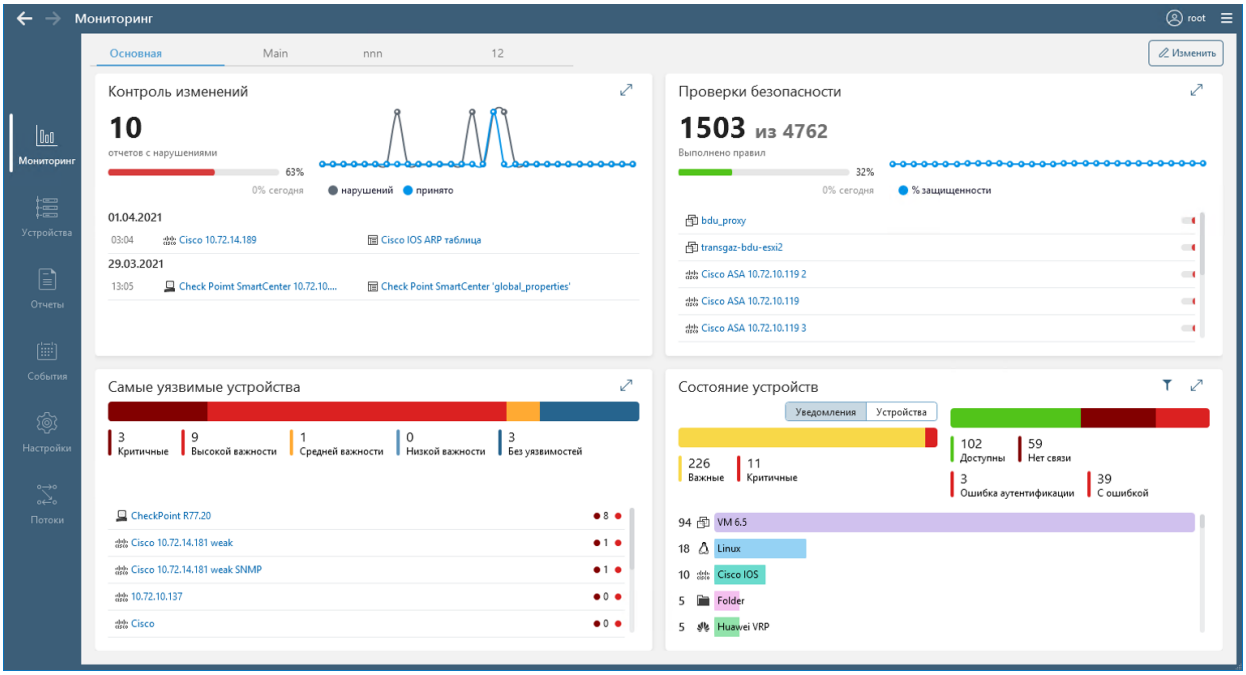


Рисунок 13 – Раздел **Мониторинг**

После установки комплекса страница раздела **Мониторинг** содержит одну (основную) вкладку, разделенную на области (далее – виджеты), в которых в графическом и текстовом виде представлены общие сведения о состоянии контролируемых на сервере ПК «Efros Config Inspector» v.4 устройств. По умолчанию страница содержит виджеты (далее – виджеты «по умолчанию»):

- ***Контроль изменений*** – данные о количестве измененных отчетов, находящихся на контроле, в точном выражении и в процентах от общего числа таких отчетов, линейный график изменения количества отчетов с нарушениями и принятых отчетов за предшествующий месяц, а также список последних десяти выявленных отчетов с нарушенной целостностью;
- ***Самые уязвимые устройства*** – количество устройств, на которых выявлены уязвимости, сгруппированные по степени критичности уязвимостей, а также список десяти последних устройств, на которых выявлено наибольшее количество уязвимостей, отсортированный по степени критичности;
- ***Проверки безопасности*** – данные о выполненных на устройствах правилах проверок безопасности в точном выражении и в процентах от их общего количества, линейный график изменения защищенности устройств за предшествующий месяц, а также список из десяти

последних устройств с наименьшим процентом выполненных правил (самые незащищенные устройства);

- ***Состояние устройств*** – общие сведения о количестве контролируемых устройств и результатах их проверок. При выборе переключателя:
  а) ***Уведомления*** – отображается количество уведомлений (по категориям) на всех выбранных при настройке виджета устройствах;
  б) ***Устройства*** – отображается количество устройств с соответствующими категориями уведомлений.

Пользователь имеет возможность по нажатию в заголовке страницы кнопки ***Изменить*** перейти в режим настройки состава вкладок страницы и элементов вкладок раздела **Мониторинг** (см. п. 2.2.5 «Настройка страницы раздела Мониторинг»). В режиме редактирования для виджетов по умолчанию пользователь может изменить:

- в виджете ***Контроль изменений*** – для блока с данными о количестве измененных отчетов – период обновления с 5 минут на 1 минуту или 10 минут, для блока с графиком – период выборки данных с 30 дней на 7 или 14 дней, период обновления с 5 минут на 1 минуту или 10 минут, тип графика с линейного на столбчатый, тип отображаемых данных с *Нарушения и принято* на *Только нарушения* или *Только принято*, для блока со списком отчетов – количество отображаемых отчетов с 10 на 5 или 15;
- в виджете ***Самые уязвимые устройства*** – для блока со списком устройств – количество отображаемых устройств с 10 на 5 или 15;
- в виджете ***Проверки безопасности*** – для блока с данными о количестве выполненных правилах – период обновления с 5 минут на 1 минуту или 10 минут, для блока с графиком – период выборки данных с 30 дней на 7 или 14 дней, период обновления с 5 минут на 1 минуту или 10 минут, тип графика с линейного на столбчатый, для блока со списком устройств – количество отображаемых устройств с 10 на 5 или 15, тип отображаемых данных с *Самые незащищенные* на *Самые защищенные;*
- в виджете ***Состояние устройств*** – для блока о количестве уведомлений – выбрать режим отображения данных *Уведомления* или *Устройства*, для блока о состоянии устройств – вид графика *Линейное распределение* или *Гистограмма.*

В разделе **Мониторинг** можно просмотреть краткую информацию о состоянии каждого из отображаемого в нем устройств – для этого необходимо щелкнуть по имени устройства левой кнопкой манипулятора типа «мышь» (далее – «мышь»). В результате откроется карточка устройства (рис. 14), в которой приведены основные сведения о его конфигурации, уровне защищенности, обнаруженных уязвимостях (с учетом наличия скрытых уязвимостей) и количестве уведомлений по типам (отображается информация только об имеющихся уведомлениях).

Пользователь имеет возможность в карточке выделить и скопировать данные устройства: имя устройства, адрес, описание (при его наличии в карточке), модель,

версию. Из карточки устройства можно перейти на вкладку ***Статус*** раздела **Устройства**, нажав расположенную в нижней части карточки кнопку ***Перейти к устройству***.

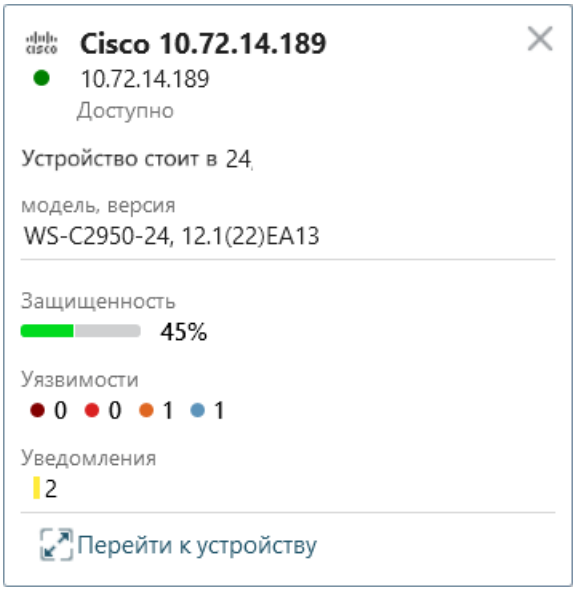


Рисунок 14 – Карточка устройства в разделе **Мониторинг**

Также из раздела **Мониторинг** можно перейти в форму сравнения отчета с эталоном, нажав на имя отчета с нарушенной целостностью (подробнее о сравнении отчетов см. п. 2.9.6 «Сравнение отчета с эталонной версией» настоящего Руководства).

Для каждого отображаемого в разделе **Мониторинг** виджета по умолчанию и виджета, созданного пользователем и содержащего составные элементы одной категории, существует возможность просмотра подробного отчета, для этого необходимо нажать кнопку «⤢», которая расположена в верхнем правом углу виджета. Для выхода из режима просмотра подробного отчета и перехода в раздел **Мониторинг** необходимо нажать кнопку «✕» в ***Панели выбора раздела консоли***.

Примечание – В блоках со списками отчетов, устройств подробных отчетов виджетов пользователю доступен поиск отчетов, устройств (поле поиска). Для поиска по точному совпадению фразы (например, 12:22 или Cisco ASA) необходимо фразу указать в кавычках (например, “12:22” или “ Cisco ASA”).

Если отсутствуют данные для отображения в виджете, то в виджете будет отображаться пиктограмма либо и текст *Данные отсутствуют*.

2.2.1. Просмотр подробного отчета в области Контроль изменений

При нажатии в виджете *Контроль изменений* кнопки «⤢» открывается отчет, в котором приводятся подробные сведения о состоянии контролируемых устройств (рис. 15):

- круговая диаграмма состояния отчетов, поставленных на контроль целостности – приводятся сведения об общем количестве отчетов,

целостность которых контролируется, результатах выполнения их проверки целостности в процентах и точном количестве;
- график изменения контролируемых отчетов за последний месяц – приводятся сведения о количестве выявленных за определенный день нарушений целостности отчетов и количестве отчетов, изменения которых были подтверждены администратором комплекса;
- список отчетов с нарушенным контролем целостности;
- список выявленных нарушений отчетов по типам контролируемого оборудования.

При наведении курсора на точку в области графика отображаются данные за соответствующий день (см. рис. 15).

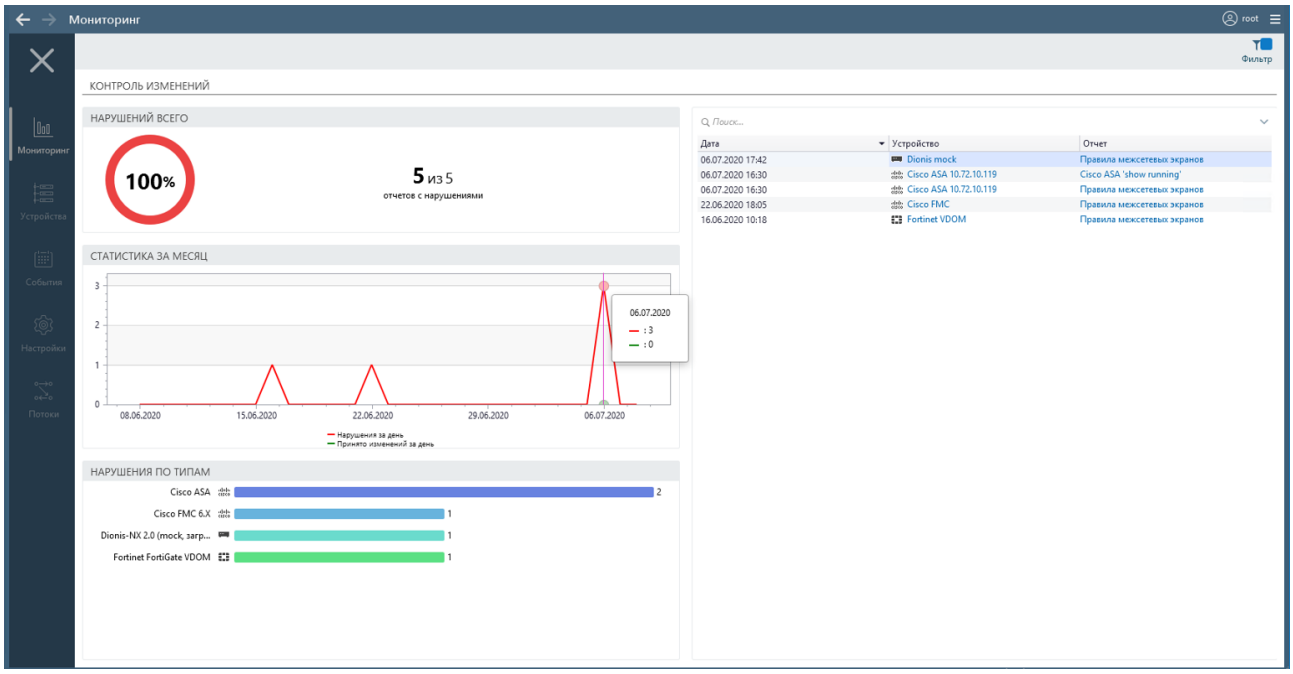


Рисунок 15 – Раздел **Мониторинг**. Отчет ***Контроль изменений***

2.2.2. Просмотр подробного отчета в области Проверки безопасности

При нажатии в виджете *Проверки безопасности* кнопки «⤢» открывается отчет, в котором приводятся подробные сведения о проверках безопасности, проведенных на контролируемых устройствах (рис. 16):

- круговая диаграмма выполнения правил, входящих в проверки, на всех устройствах – приводятся сведения об общем количестве правил, которые содержатся в проверках безопасности, результатах выполнения этих правил в процентах и точном количестве;
- график изменения выполнения правил, входящих в проверки, за последний месяц – приводятся сведения о количестве выполненных и невыполненных за определенный день в ходе проверки правил;
- список типов контролируемого оборудования с результатами выполненных проверок на всех устройствах каждого типа;
- список устройств с результатами выполнения на них проверок безопасности.

При наведении курсора на точку в области графика отображаются данные за соответствующий день (см. рис. 16).

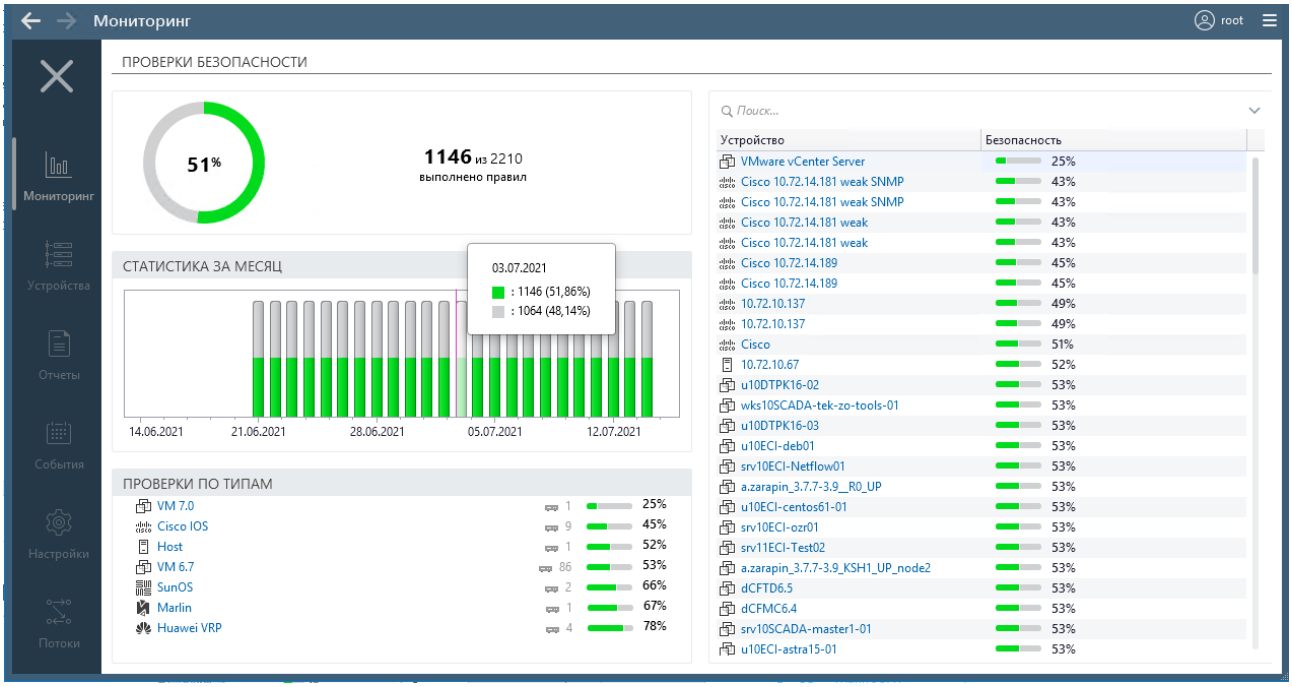


Рисунок 16 – Раздел **Мониторинг**. Отчет ***Проверки безопасности***

2.2.3. Просмотр подробного отчета в области Самые уязвимые устройства

При нажатии в виджете *Самые уязвимые устройства* кнопки «⤢» открывается отчет, в котором приводятся подробные сведения о проверках контролируемых устройств на наличие уязвимостей (рис. 17):

а) линейная диаграмма уязвимости контролируемых устройств – приводится количество устройств, на которых выявлены уязвимости, сгруппированные по степени критичности:
   - *Критичные* – устройства, при проверке которых обнаружена хоть одна уязвимость с *Критичным* уровнем;
   - *Высокой важности* – устройства, при проверке которых не обнаружено уязвимостей с *Критичным* уровнем, но выявлена хоть одна уязвимость с *Важным* уровнем критичности;
   - *Средней важности* – устройства, при проверке которых не обнаружено уязвимостей с *Критичным* или *Важным* уровнем, но выявлена хоть одна уязвимость со *Средним* уровнем критичности;
   - *Низкой важности* – устройства, при проверке которых не обнаружено уязвимостей с *Критичным, Важным* или *Средним* уровнем, но выявлена хоть одна уязвимость с *Низким* уровнем;

б) график изменения количества устройств с выявленными уязвимостями за месяц – приводятся сведения о количестве устройств для каждой степени критичности уязвимостей за определенный день;

в) список устройств с количеством выявленных на них уязвимостей, сгруппированных по степени критичности;

г) список типов контролируемого оборудования с количеством выявленных на них уязвимостей, сгруппированных по степени критичности, для каждого типа.

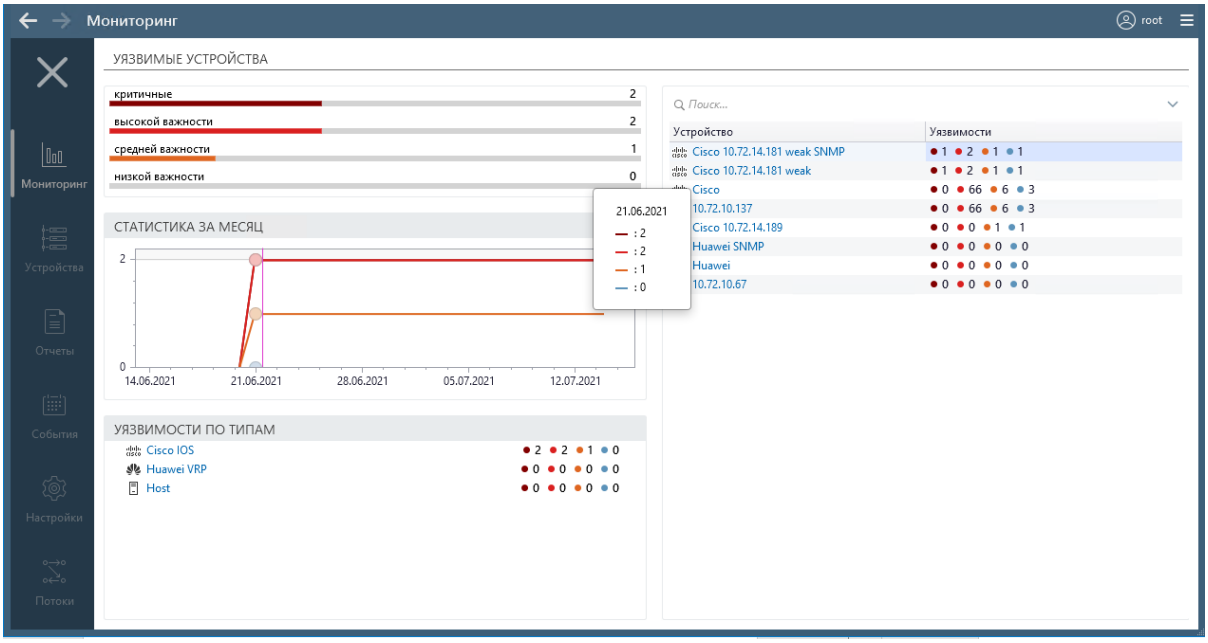


Рисунок 17 – Раздел **Мониторинг**. Отчет ***Уязвимые устройства***

При наведении курсора на точку в области графика отображаются данные за соответствующий день (см. рис. 17).

2.2.4. Просмотр подробного отчета в области Состояние устройств

При нажатии в виджете *Состояние устройств* кнопки «⤢» открывается отчет, в котором приводятся подробные сведения о состоянии контролируемых устройств (рис. 18):

а) линейная диаграмма статусов контролируемых устройств – приводится общее количество устройств, а также количество устройств для каждого из возможных статусов:
- *Нет связи* – при выполнении последней операции с устройством оно было недоступно для комплекса;
- *Критично* – в результате загрузки с устройства отчетов получены уведомления о нарушениях (ошибка загрузки отчета, ошибка проверки устройства, нарушение целостности контролируемого отчета и т.д.);
- *Важно* – в результате загрузки с устройства отчетов получены уведомления со статусом *Важно* и нет уведомлений со статусом *Критично*;
- *Информация* – в результате загрузки с устройства отчетов получены уведомления со статусом *Информация* и нет уведомлений со статусом *Критично* или *Важно*;
- *Без уведомлений* – для устройства отсутствуют уведомления;
- *Сервисный режим* – устройство переведено в сервисный режим.

б) график изменения статуса состояния устройств за месяц – приводятся сведения о количестве устройств для каждого статуса состояния за определенный день;
в) список всех контролируемых текущей серверной частью комплекса устройств с указанием статуса состояния каждого устройства. Для состояния *Нет связи* в скобках указывается время недоступности устройства, например, «2 ч» или «128 дн.»;
г) список типов контролируемого оборудования с указанием общего количества устройств каждого типа.

При наведении курсора на точку в области графика отображаются данные за соответствующий день (см. рис. 18).

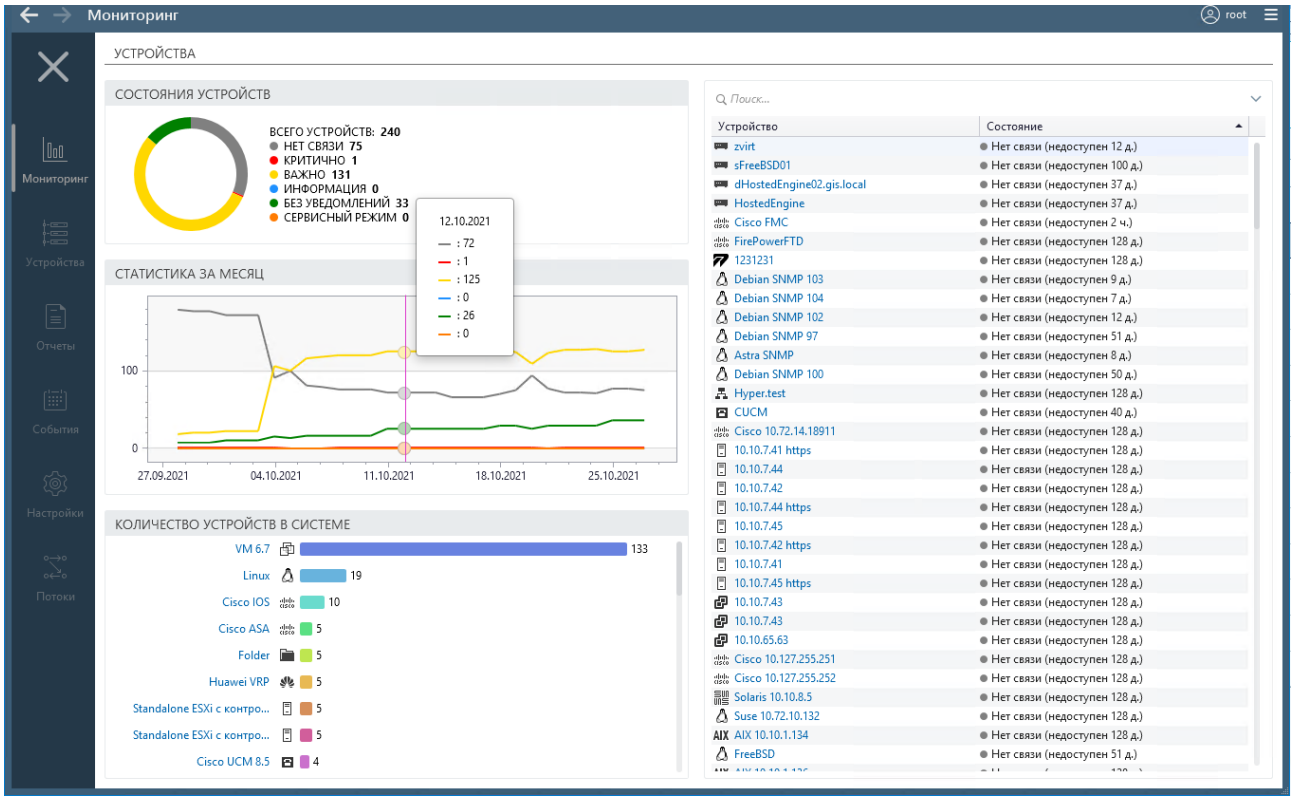


Рисунок 18 – Раздел **Мониторинг**. Отчет ***Устройства***

2.2.5. Настройка страницы раздела Мониторинг

В разделе **Мониторинг** пользователь имеет возможность добавить вкладки с виджетами, настроить на основной и дополнительных вкладках страницы их название, состав виджетов данных, состав отображаемых в них данных.

Для перехода в режим настройки раздела необходимо нажать в заголовке страницы раздела **Мониторинг** кнопку ***Изменить***. В заголовке дополнительно отобразятся кнопки (рис. 19):

- ***Редактировать*** (✎) – для перехода в окно редактирования наименования вкладки;
- ***Удалить*** (🗑) – для удаления вкладки;

- ***Добавить*** (+) – для добавления новой вкладки, по нажатию кнопки открывается окно ввода наименования новой вкладки;
- ***Новый виджет*** (+ Новый виджет) – для перехода в окно выбора добавляемого виджета;
- ***Меню*** (ooo) – для восстановления основной вкладки**,** а также экспорта и импорта всех настроек страницы раздела **Мониторинг**;
- ***Выход*** (✕) – для выхода из режима редактирования (с сохранением внесенных изменений).

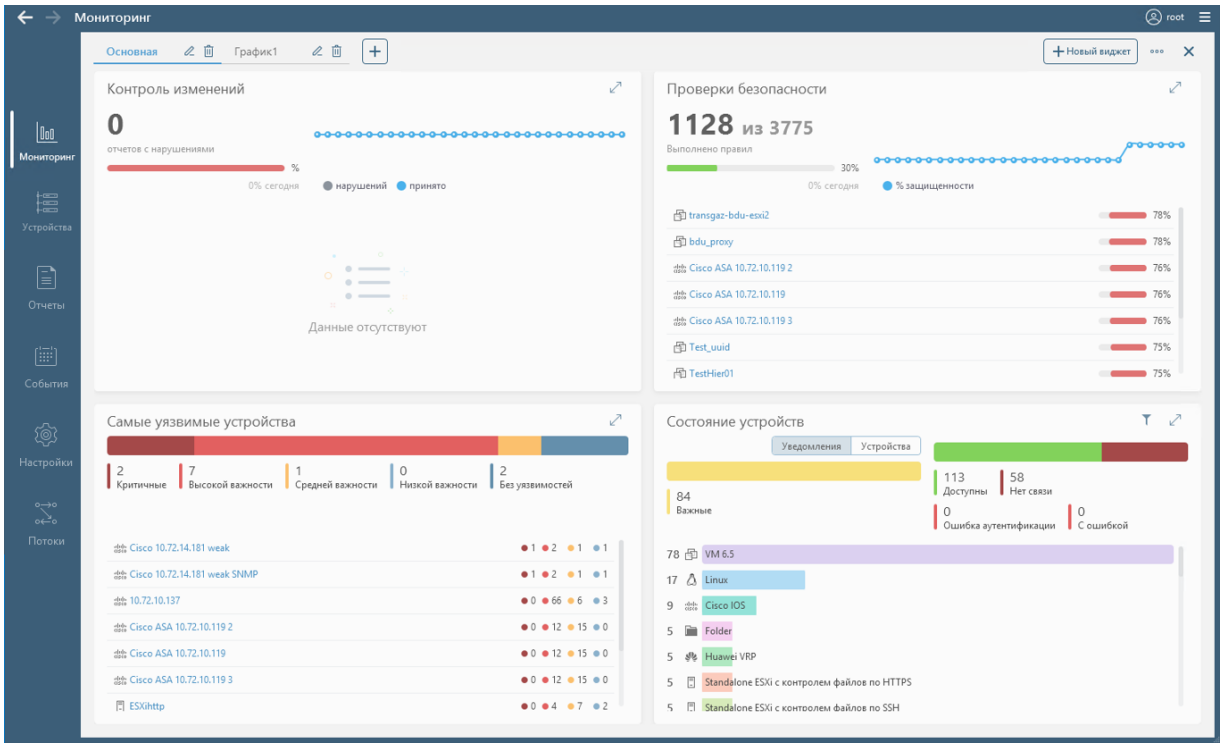


Рисунок 19 – Раздел **Мониторинг** в режиме настройки вкладок страницы

2.2.5.1. Добавление вкладки страницы раздела Мониторинг

Для добавления новой вкладки на страницу раздела **Мониторинг** необходимо в режиме настройки раздела нажать кнопку ***Добавить*** (+)**,** в открывшемся окне (рис. 20) ввести наименование новой вкладки и нажать кнопку ***Сохранить***.

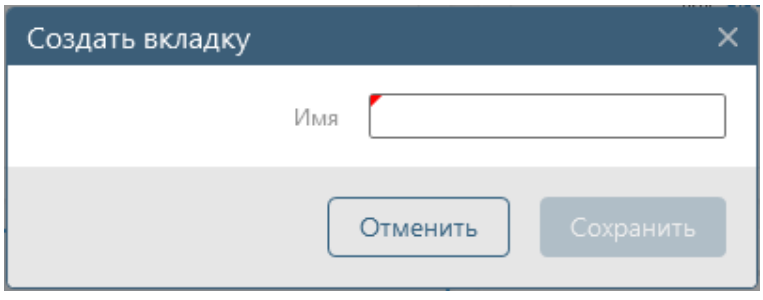


Рисунок 20 – Окно **Создать вкладку**

Созданная вкладка не будет содержать виджеты. Пользователю необходимо в соответствии с пунктами 2.2.5.3 «Добавление виджета на вкладку страницы

Мониторинг» и 2.2.5.4 «Настройка виджетов» добавить и настроить виджеты вкладки.

2.2.5.2. Редактирование наименования вкладки страницы

Для внесения изменений в наименование вкладки страницы раздела **Мониторинг** необходимо в режиме настройки раздела выбрать изменяемую вкладку, нажать справа от ее наименования кнопку ***Редактировать,*** в открывшемся окне (рис. 21) внести изменения и нажать кнопку ***Сохранить***.

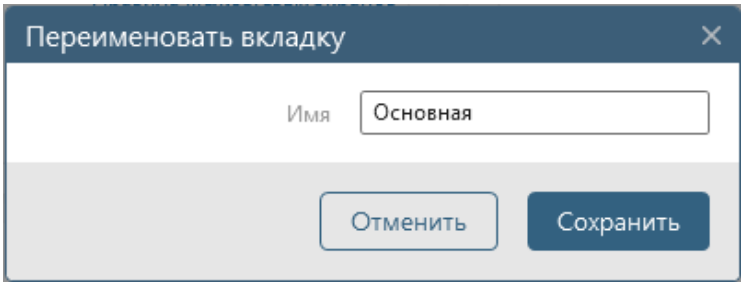


Рисунок 21 – Окно **Переименовать вкладку**

2.2.5.3. Добавление виджета на вкладку страницы Мониторинг

Для добавления виджета на вкладку страницы раздела **Мониторинг** необходимо в режиме настройки раздела:

1) Выбрать изменяемую вкладку.
2) Нажать кнопку ***Новый виджет***. Откроется панель **Новый виджет** (рис. 22), содержащая блок **Другие,** блоки с наименованиями стандартных виджетов, а также блок **Иерархия**, каждый блок содержит список доступных для выбора типов данных. Блоки доступны для сворачивания/разворачивания по нажатию в заголовке блока кнопки ⌄/›.
3) Выбрать щелчком левой кнопки «мыши» добавляемый тип данных. На странице будет добавлен новый виджет с наименованием соответствующего блока, виджет будет содержать данные выбранного типа для всех устройств комплекса, виджет категории **Иерархия** будет содержать данные устройств, подключенных к выбранным серверам комплекса (одновременно могут быть выбраны не более трех серверов, входящих в иерархию).

Примечание – При выборе значения ***Старый виджет*** на странице будет добавлен дубликат имеющегося виджета для соответствующего блока (со всеми типами данных «по умолчанию»).

Для добавления виджета ***Составной элемент*** необходимо сначала выбрать щелчком левой кнопки «мыши» тип данных ***Составной элемент***, на странице будет добавлен новый виджет с наименованием ***Составной элемент.*** Затем необходимо выбрать добавляемые в него типы данных (элементы виджета) «перетаскиванием» с помощью «мыши» их наименования в область виджета.

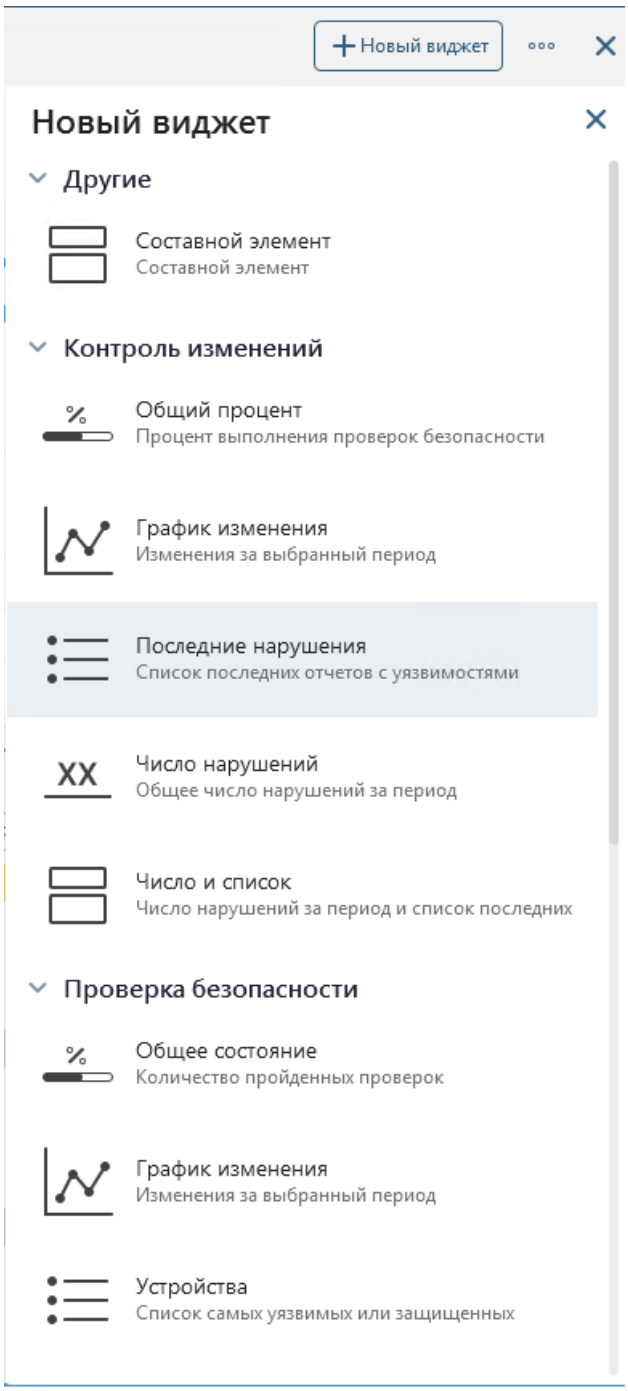


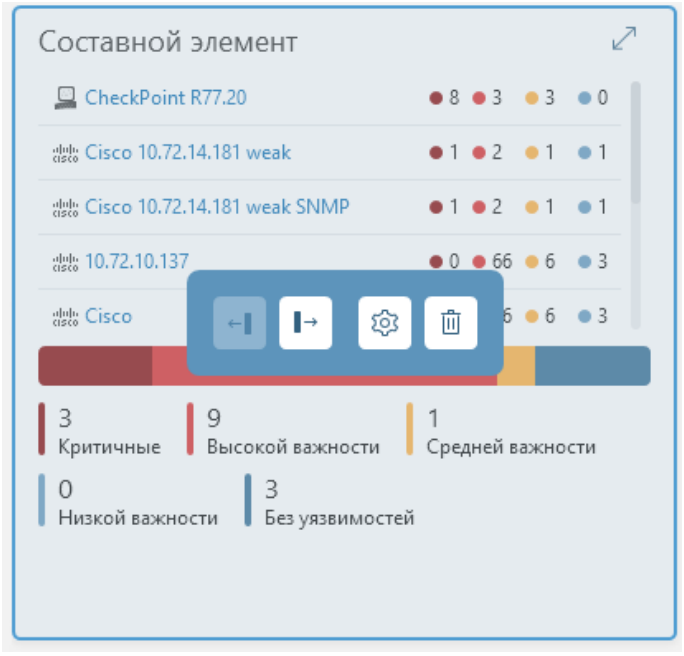
Рисунок 22 – Панель **Новый виджет**

2.2.5.4. Настройка виджетов

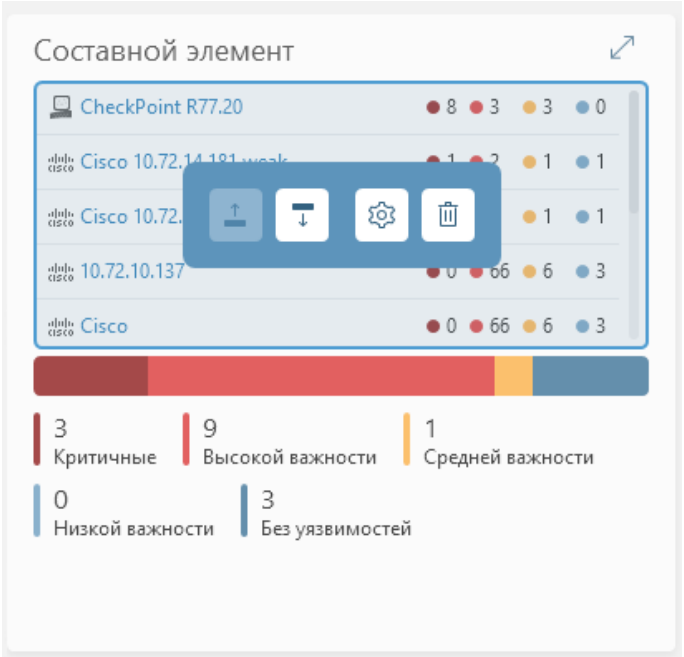
Настройка виджетов доступна только в режиме настройки раздела. Настроить расположение виджетов на странице или элементов внутри составных виджетов пользователь может путем перетаскивания виджетов и их элементов с помощью «мыши» за строку заголовка виджета либо, используя кнопки панели редактирования виджета/элемента виджета, для чего необходимо:

- установить курсор в заголовок виджета (рис. 23, а – для перемещения виджета в целом), в область элемента виджета (рис. 23, б – для перемещения элемента виджета);

– нажимая в раскрывшейся панели редактирования виджета/элемента виджета кнопки ***Вверх*** (), ***Вниз*** (), ***Влево*** (), ***Вправо*** () переместить виджет или его элемент в требуемое положение на странице.



а) виджет в целом



б) элемент виджета (список устройств)

Рисунок 23 – Виджет и элемент виджета в режиме редактирования

Примечание – Состав кнопок перемещения в окне настройки зависит от размера окна консоли и исходного местоположения виджета/элемента виджета.

Для настройки параметров виджета/элемента виджета необходимо выполнить следующие действия:

- установить курсор в заголовок виджета (для настройки виджета в целом) либо в область элемента виджета (для настройки элемента виджета) и нажать кнопку ***Настройки*** (⚙). Откроется окно **Настройка элемента**. На рис. 24 приведен пример окна настройки для составного виджета (в целом) с названием по умолчанию *Составной элемент*, в состав виджета входят элементы *Уведомления*, *Число нарушений* и *Доступность устройств*;

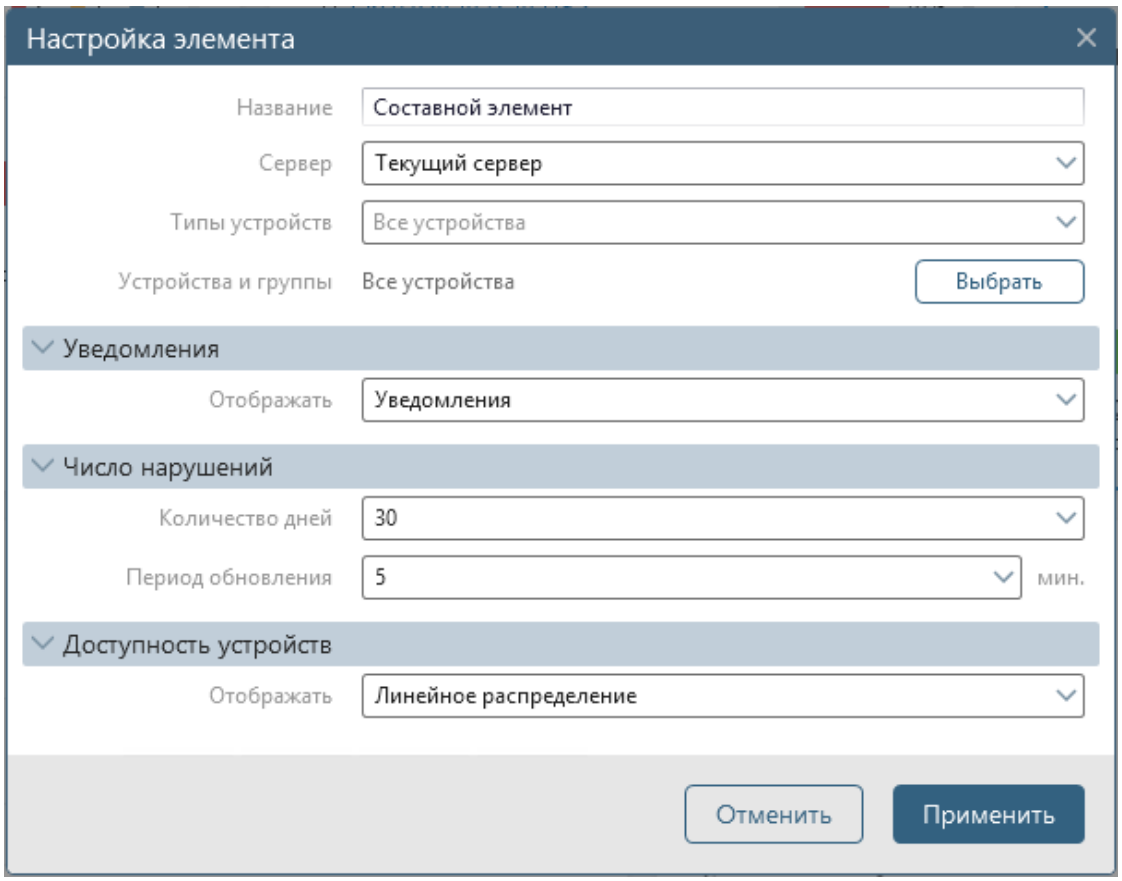


Рисунок 24 – Окно **Настройка элемента**

- далее внести требуемые изменения в поля окна **Настройка элемента**:
  а) изменить название виджета;
  б) выбрать сервер, данные по устройствам которого должны отображаться в виджете (список поля ***Сервер*** соответствует списку серверов, доступных в разделе **Устройства**);
  в) выбрать установкой флагов в полях списка ***Типы устройств*** требуемый тип или типы устройств (список содержит все типы устройств, поддерживаемые комплексом, выбор подтверждается нажатием кнопки ***Применить*** в нижней части списка);
  г) выбрать установкой флагов группы устройств/устройства в окне **Выбор устройств** (рис. 25), которое открывается по нажатию кнопки ***Выбрать*** (состав доступных для выбора групп устройств/устройств

зависит от выбранных на шаге ***в*** типов устройств). Для сохранения сделанного выбора – нажать в окне кнопку ***Выбрать***;

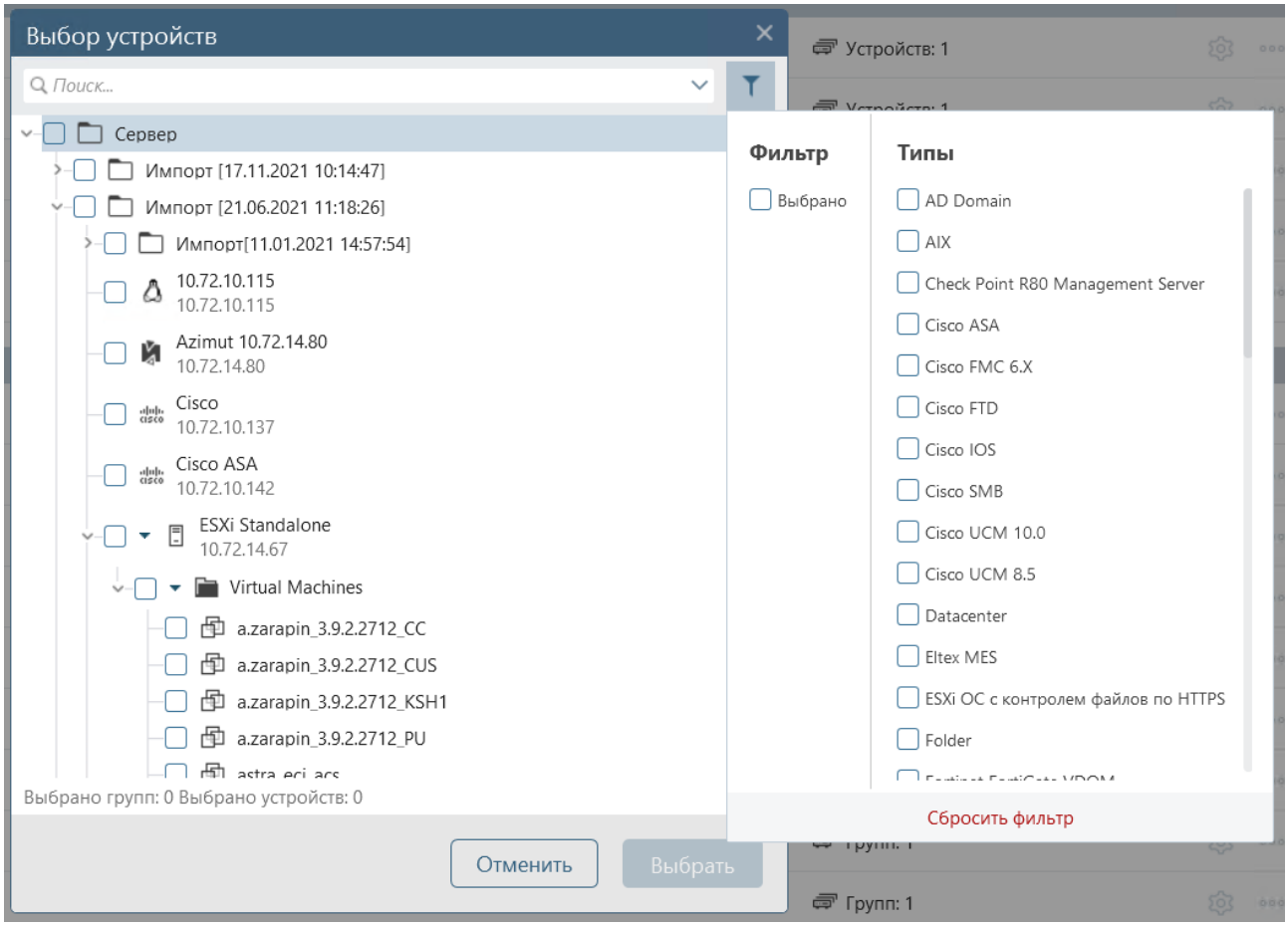


Рисунок 25 – Окно **Выбор устройств**

Примечание –. В окне выбора устройств:

- доступен поиск устройств и фильтрация списка по признаку *Выбрано* и типам устройств. Окно фильтрации открывается по кнопке ***Фильтр*** (). После установки в поле окна **Выбрано** флага, в списке отображаются только выбранные группы устройств/устройства. Отмена фильтрации выполняется по нажатию в окне ссылки ***Сбросить фильтр***;
- при выборе/снятии выбора с папки (не с хостами (например, на рис. 25 это группы «*Импорт…*»)) выбираются/снимается выбор всех дочерних элементов папки, при этом выбор/снятие выбора со всех дочерних элементов не приводит к выбору/снятию выбора папки;
- при выборе/снятии выбора с хоста (справа от поля для флага отображается кнопка «▾» (например, на рис. 25 это *ESXi Standalone* и *Virtual Machines*)) выбор/снятие выбора всех дочерних элементов не выполняется, для выбора/снятия выбора со всех дочерних элементов необходимо нажать кнопку «▾» и выбрать в раскрывшемся меню требуемое действие (рис. 26).

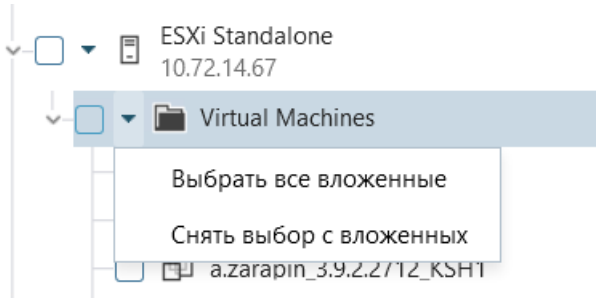


Рисунок 26 – Меню выбора действия с дочерними элементами хоста

д) выбрать дополнительные параметры, состав которых зависит от типа виджета/элемента виджета, например:
- количество дней, за которые будет отображаться информация (7,14 или 30);
- период обновления данных (1, 5 или 10 минут);
- количество элементов, отображаемых в виджете (5, 10, 15);
- тип графика *Линейный* или *Столбчатый*;
- отображать данные по самым защищенным или самым незащищенным устройствам;

е) в виджете категории ***Иерархия*** выбрать состав серверов (одновременно могут быть выбраны не более трех серверов), данные устройств которых должны отображаться в виджете (выбор серверов осуществляется установкой флагов в окне, которое открывается по нажатию кнопки ***Изменить***), а также установкой переключателей скрыть или выбрать отображение в виджете данных о защищенности, состоянии устройств и наличии уведомлений от устройств;

– нажать кнопку ***Применить***. Окно настройки закроется, внесенные изменения будут применены, данные виджета обновятся в соответствии с заданными параметрами.

После выхода из режима редактирования страницы раздела (по нажатию кнопки ***Выход*** (✕)) в заголовке виджета, в котором при настройке были внесены изменения в состав групп и типов устройств, отобразится кнопка ***Фильтр*** (▼). По нажатию кнопки ***Фильтр*** откроется окно со списками групп и типов устройств, для которых отображаются данные в виджете (рис. 27).

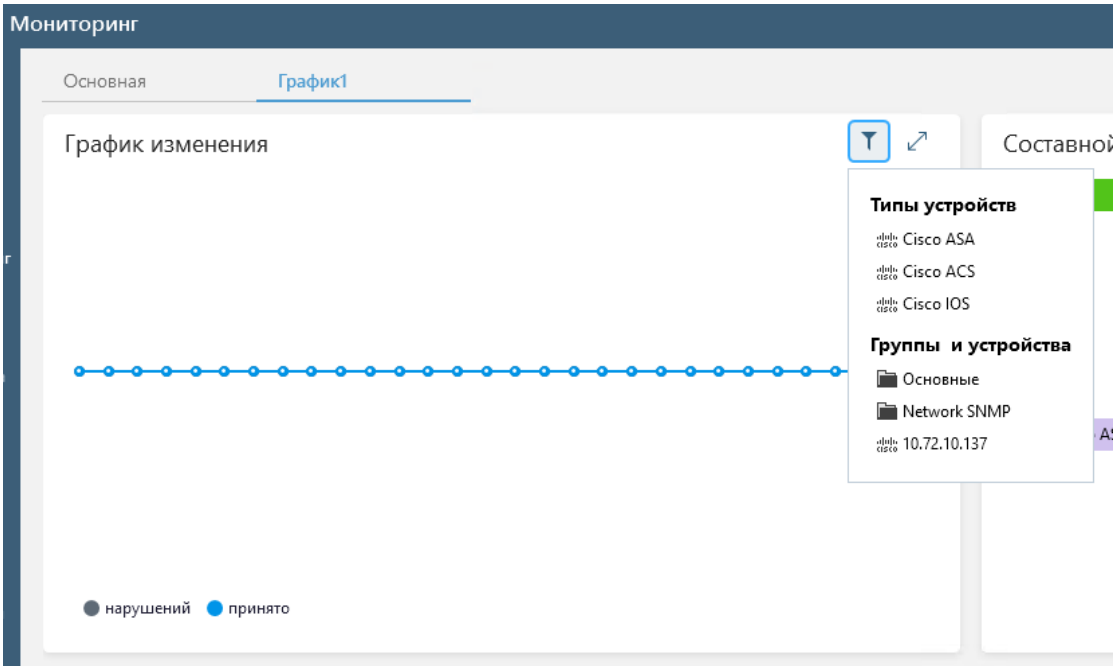
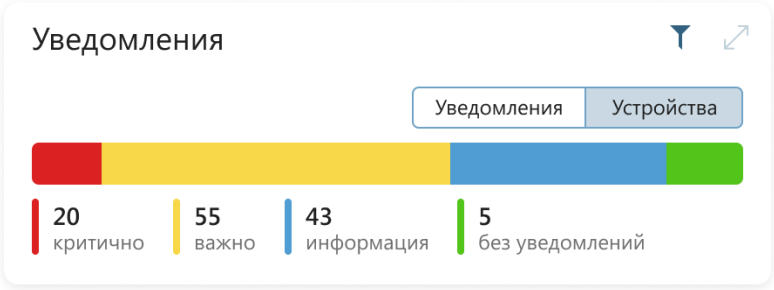


Рисунок 27 – Виджет с кнопкой ***Фильтр***

В виджете **Уведомления** (рис. 28) пользователь имеет возможность изменить выводимые данные без перехода в окно настройки виджета. При выборе переключателя:

- ***Уведомления*** – отображается количество уведомлений (по категориям) на всех выбранных при настройке виджета устройствах (рис. 28, а);
- ***Устройства*** – отображается количество устройств с соответствующими категориями уведомлений (рис. 28, б).

а)



б)

Рисунок 28 – Виджет **Уведомления**

2.2.5.5. Удаление виджета

Для удаления виджета необходимо в режиме настройки раздела:

- установить курсор в область виджета;
- нажать в раскрывшейся панели редактирования (см. рис. 23) кнопку ***Удалить*** ().

2.2.5.6. Удаление вкладки страницы раздела Мониторинг

Для удаления вкладки страницы раздела **Мониторинг** необходимо в режиме настройки раздела выбрать удаляемую вкладку, нажать справа от ее наименования кнопку ***Удалить,*** в открывшемся окне подтверждения нажать кнопку ***Удалить***. Вкладка будет удалена.

2.2.5.7. Восстановление основной вкладки, экспорт и импорт настроек страницы раздела Мониторинг

В разделе Мониторинг реализована возможность восстановления основной вкладки страницы с виджетами «по умолчанию», а также сохранения (экспорта) текущих настроек всех вкладок страницы в файл формата XML и их импорта из созданного файла.

Для восстановления основной вкладки пользователю необходимо выполнить следующие действия:

1) Перейти в режим настройки раздела **Мониторинг**.
2) Нажать в заголовке страницы кнопку ***Меню*** () и выбрать в раскрывшемся меню пункт ***Добавить вкладку по умолчанию***.. На странице раздела будет добавлена вкладка с названием **Основная**, содержащая виджеты «по умолчанию».

Для экспорта параметров вкладок пользователю необходимо выполнить следующие действия:

1) Перейти в режим настройки раздела **Мониторинг**.
2) Нажать в заголовке страницы кнопку ***Меню*** () и выбрать в раскрывшемся меню пункт ***Экспорт данных***.
3) В открывшемся стандартном окне ОС Windows «Сохранить как» указать имя и каталог размещения файла, в который будет произведен экспорт параметров вкладок, и нажать кнопку ***Сохранить***. Параметры вкладок (наименование, состав и параметры виджетов) будут сохранены в указанном файле.

Для импорта настроек вкладок пользователю необходимо выполнить следующие действия:

1) Перейти в режим настройки раздела **Мониторинг**.
2) Нажать в заголовке страницы кнопку ***Меню*** () и выбрать в раскрывшемся меню пункт ***Импорт***.
3) В открывшемся стандартном окне ОС Windows **Открыть** указать файл с импортируемыми данными и нажать кнопку ***Открыть***.
4) На странице раздела будут добавлены вкладки с параметрами, сохраненными в выбранном на шаге 3 файле.

2.3. Настройка комплекса

Функции администрирования комплекса и функции настройки контроля устройств комплекса доступны пользователям в разделе **Настройки** клиентской консоли (рис.29). Состав доступных пользователю настроек зависит от его прав в комплексе (см. п. 1.2 «Пользователи ПК «Efros Config Inspector» v.4»).

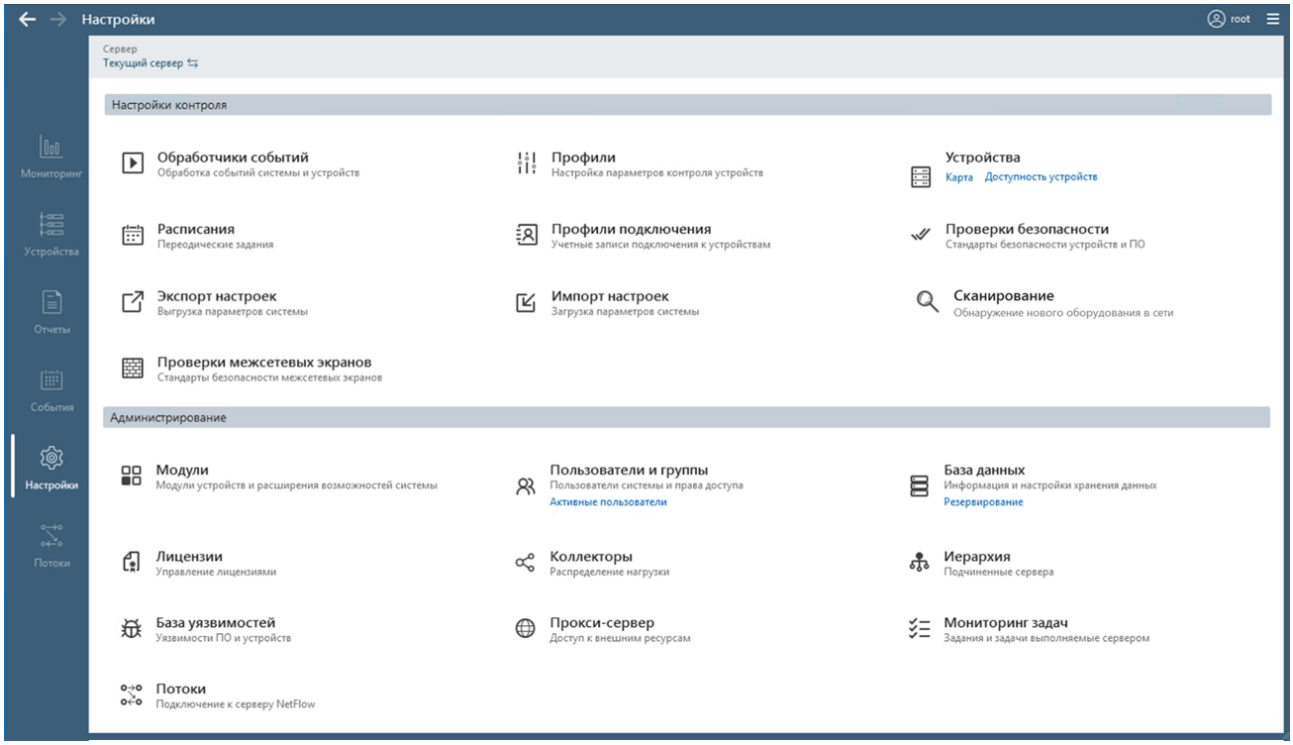


Рисунок 29 – Раздел **Настройки** для текущего сервера (главный в иерархии)

Подробное описание выполнения административных функций приведено в документе 643.72410666.00082-01 96 01-01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование», функций настройки контроля устройств – в документе 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».

2.4. Просмотр и управление списком устройств в разделе Устройства

Раздел **Устройства** (рис. 30) доступен всем пользователям комплекса и предназначен для работы с контролируемыми устройствами:

- просмотра/изменения списка устройств;
- просмотра/изменения свойств групп устройств и отдельных устройств;
- просмотра/изменения уровней доступа пользователей к группам устройств и отдельным устройствам;
- загрузки отчетов с устройств;
- просмотра уведомлений, последних и архивных отчетов и событий устройств;

- выполнения действий с устройствами;
- настройки списка доступных для запуска отчетов устройств.

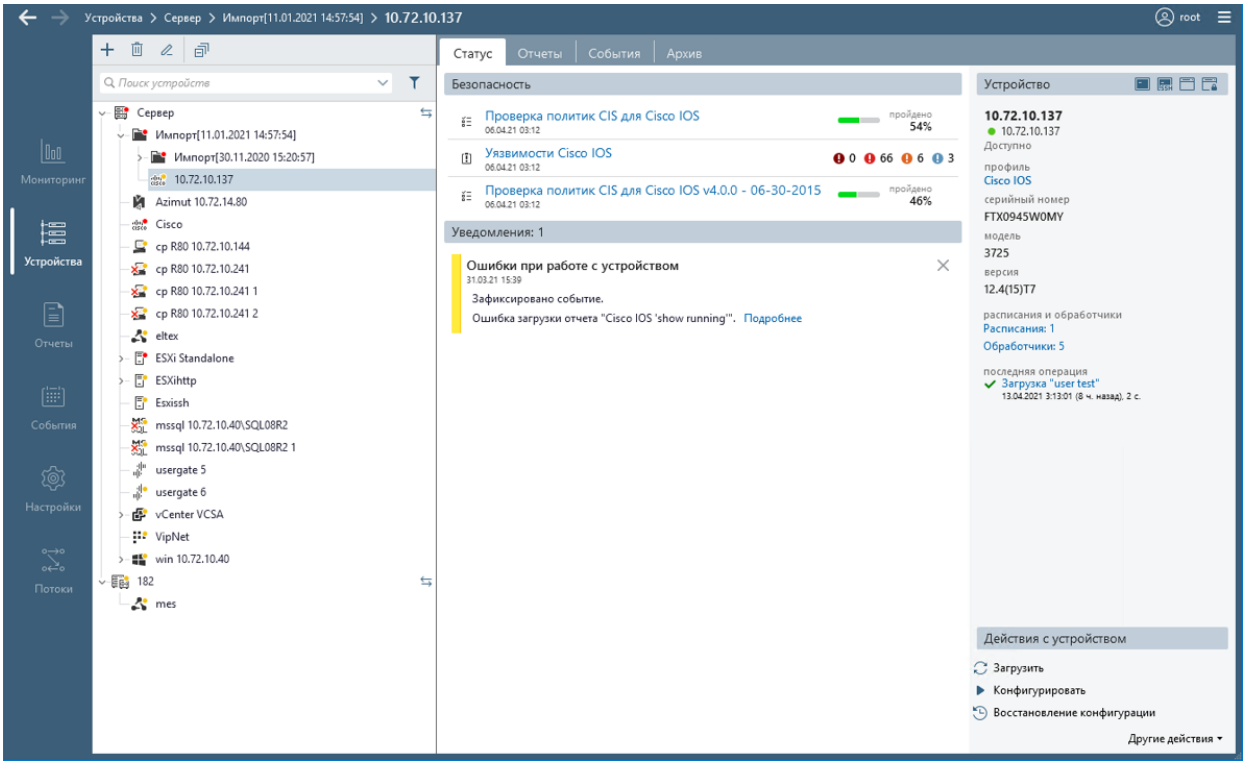


Рисунок 30 – Клиентская консоль. Раздел **Устройства**

Доступность действий с устройствами определяется назначенными пользователю администратором прав доступа к устройствам (см. п. 1.2 «Пользователи ПК «Efros Config Inspector» v.4»).

Рабочая область раздела **Устройства** разделена на:

- панель списка устройств.
- вкладки: ***Статус***, ***Отчеты***, ***События*** (группировка списка событий во вкладке по умолчанию отсутствует), ***Архив*** и ***Устройства*** (вкладка отображается только для групп).

Примечание – Размер панелей и вкладок настраивается перемещением с помощью «мыши» границ панелей/вкладок, расположенных во внутренней части рабочей области.

2.4.1. Панель списка устройств

Панель списка устройств (рис. 31) содержит:

- панель элементов управления устройствами (группами устройств). Перечень и назначение элементов управления приведены в таблице 4;
- поле поиска устройства/группы устройств. Позволяет выполнить поиск в списке устройств по комбинации букв и символов из названия искомого устройства/группы;
- кнопку ***Фильтр*** ( ). По нажатию кнопки открывается окно фильтрации, в котором возможно установить фильтр поиска, по признакам *Типы*, *Состояние*, *Уведомления*» или сбросить настройки фильтра;

– древовидный список устройств.

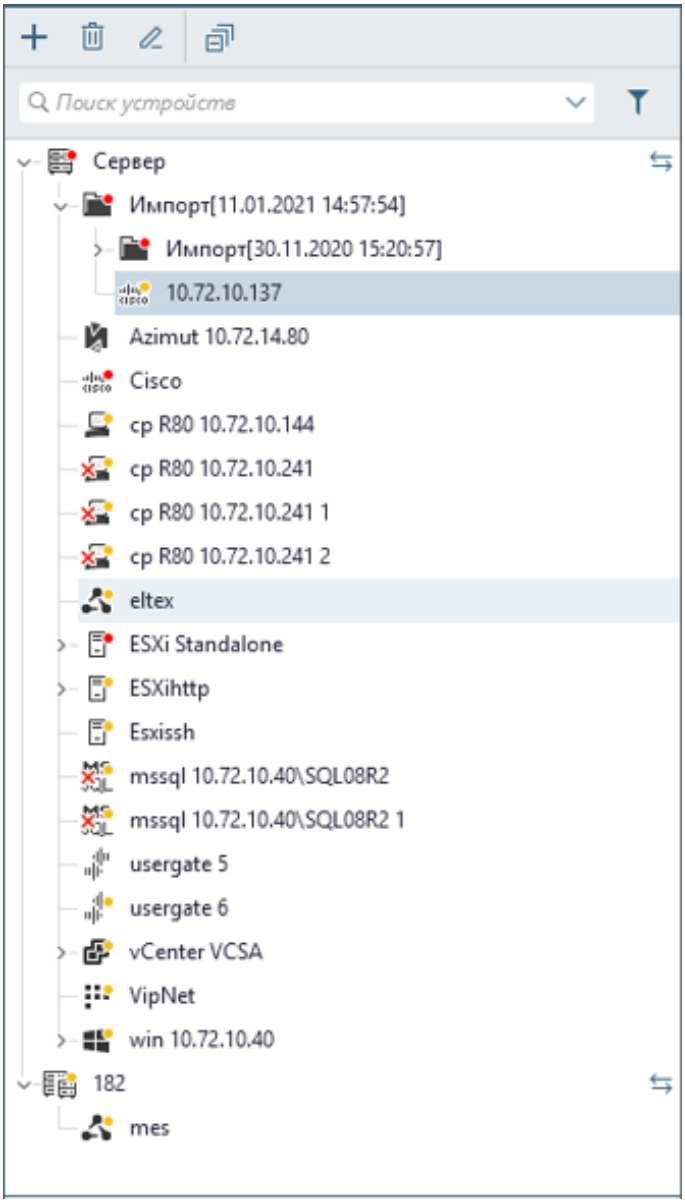


Рисунок 31 – Панель списка устройств

Таблица 4 – Перечень и назначение элементов управления панели списка устройств

Элемент управления	Внешний вид	Назначение
Кнопка ***Добавить***		Открывает окно добавления нового устройства или новой группы устройств, для ввода общих сведений об устройстве и назначения прав доступа пользователей к устройству (группе). (см. п. 2.5.2.1 «Добавление устройства», п. 2.5.1.1 «Добавление группы»).
Кнопка ***Удалить***		Открывает окно подтверждения удаления, выделенного в текущий момент времени в списке устройства/группы устройств. После нажатия в окне кнопки ***Удалить***, удаляются все данные соответствующего устройства или группы устройств (удаляются данные группы и всех устройств, входящих в группу).

Элемент управления	Внешний вид	Назначение
		Примечание – Корневая группа устройств не доступна для удаления, кнопка ***Удалить*** для нее будет неактивна
Кнопка ***Свойства***		Открывает окно редактирования параметров для выделенного в текущий момент времени в списке устройства/группы устройств (см. пункты 2.5.1.6 «Изменение параметров группы», 2.5.2.5 «Изменение параметров устройства»).
Кнопка ***Свернуть все***		Предназначена для отображения только групп (типов, профилей) контролируемого текущей серверной частью комплекса оборудования – для просмотра списка оборудования, входящего в группу (тип, профиль), необходимо нажать на кнопку раскрытия, расположенную слева от имени группы (типа, профиля).

ПК «Efros Config Inspector» v.4 поддерживает иерархию подключенных серверов. В разделе **Устройства** (в том числе и в дереве списка) могут отображаться данные только с трех серверов одновременно. При настроенной иерархии в строке выбранных для отображения в текущий момент времени серверов расположена кнопка ***Выбор серверов*** «⇆». По нажатию кнопки открывается окно **Выбор серверов** (см. рис. 32) со списком доступных для выбора в соответствии с иерархией серверов. Выбор осуществляется установкой флагов и применяется по нажатию кнопки ***Выбрать.*** До окончания процесса подключения выбранных серверов и отображения их данных в разделе **Устройства** в правой нижней части консоли будет отображаться баннер с данными о ходе подключения серверов.

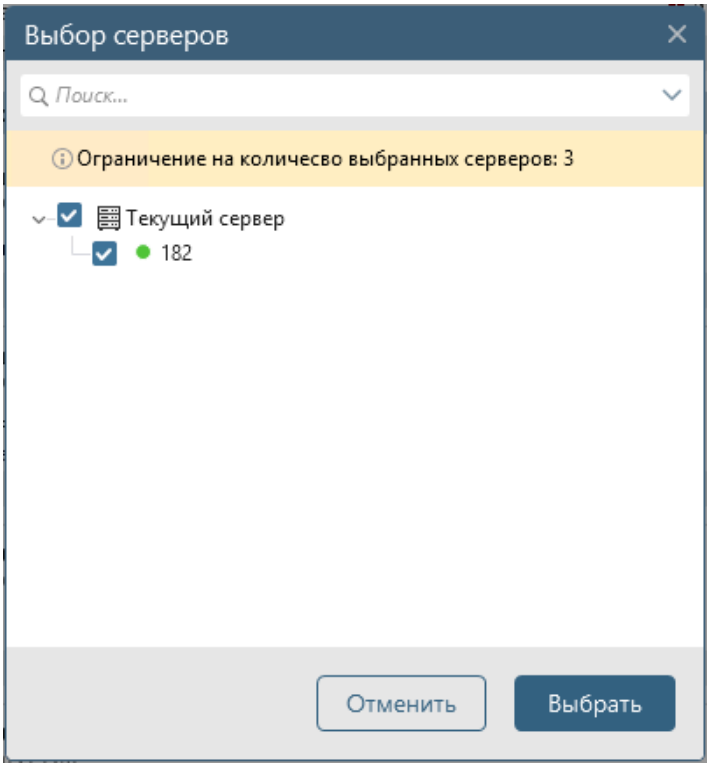


Рисунок 32 – Окно выбора серверов

В панели списка устройств объекты обладают контекстным меню для быстрого доступа к основным функциям (рис. 33).

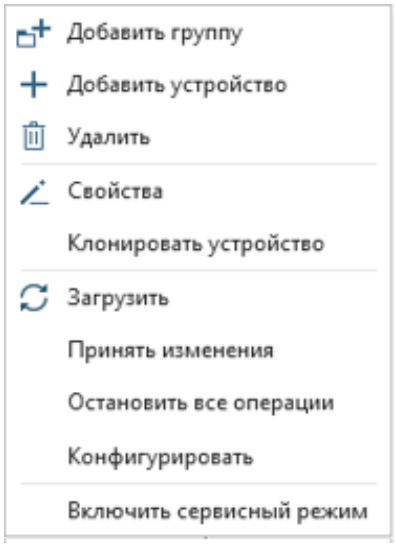


Рисунок 33 – Контекстное меню устройства

Контекстное меню содержит команды ***Добавить группу***, ***Добавить устройство***, ***Удалить, Свойства***, описание которых приведено в таблице 4, и дополнительно команды:

- ***Загрузить –*** для запуска загрузки всех доступных и разрешенных (при настройке) для выделенных устройств/группы устройств отчетов (см. п.2.8.2 «Загрузка отчетов для устройства/группы устройств»);
- ***Принять изменения –*** для запуска задания подтверждения изменений всех конфигурационных файлов и списков выделенных устройств/группы устройств;
- ***Клонировать устройство –*** для создания нового устройства на основе параметров выбранного устройства;
- ***Остановить все операции –*** для остановки выполнения проверок и загрузки отчетов на выделенных устройствах или на всех устройствах, входящих в выделенную группу;
- ***Конфигурировать –*** для выполнения действий по конфигурированию выбранного устройства;
- ***Включить сервисный режим –*** для выполнения перевода устройства в сервисный режим.

В контекстном меню группы пункт ***Клонировать устройство*** неактивен, пункт пункт ***Конфигурировать*** заменен на ***Конфигурация устройств***, пункт ***Включить сервисный режим*** – отсутствует. В контекстном меню корневой группы пункт ***Удалить*** неактивен (***Корневую группу*** удалить нельзя).

Для возможности добавления контролируемых устройств необходимо предварительно выполнить подключение внешнего модуля, обеспечивающего подключение устройств соответствующего типа, для чего обратиться к администратору ПК «Efros Config Inspector» v.4 (выполняется в соответствии с руководством администратора ПК «Efros Config Inspector» v.4).

В верхнем правом углу пиктограммы устройства может отображаться признак его состояния – круг, цвет которого отображает текущее состояние устройства (возможные варианты отображения пиктограммы и соответствующие им состояния устройства приведены в таблице 5).

Таблица 5 – Возможные состояния устройства

Пиктограмма	Состояние устройства
Отсутствует	Нормальное состояние устройства
Круг зеленого цвета	Выполнение операции, запущенной из текущей консоли
Круг желтого цвета	Обнаружено событие контроля (например, не пройдена проверка устройства)
Круг красного цвета	При выполнении операции на устройстве возникла ошибка: при загрузке отчета, нарушена целостность отчета и т.д.

В левой части пиктограммы устройства может отображаться:

- красный крест, который свидетельствует о том, что последняя выполняемая с устройством операция закончилась ошибкой;
- красный ключ, который указывает, что последняя операция с устройством закончилась ошибкой аутентификации;
- оранжевый ключ, который означает, что устройство переведено в сервисный режим.

В верхнем правом углу пиктограммы группы устройств, в которую входит хотя бы одно устройство, для которого:

- обнаружено событие – будет отображаться круг желтого цвета;
- обнаружена ошибка – будет отображаться круг красного цвета.

Все объекты в панели списка устройств, за исключением ***Корневой группы***, можно перемещать. Для этого следует выделить один или несколько (с использованием клавиш **<Ctrl>** или **<Shift>**) объектов (устройств и/или групп) и, зажав левую кнопку «мыши», переместить их в нужную группу.

2.4.2. Вкладка Статус

Вкладка ***Статус*** (рис. 34) содержит сведения, относящиеся к устройству/группе устройств, выделенному в панели списка устройств. Вкладка разделена на панели:

- **Безопасность** (см. подпункт 2.4.2.1);
- **Уведомления (список уведомлений)** (см. подпункт 2.4.2.2);
- **Устройство** (см. подпункт 2.4.2.3);
- **Состояние устройств** (только для группы) (см. подпункт 2.4.2.4);
- **Уведомления (диаграмма категорий уведомлений)** (только для группы) (см. подпункт 2.4.2.5);
- **Действия с устройством** (см. подпункт 2.4.2.6).

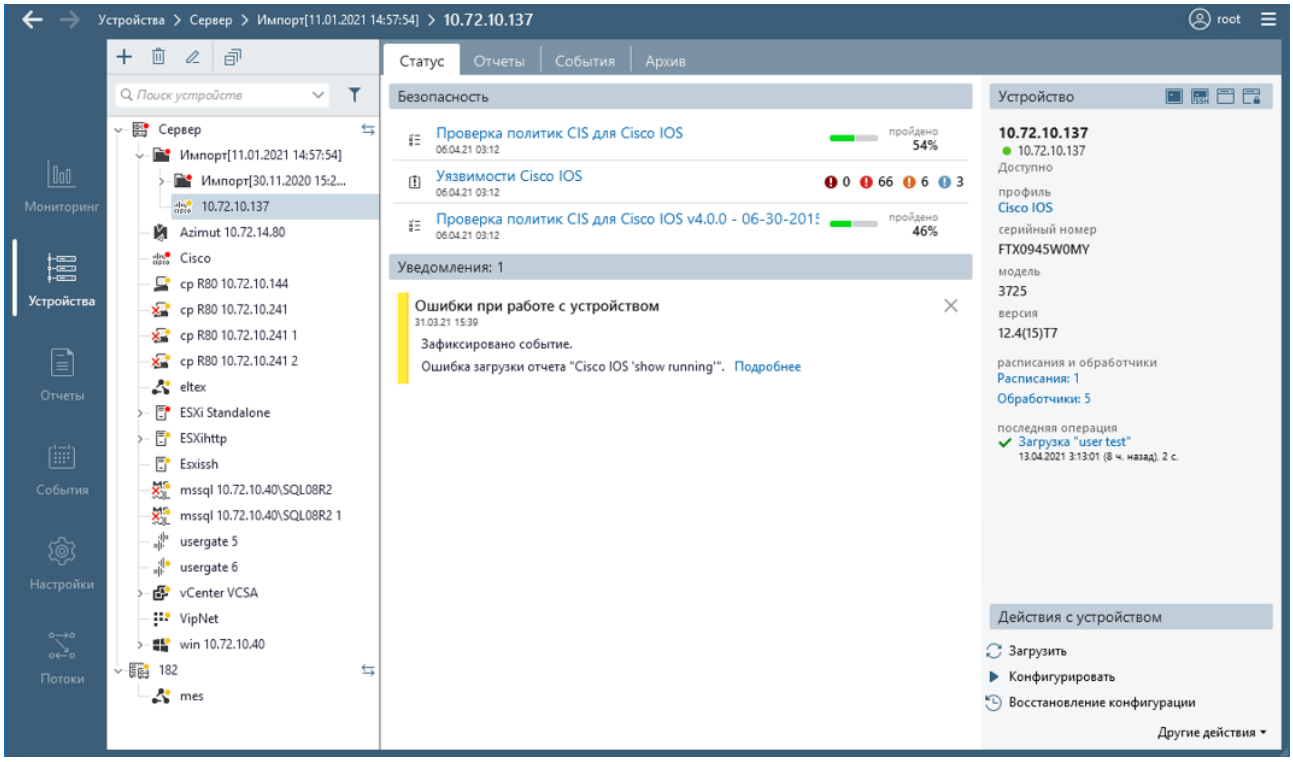


Рисунок 34 – Вкладка ***Статус*** для устройства

2.4.2.1. Панель Безопасность

Информация, отображаемая в панели *Безопасность* вкладки ***Статус*** для группы устройств и отдельного устройства, отличается. Для отдельного устройства (см. пример на рис. 35) в панели *Безопасность* отображается информация о результатах выполнения на нем проверок, для группы устройств (см. пример на рис. 36) – суммарные результаты выполнения проверок для всех устройств, входящих в выделенную группу.

Результаты выполнения проверок безопасности для отдельного устройства представлены в виде процента положительного завершения выполнения для каждого из правил, содержащихся в проверке этого устройства, для группы в заголовке блока **Проверки безопасности** – общий процент положительного завершения выполнения правил, содержащихся в проверке, для всех устройств, входящих в группу, и в списке блока ***Типов устройств –*** для устройств каждого типа отдельно.

Результат выполнения проверок на наличие уязвимостей для отдельного устройства представлен в виде количества уязвимостей, найденных при выполнении проверки, по уровню критичности (критичность по CVSS, рассчитанная БДУ):

- «» – *Критический*;
- «» – *Высокий*;
- «» – *Средний*;
- «» – *Низкий*;
- «» – *Скрытые уязвимости* – уязвимости на устройствах, скрытые пользователем средствами сервера ПК. При отсутствии скрытых уязвимостей, пиктограмма «» и количество «0» не отображаются.

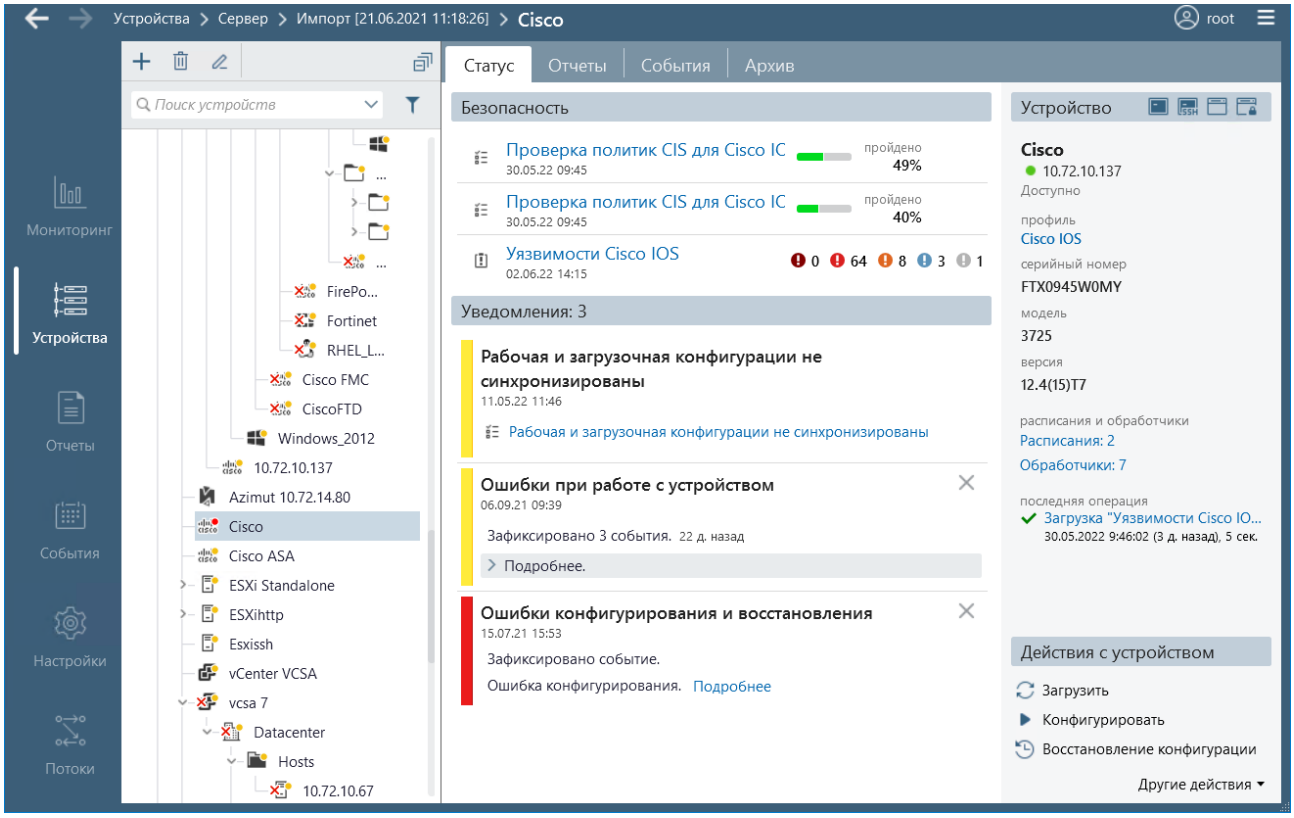


Рисунок 35 – Пример просмотра панели *Безопасность* для устройства

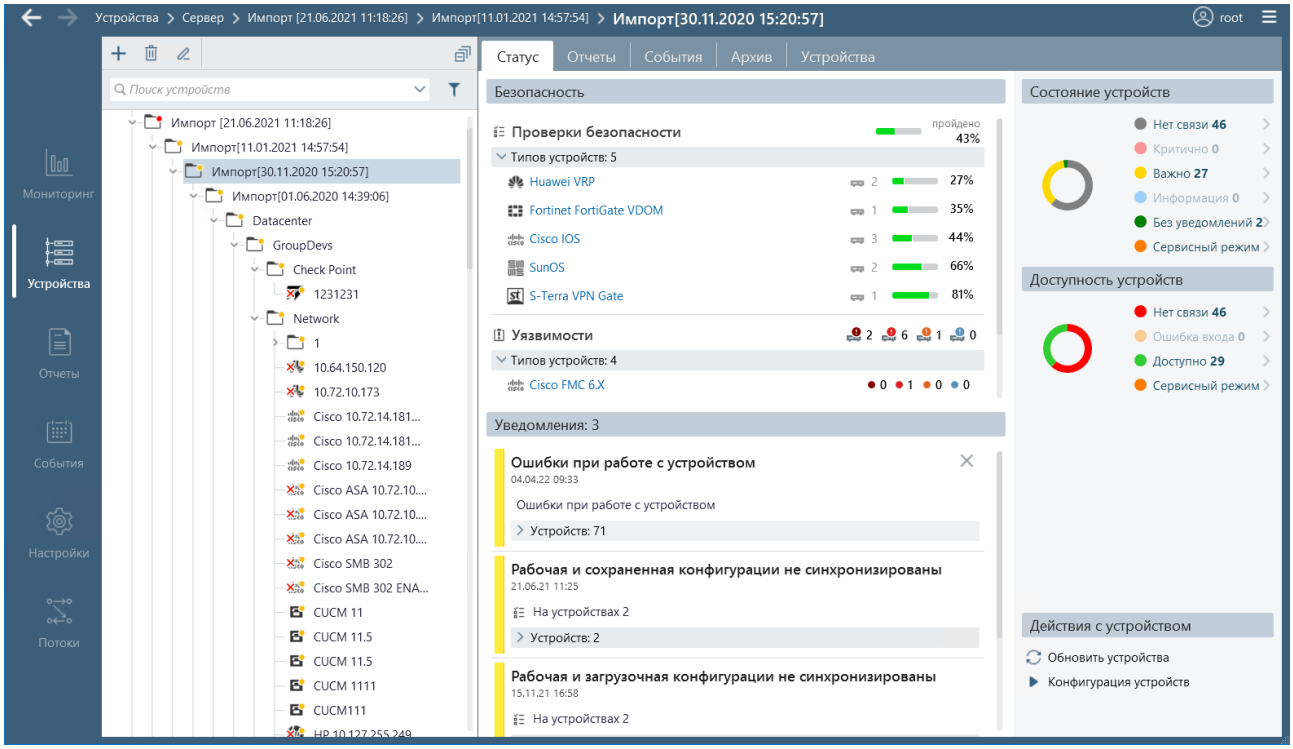


Рисунок 36 – Пример просмотра панели *Безопасность* для группы устройств

Примечание – Пользователь с полными правами на устройстве имеет возможность скрыть уязвимости в отчете по уязвимостям устройства. (подробнее см. п. 2.9.1.4 «Скрытие уязвимостей») или в общем отчете по уязвимостям (подробнее см. п. 2.12.1.2 «Ввод параметров отчета и просмотр отчета для типа шаблона *Уязвимости устройств*»).

Результат выполнения проверок на наличие уязвимостей для группы в заголовке блока **Уязвимости** содержит количество устройств, из числа входящих в группу, для каждого уровня критичности уязвимости: *Критический*, *Высокий, Средний* или *Низкий*, наличие скрытых уязвимостей не учитывается, и в списке блока ***Типов устройств*** – для устройств каждого типа отдельно (в том числе отображается количество отключенных уязвимостей, при их наличии хотя бы для одного типа устройств).

При отображении результатов проверки на наличие уязвимостей используется следующий принцип подсчета количества устройств по типам уязвимостей:

- *Критический* уровень – количество устройств, при проверке которых обнаружена хоть одна уязвимость с *Критическим* уровнем;
- *Высокий* уровень – количество устройств, при проверке которых не обнаружено уязвимостей с *Критическим* уровнем, а выявлена хоть одна уязвимость с *Высоким* уровнем критичности;
- *Средний* уровень – количество устройств, при проверке которых не обнаружено уязвимостей с *Критическим* или *Высоким* уровнем, а выявлена хоть одна уязвимость со *Седним* уровнем критичности;
- *Низкий* уровень – количество устройств, при проверке которых не обнаружено уязвимостей с *Критическим, Высоким* или *Средним* уровнем, а выявлена хоть одна уязвимость с *Низким* уровнем критичности.

Интерфейс панели *Безопасность* позволяет просмотреть типы устройств группы, по которым выявлены указанные уязвимости.

2.4.2.2. Панель Уведомления (список уведомлений)

В панели *Уведомления* со списком уведомлений вкладки ***Статус*** отображаются уведомления о произошедших событиях контроля устройства (группы устройств) и об ошибках выполнения заданий. Уведомление содержит:

- заголовок – наименование уведомления;
- дату и время отправки уведомления;
- наименование устройства или список устройств, с которыми связано уведомление, (отображается в панели *Уведомления* только для групп устройств);
- текст уведомления.

Наименование устройства в списке уведомлений группы является ссылкой, при переходе по которой в разделе **Устройства** консоли открывается вкладка ***Статус*** с данными выбранного устройства. Текст уведомления может содержать ссылку на отчет, по результатам которого было отправлено уведомление.

Заголовок уведомления может содержать в правом верхнем углу кнопку ***Удалить уведомление*** «✕» - для удаления выбранного уведомления (кнопка есть только во вкладке ***Статус*** для выбранного устройства), или кнопку ***Принять новую версию за эталон*** «✓» - для принятия новой версии загруженного отчета за эталон.

Уведомления удаляются из списка уведомлений в зависимости от их типа следующим образом:

- ***Проверка не пройдена*** – только автоматически после успешного прохождения соответствующей проверки;
- событие выполнение триггера (например, ***Ошибки при работе с устройством*** – по нажатию кнопки ***Удалить уведомление*** (✕) во вкладке **Статус** устройства);
- ***Нарушение целостности*** – либо после принятия новой версии отчета в качестве эталона по нажатию кнопки ***Принять новую версию за эталон*** (✓), либо после отмены изменений конфигурации оборудования и проведения повторной загрузки отчета.

Внешний вид панели *Уведомления* со списком уведомлений при отсутствии уведомлений приведен на рисунке 37.

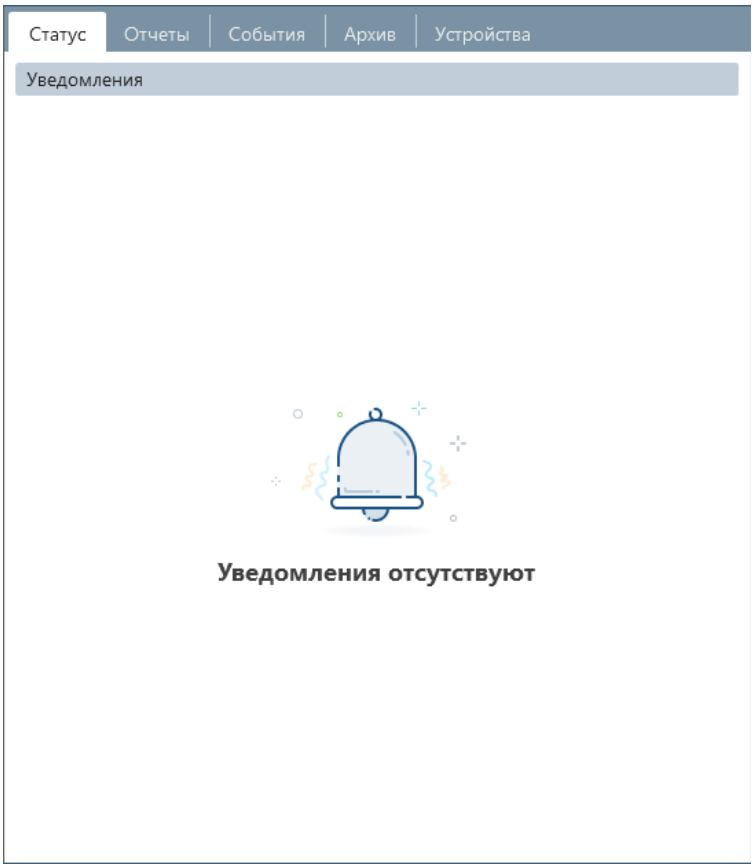


Рисунок 37 – Внешний вид панели *Уведомления* со списком уведомлений при отсутствии уведомлений

2.4.2.3. Панель Устройство

Пример панели *Устройство* вкладки ***Статус*** приведен на рис. 38.

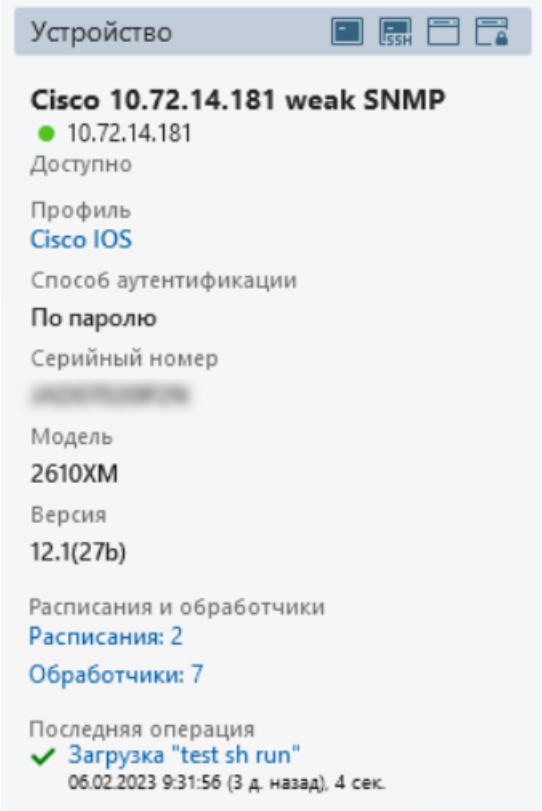


Рисунок 38 – Панель *Устройство*

Панель содержит:

- название модели устройства и версию установленного на устройстве ПО (если оно есть у устройства),
- текущий статус устройства:
  а) ***нет связи*** – последняя операция с устройством (загрузка отчетов, проверка связи) завершилась ошибкой;
  б) ***ошибка входа*** – при выполнении операции с устройством (загрузка отчетов, проверка связи) произошла ошибка аутентификации;
  в) ***доступно*** – последняя операция с устройством выполнена успешно;
  г) ***сервисный режим –*** устройство переведено в сервисный режим;
- область *Профиль* с наименованием профиля настроек устройства. Является ссылкой для перехода в форму просмотра и настройки параметров (при наличии прав на внесение изменений) соответствующего профиля;
- общие данные об устройстве, указанные при добавлении/редактировании устройства (если у устройства есть DNS-имя и IP-адрес (они отличаются), то отображаются оба адреса),
- область *Расписания и обработчики* с двумя ссылками:
  а) ***Расписания*** – открывает вкладку *Расписания* (рис. 39) окна свойств выбранного устройства (содержит данные только включенных (активных) и разрешенных к использованию для выбранного устройства расписаний);

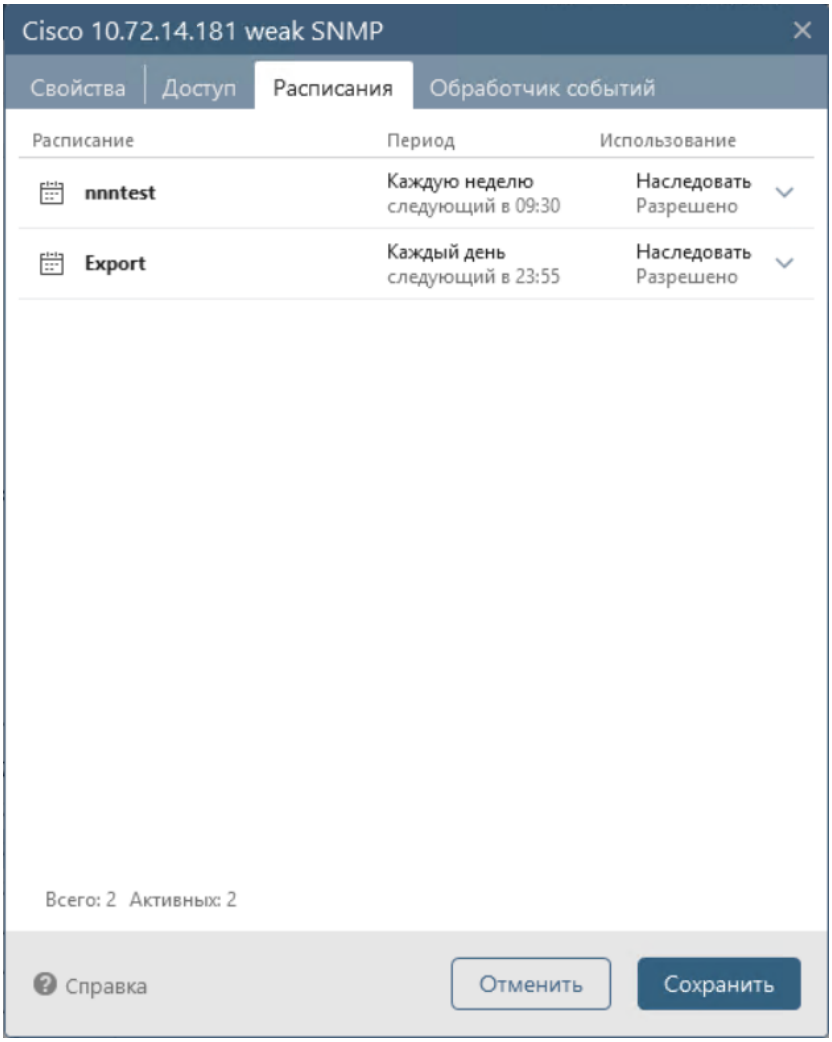


Рисунок 39 – Вкладка *Расписания*

б) ***Обработчики*** – открывает вкладку *Обработчик событий* (рис. 40) окна свойств выбранного устройства (содержит список триггеров, связанных с выбранным устройством (данные только включенных (активных) и разрешенных к использованию для выбранного устройства обработчиков событий);

- область *Последняя операция* с информацией о результатах выполнения последней операции с устройством, с указаним даты, времени и длительности выполнения операции и ссылкой для открытия окна с отчетом о выполнении операции, пример отчета приведен на рис. 41.

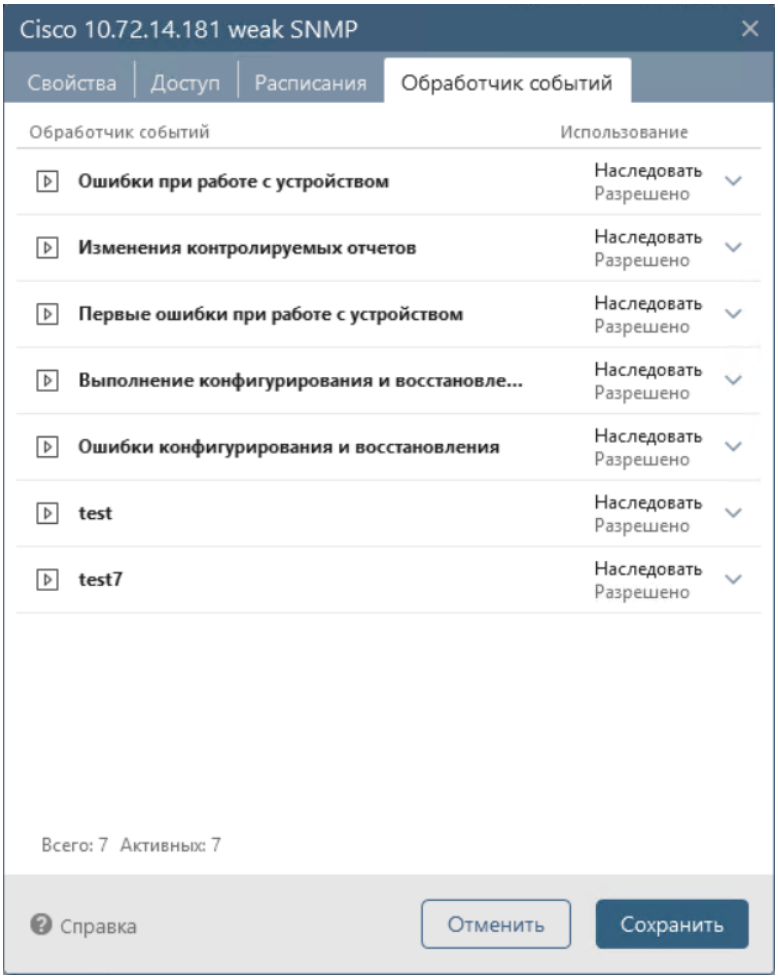


Рисунок 40 – Вкладка *Обработчики событий*

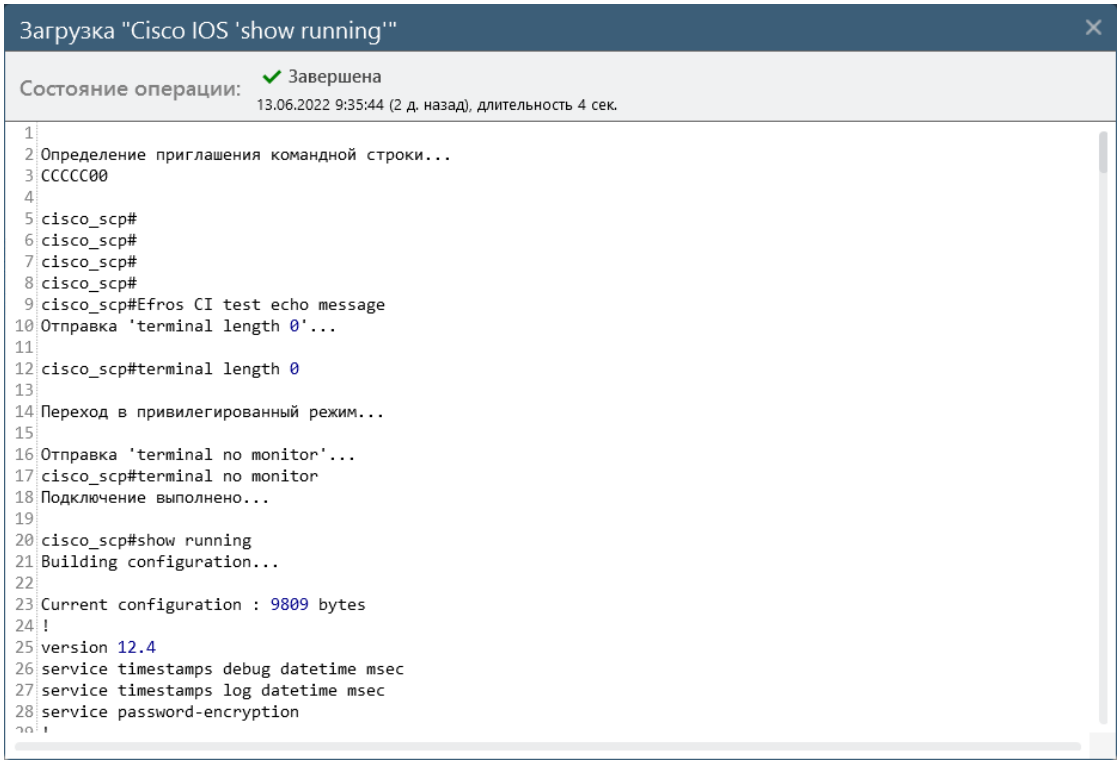


Рисунок 41 – Окно результатов выполнения операции *Загрузка «Cisco IOS ‘show running ‘»*

Для группы устройств панель *Устройство* во вкладке не отображается.

Заголовок панели может содержать кнопки запуска внешних программ для соединения с контролируемым устройством по протоколам SSH, Telnet, HTTP и HTTPs. Состав кнопок зависит от типа устройства. Активность кнопки зависит от разрешения запуска соответствующей программы в окне **Настройки запуска внешних программ** (подробнее см. п. 2.1.3 «Настройки запуска внешних программ»).

Например, на рис. 38 заголовок панели *Устройство* содержит кнопки запуска внешних программ, поддерживаемых устройствами Cisco:

 – кнопка для соединения по протоколу Telnet;

 – кнопка для соединения по протоколу SSH;

 – кнопка для соединения по протоколу HTTP;

 – кнопка для соединения по протоколу HTTPS.

2.4.2.4. Панель Состояние устройств

Панель *Состояние устройств* вкладки ***Статус*** (рис. 42) отображается только для выделенной в панели списка устройств группы и содержит графическое представление информации о статусах (состояниях) контролируемых устройств, которые входят в выделенную группу:

- ***нет связи*** – последняя операция с устройством (загрузка отчетов, проверка связи), входящим в выделенную группу, завершилась ошибкой;
- ***ошибка входа*** – при выполнении операции с устройством (загрузка отчетов, проверка связи), входящим в выделенную группу, произошла ошибка аутентификации;
- ***доступно*** – последняя операция с устройством, входящим в выделенную группу, выполнена успешно;
- ***сервисный режим*** – устройство, входящее в выделенную группу, переведено в сервисный режим.

Для каждого статуса приводятся сведения о количестве устройств выделенной группы в соответствующем состоянии.

При выборе одного из состояний устройств (щелчок левой кнопкой «мыши» на строке) происходит переход во вкладку ***Устройства*** выделенной в панели устройств группы. Во вкладке ***Устройства*** будет отображаться список устройств группы в выбранном состоянии – активирован соответствующий фильтр группы ***Состояние*** (подробнее о вкладке ***Устройства*** см. п. 2.4.6 «Вкладка Устройства» настоящего Руководства).

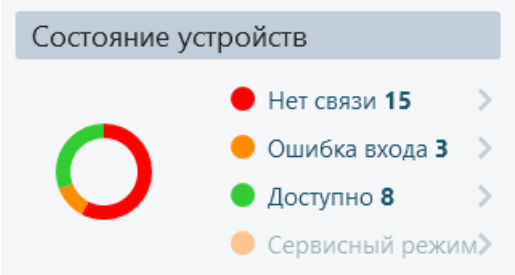


Рисунок 42 – Панель *Состояние устройств*

2.4.2.5. Панель Уведомления (диаграмма категорий уведомлений)

Панель *Уведомления* с диаграммой категорий уведомлений вкладки ***Статус*** (рис. 43) отображается только для выделенной в панели списка устройств группы и содержит графическое представление информации о наличии уведомлений различных категорий, поступивших с устройств группы.

Рисунок 43 – Панель *Уведомления* с диаграммой категорий уведомлений

Также приводятся сведения о количестве устройств выделенной группы для каждого из возможных категорий уведомлений. При выборе одной из категории уведомлений устройств (щелчок левой кнопкой «мыши» на имени категории) происходит переход во вкладку ***Устройства*** выделенной в панели устройств группы, в списке устройств которой отображаются устройства с выбранной категорией уведомлений – активирован соответствующий фильтр группы ***Уведомления*** (подробнее о вкладке ***Устройства*** см. п.2.4.6 «Вкладка Устройства»).

2.4.2.6. Панель Действия с устройством

Блок полей *Действия с устройством* (см. рис. 34) содержит перечень основных операций, которые доступны для выполнения на выбранном устройстве/группе с сервера ПК. Список доступных операций в области ***Действия с устройством*** зависит от типа устройства/группы.

Для устройств список может содержать операции ***Загрузить, Конфигурировать, Восстановление конфигурации***. В нижней части блока расположен раскрывающийся список ***Другие действия***, в котором размещаются действия с устройством, не вошедшие в основной список блока, (например, ***Проверить соединение***, ***Скопировать running в startup***) и активные кнопки запуска внешних программ.

Для группы устройств список содержит операции ***Обновить устройства***, при выборе которой обновляются все отчеты на вложенных устройствах, и

Конфигурация устройств, при выборе которой открывается окно **Конфигурирование оборудования** (рис. 44).

Примечание – Если в панели списка устройств выбрано устройство, не поддерживающее конфигурирование, или группа таких устройств, то операции ***Конфигурировать, Восстановление конфигурации*** и ***Конфигурация устройств*** будут отсутствовать в панели.

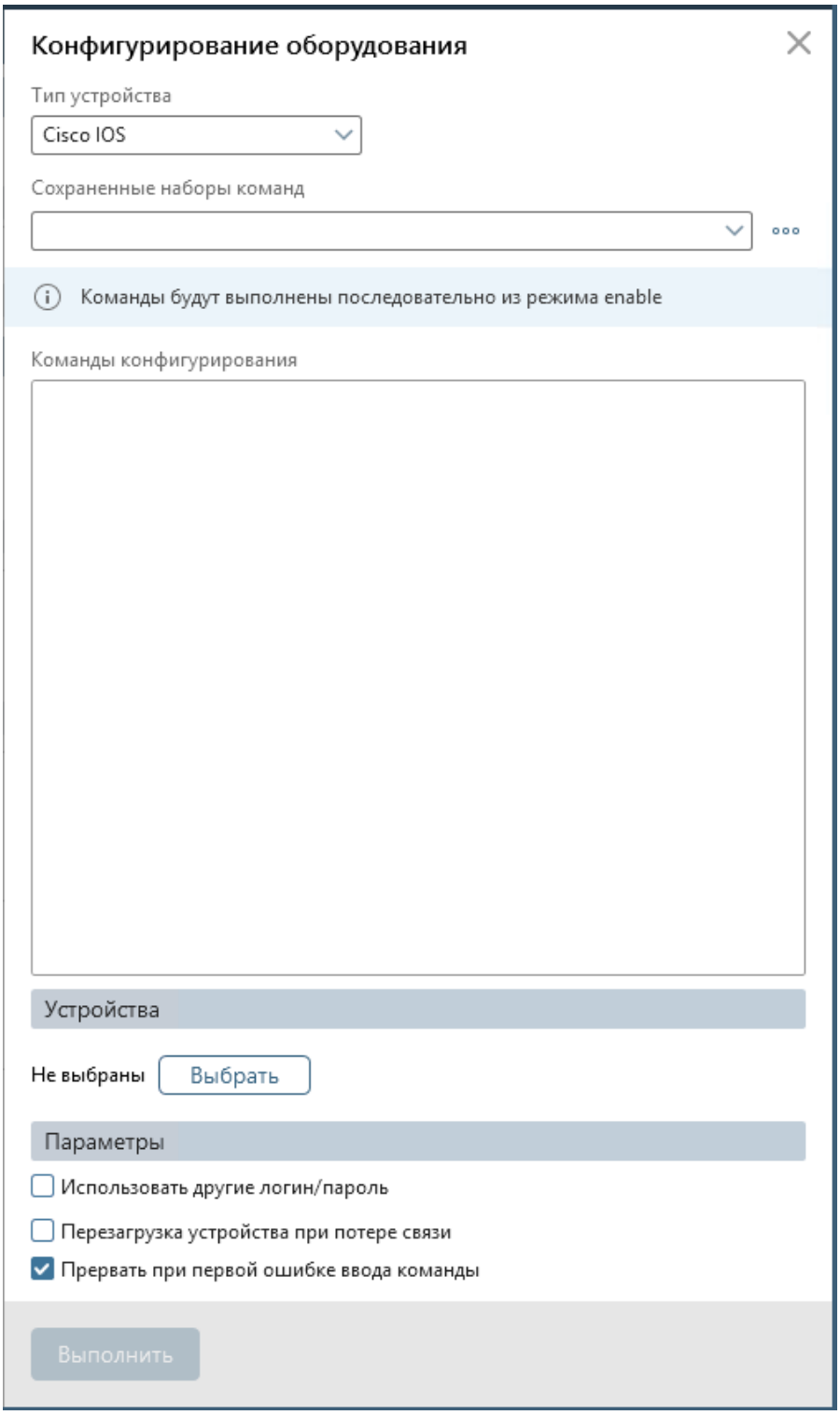


Рисунок 44 – Окно **Конфигурирование оборудования**

2.4.3. Вкладка Отчеты

Вкладка ***Отчеты*** раздела **Устройства** (рис. 45) содержит список отчетов, разрешенных для загрузки с выбранного устройства/группы. По умолчанию используется группировка отчетов по их формату (***Конфигурации***, ***Проверки***). В заголовке групп отображается количество активных отчетов (во всех состояниях, кроме *Запрещено* (см. ниже)) соответствующего формата для устройства.

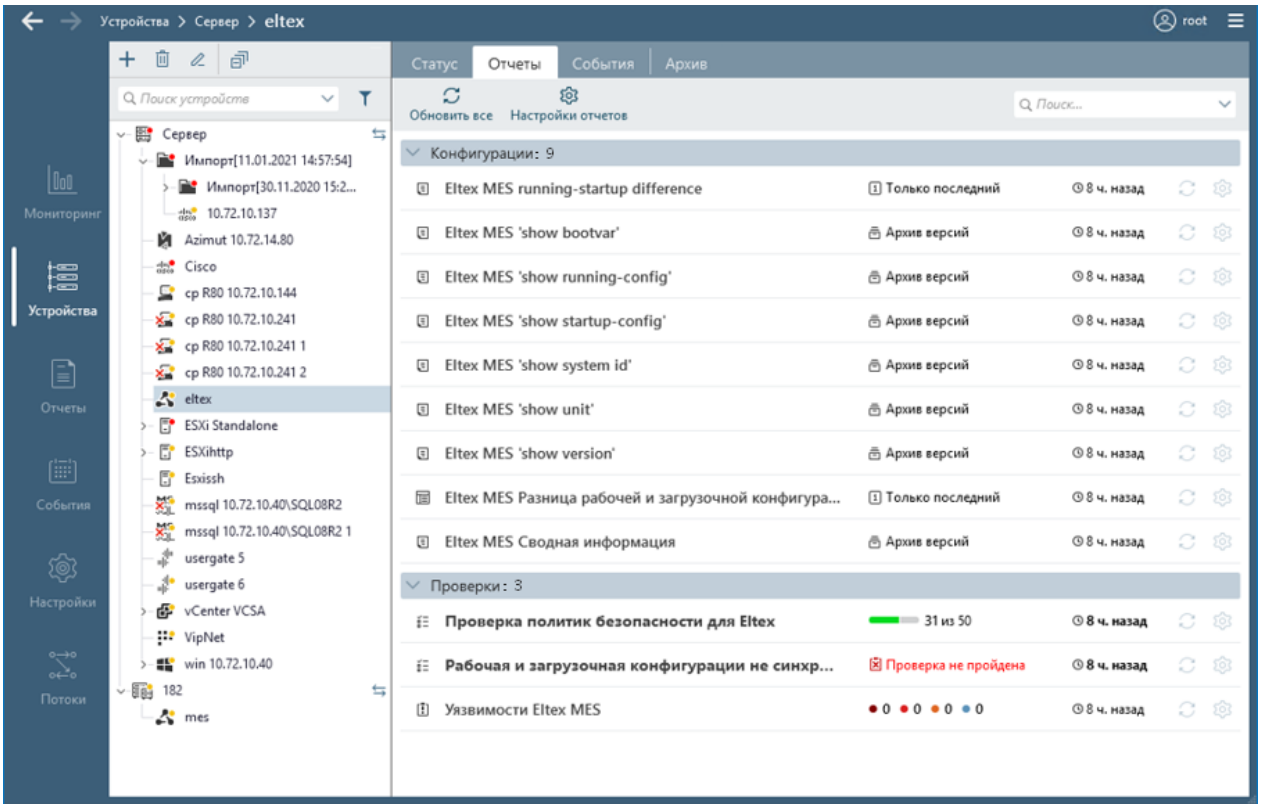


Рисунок 45 – Вкладка **Отчеты**

Для каждого отчета построчно отображаются:

- пиктограмма типа отчета:
  а) отчеты формата ***Конфигурации*** – общие (встроенные) отчеты: текстовый «» и структурированный «», пользовательский отчет «» и отчет типа *Фильтр* «», созданный на основе другого отчета путем фильтрации данных;
  б) отчеты формата ***Проверки*** – пользовательская проверка «», стандартная проверка «», проверки по межсетевым экранам (МЭ) «» и проверка на уязвимости «»;
- название отчета;
- состояние загруженного отчета в БД комплекса;
- время, прошедшее с момента загрузки последней версии отчета. В случае ошибки загрузки отчета с устройства в поле ***Дата обновления*** такого отчета появится соответствующее сообщение;
- кнопка ***Обновить*** () – для запуска обновления отчета;
- кнопка ***Настройки*** () – для перехода в окно настройки отчета (см. п. 2.6 «Настройка отчетов устройств»).

Возможные значения состояния загруженного отчета формата ***Конфигурации*** соответствуют варианту его использования для контролируемого устройства (подробнее о настройке отчетов см. п. 2.6 «Настройка отчетов устройств»):

- ***Контроль изменений*** – выполняется контроль целостности версии отчета, принятой за эталон, в случае если загруженная с устройства версия отчета отличается от версии, принятой за эталон, пользователю выдается оповещение;
- ***Архив версий*** – в БД комплекса сохраняются все загруженные версии отчета, отличные от первой загруженной. Контроль целостности (КЦ) не выполняется;
- ***Только последний*** – в БД комплекса сохраняется только последняя загруженная с устройства версия отчета, вне зависимости от наличия в ней изменений относительно предыдущей версии. КЦ не выполняется, изменения отчета не контролируются;
- ***Запрещено*** – загрузка отчета с устройств запрещена вне зависимости от настроек базового профиля;
- ***Наследовать (XXXXXX)*** – применяются настройки базового профиля. В скобках отображается значение, установленное в базовом профиле: *Контроль изменений, Архив версий, Только последний* или *Запрещено*.

Возможные значения состояния загруженного отчета формата ***Проверки:***

- ***для отчетов по оптимизации правил*** – количество теневых и избыточных правил, а также при их наличии – неиспользуемых и нулевых правил;
- ***для отчетов по уязвимости устройств*** – количество уязвимостей, найденных при выполнении проверки, по уровню критичности, с учетом скрытых уязвимостей (аналогично панели Безопасность (см. п. 2.4.2.1 «Панель Безопасность»));
- ***для отчетов по проверкам безопасности*** – процент выполнения проверок в графическом виде и количество пройденных проверок из их общего числа;
- ***для других отчетов по проверкам*** – результат выполнения проверки: пройдена или не пройдена.

Для отчетов проверок МЭ (отчет оптимизации правил, отчеты зонного анализа и отчет стандартов МЭ) слева от значения состояния может отображаться признак их неактуальности в виде пиктограммы «  » (появляется при изменении настроек отчетов проверок МЭ до обновления отчета). При наведении курсора на пиктограмму отображается всплывающая подсказка *Настройки проверки изменились, для получения актуальных данных обновите отчет*. При открытии такого отчета на просмотр отображается сообщение с тем же текстом и кнопкой ***Обновить***. После обновления отчета пиктограмма исчезает.

Отчеты, запрещенные к загрузке с выбранного устройства, во вкладке ***Отчеты*** раздела **Устройства** не отображаются, доступны для просмотра и настройки в разделе **Профили**.

Во вкладке **Отчеты** пользователю доступны функции:

- обновления всех отчетов выбранного устройства по нажатию кнопки ***Обновить все*** (🔄) в заголовке вкладки ***Отчеты***;
- просмотра последней версии загруженного отчета (см. п. 2.9.1 «Просмотр отчета»);
- загрузки отчета (см. п. 2.9.2 «Просмотр истории изменений конфигурации, проверок устройства»);
- настройки отчетов (см. п. 2.6 «Настройка отчетов устройств»).

2.4.4. Вкладка События

Вкладка ***События*** раздела **Устройства** (рис. 46) содержит панели:

- списка событий;
- ***Подробности*** – с данными выбранного в списке события;
- фильтрации списка событий.

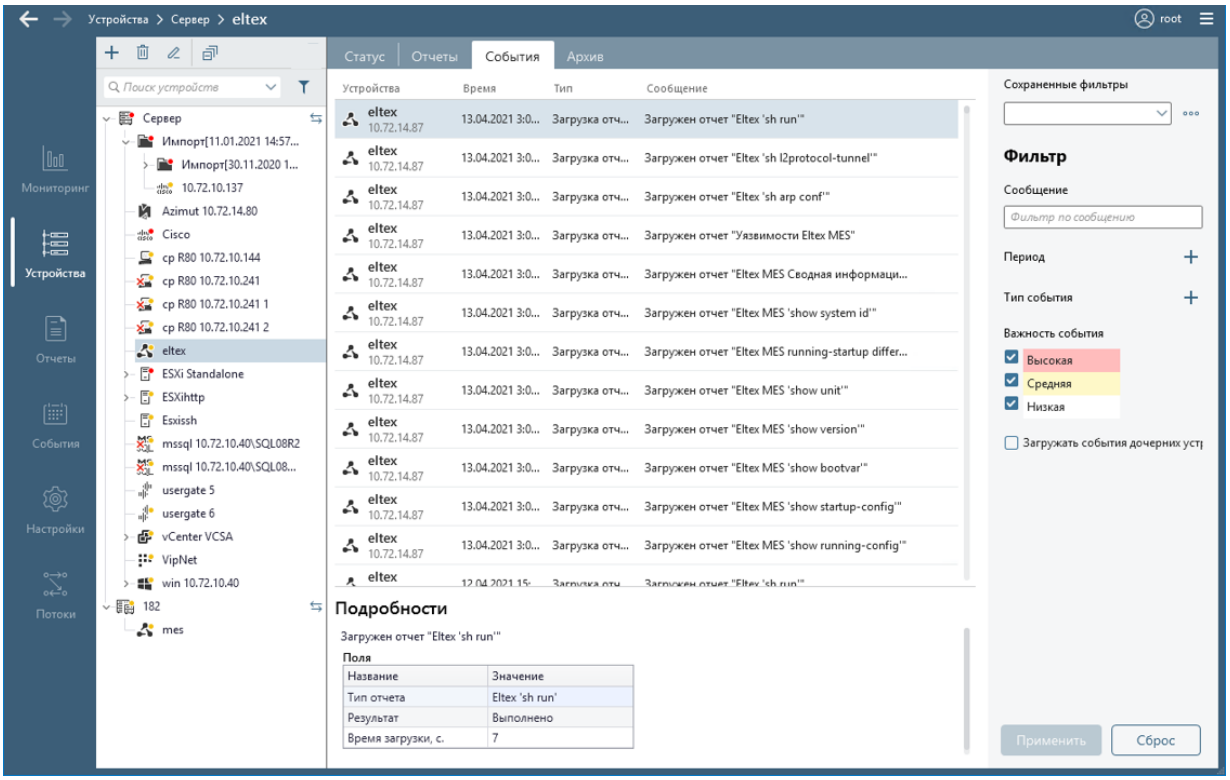


Рисунок 46 – Вкладка ***События***

Панель списка событий содержит список всех зафиксированных для устройства/группы устройств событий. Для каждого события построчно отображаются:

- наименование и IP-адрес устройства/наименование группы;
- дата и время произошедшего события;
- тип события;
- текст с кратким описанием события.

Примечание – Для отображения во вкладке событий группы событий дочерних устройств необходимо в панели фильтрации *Фильтр* установить флаг в поле *Загружать события дочерних устройств* и нажать кнопку ***Применить***.

Пользователь имеет возможность копирования текста события для последующей его обработки средствами другого ПО.

Группировка списка событий во вкладке ***События*** по умолчанию отсутствует. В панели списка событий пользователю доступны операции группировки, сортировки и фильтрации с использованием параметров, расположенных в панели фильтрации (см. п. 2.11.3 «Фильтрация событий с использованием панели фильтрации»).

Для обновления списка событий, с учетом заданных ранее пользователем правил фильтрации, необходимо нажать кнопку ***Обновить*** во всплывающем сообщении ***«Список событий изменился. Обновить»***.

2.4.5. Вкладка Архив

Вкладка ***Архив*** раздела **Устройства** (рис. 47) содержит список всех загруженных в БД комплекса версий отчетов устройства/группы, для которых установлен режим использования ***Архив версий*** или ***Контроль изменений*** (подробнее о настройке отчетов см. п. 2.6.1 «Настройка одного отчета для одного устройства»). В ***Архив*** попадают текстовые «» и структурированные «» отчеты (отчеты формата ***Конфигурации*** вкладки ***Отчеты***) и отчеты формата ***Проверки*** (обозначаются знаком «»). Эталонные отчеты помечены знаком «».

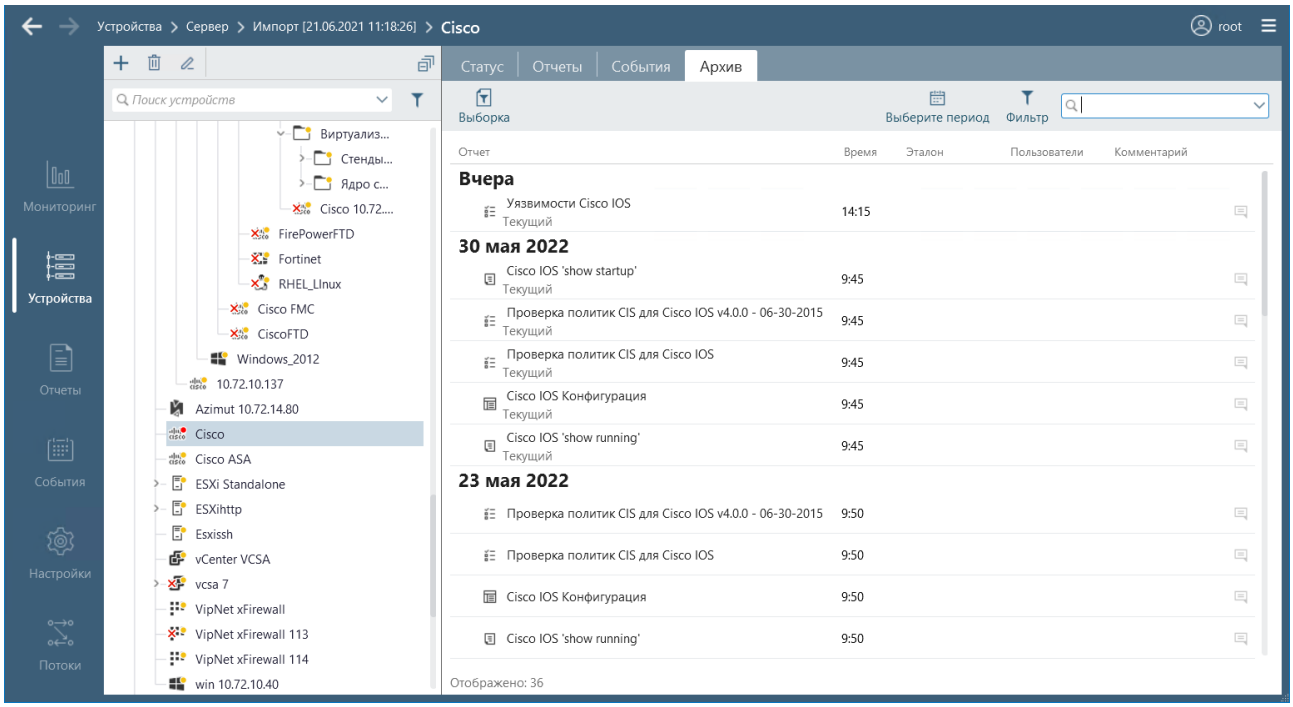


Рисунок 47 – Вкладка **Архив**

В нижней части вкладки приведено общее количество отображаемых записей. Количество отображаемых записей ограничено. Если записей более 1000, то выводятся первые 1000 записей в соответствии с заданными настройками периода и фильтрации, в окне отображается сообщение «Показано 1000 записей. Не нашли что искали? Воспользуйтесь выбором периода или фильтром». Для просмотра требуемой записи, не попавшей в число отображаемых, необходимо выбрать другой временной период и/или параметры фильтрации списка.

Список отчетов доступен пользователю для:

- настройки периода, за который отображаются записи архива. Выбор дат начала и окончания периода выполняется в окне (рис. 48), которое открывается по кнопке ***Выберите период*** (). В окне также могут быть выбраны преднастроенные периоды «*Сегодня*», «*Вчера*», «*Последние 7/14/30 дней*». Настройка применяется по нажатию кнопки ***Применить***, отменяется – по нажатию кнопки ***Очистить***;
- фильтрации по типу отчета (конфигурация/отчет о проверке), по названию отчета, по признаку эталонности (обычный/эталон/архивный эталон). Выбор и сброс фильтров выполняется в окне, которое открывается по кнопке ***Фильтр*** ();
- поиска отчетов. Поиск выполняется по мере ввода комбинации букв и символов из названия искомого отчета в поле поиска.

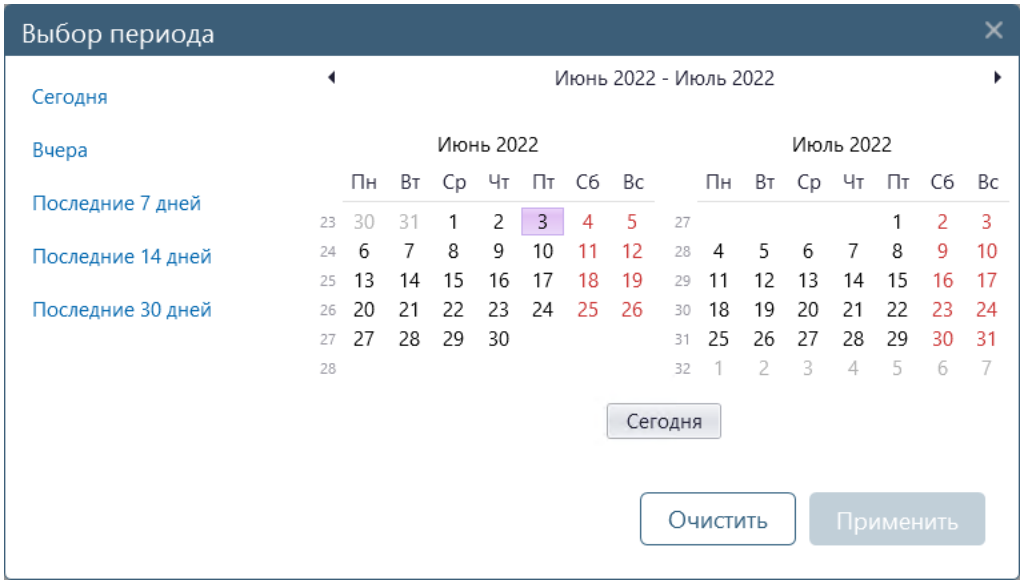


Рисунок 48 – Окно выбора периода отображаемых записей вкладки ***Архив***

Для каждого отчета построчно отображаются:

- название отчета и признак *Текущий* (отчет соответствует отчету с вкладки ***Отчеты***);
- время загрузки;
- дата и время принятия версии за эталон с указанием учетной записи пользователя, который установил версию отчета в качестве эталона (например, root 16.07.2019 13:57:48);
- имя пользователя внесшего изменения на сетевом устройстве;
- комментарий, который пользователь ввел к загруженной в архив версии отчета;
- кнопка ***Комментарий*** () для перехода в окно ввода комментария.

Во вкладке ***Архив*** пользователю доступны функции:

- просмотра отчета (см. п. 2.10.1 «Просмотр архивной версии отчета») – по двойному щелчку левой кнопки «мыши» в строке требуемого отчета;
- фильтрации отчетов по типу и времени с созданием нового отчета (см. п. 2.10.2.1 «Выборка архивных версий отчетов по типу и времени с

использованием средств управления клиентской консоли») по нажатию кнопки ***Выборка*** ();

- сравнения просматриваемой версии архивного отчета с другими отчетами (см. п. 2.10.2.2, 2.10.2.3, 2.10.2.4);
- изменения комментария к версии отчета, загруженного в архив (см. п. 2.10.2.5 «Ввод комментария к архивной версии отчета»).

2.4.6. Вкладка Устройства

При выборе в панели списка устройств раздела **Устройства** группы в рабочей области раздела появляется вкладка ***Устройства***. При переходе на эту вкладку отображается список объектов устройств, включенных в выбранную группу (рис. 49).

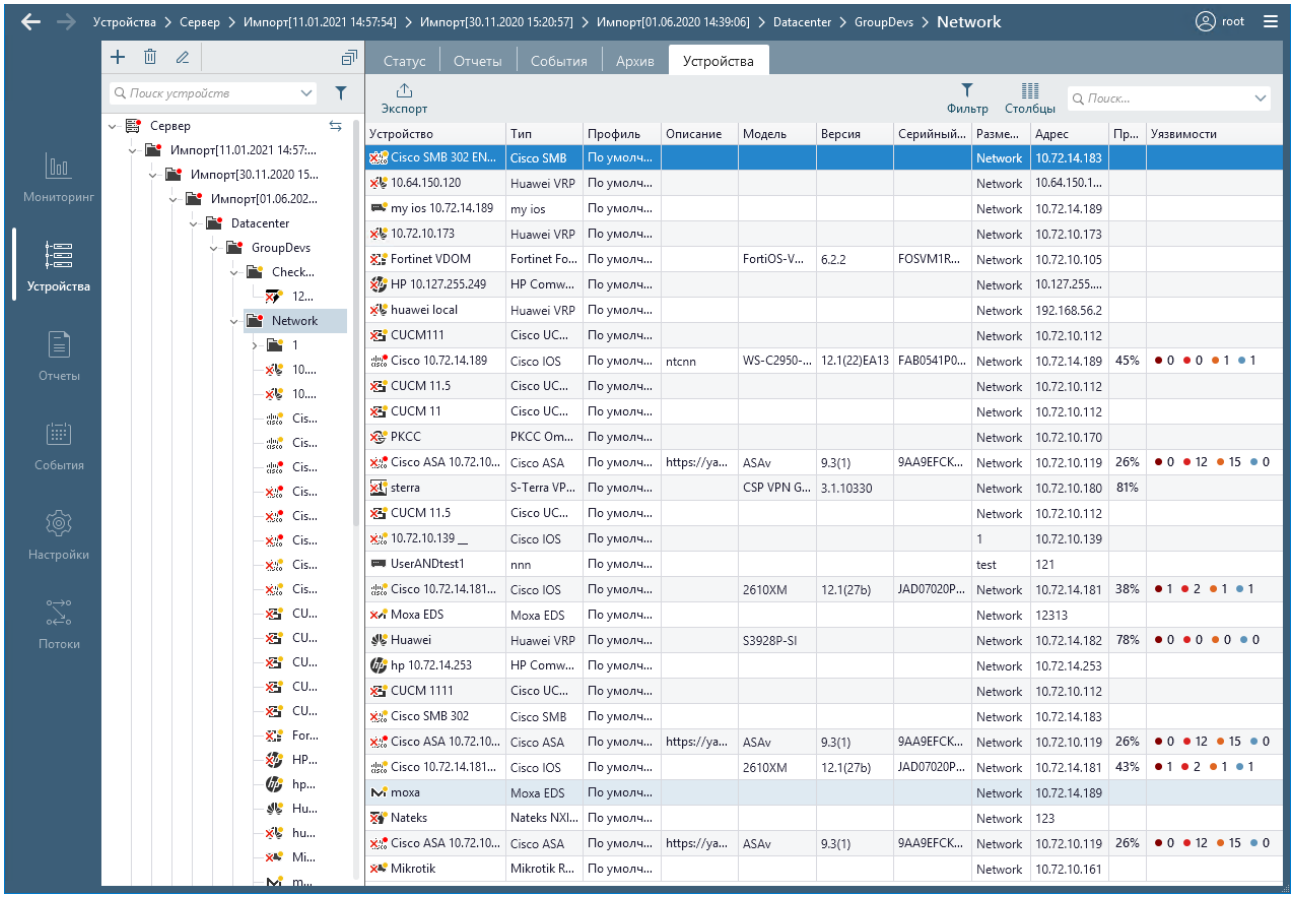


Рисунок 49 – Вкладка ***Устройства***

Для каждого устройства во вкладке отображаются общие данные об устройстве, указанные при добавлении/редактировании устройства, сведения о модели и установленной версии ОС (если они есть у устройства), а также результаты проверок безопасности устройства и количество выявленных уязвимостей, сгруппированных по уровню критичности (в том числе количество скрытых уязвимостей, при их наличии).

По двойному щелчку в любом месте строки с данными одного из объектов (устройств и каталогов/групп), в рабочей области окна произойдет переход во вкладку ***Статус*** выбранного объекта (устройства или каталога/группы).

Во вкладке ***Устройства*** существует возможность фильтрации списка устройств по их типу, состоянию, наличию уведомлений различных категорий – нажатие на кнопку ***Фильтр***, расположенную в верхней части вкладки, раскрывает окно фильтров со списками типов объектов (устройств и каталогов/групп), включенных в выделенную группу, значений параметров состояний и категорий уведомлений (рис. 50).

Для фильтрации объектов (устройств и каталогов/групп) следует отметить необходимый параметр, при этом количество выбранных параметров фильтрации будет отображаться на кнопке ***Фильтр*** (см. рис. 50). Для отмены фильтрации объектов (устройств и каталогов/групп) группы необходимо в окне фильтров нажать ссылку ***Сбросить фильтры***.

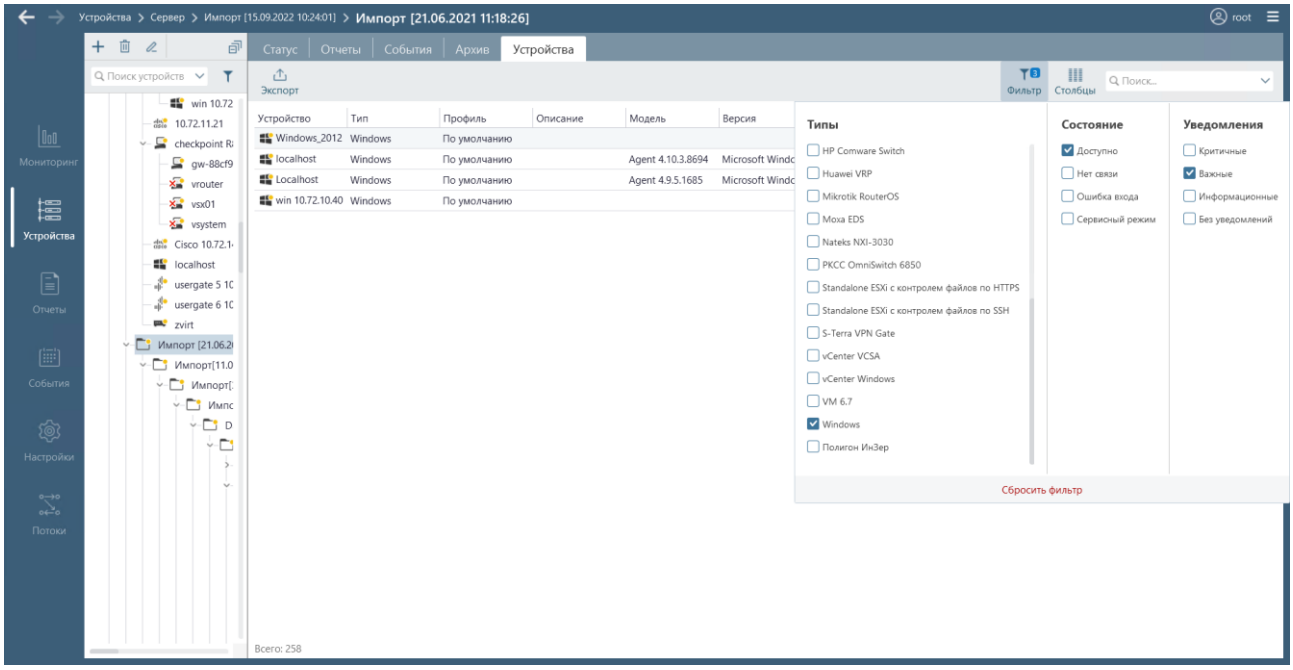


Рисунок 50 – Фильтрация списка устройств

Также во вкладке ***Устройства*** существует возможность настройки отображаемых столбцов – нажатие на кнопку ***Столбцы***, расположенную в верхней части вкладки, раскрывает список столбцов, отображаемых во вкладке. Для отображения столбца во вкладке необходимо поставить флаг напротив его имени (рис. 51).

Значение, введенное в поле ввода ***Поиск***, расположенное в верхней части вкладки, позволяет оставить в списке объектов (устройств и каталогов/групп), отображаемых во вкладке ***Устройства***, только те из них, которые удовлетворяют введенному значению.

Сортировка записей вкладки может быть выполнена по значениям всех выбранных для отображения столбцов таблицы. Столбец для сортировки и направление сортировки выполняются установкой курсора в заголовке требуемого столбца. Знак в заголовке выбранного столбца «▲» соответствует сортировке по возрастанию значений, знак «▼» – по убыванию.

Из вкладки ***Устройства*** выбранной группы существует возможность экспорта списка объектов (устройств и каталогов/групп), включенных в эту группу, в файл

отчета в формате HTML, CSV или XLSX (подробнее см. п. 2.8.3 «Получение отчета о состоянии контролируемых устройств»).

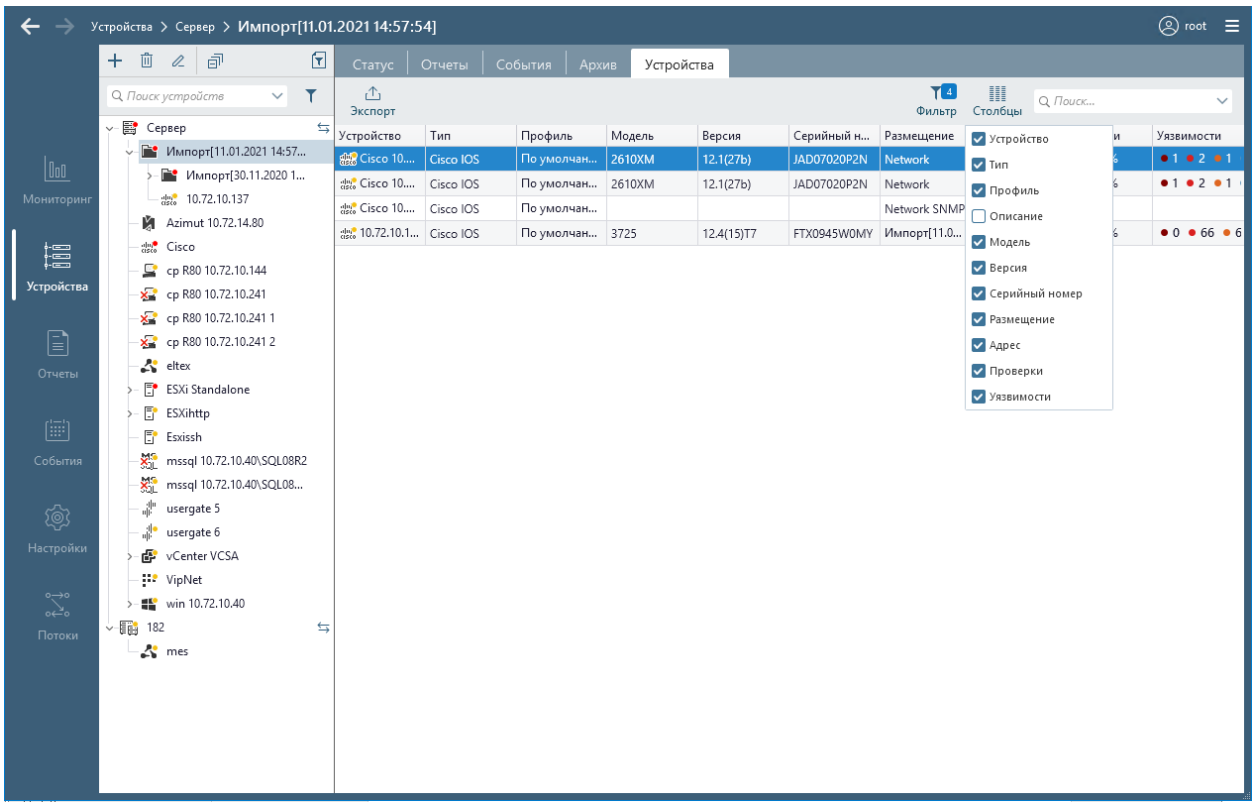


Рисунок 51 – Настройка отображения столбцов для списка устройств группы

2.5. Формирование списка контролируемых устройств

Формирование списка контролируемых устройств выполняется средствами разделов **Устройства** и **Настройки** (панель ***Настройки контроля***).

Доступ к функциям управления списком устройств в разделе **Настройки** (экспорт, импорт, сканирование сети, просмотр карты сети, установка параметров проверки доступности устройств) имеют только пользователи с правами *Управление* категории *Настройки контроля.* Подробное описание выполнения функций управления списком устройств в разделе **Настройки** приведено в документе 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».

Далее в разделе приведены правила выполнения функций управления списком устройств, доступных в разделе **Устройства**.

2.5.1. Ведение списка групп устройств

2.5.1.1. Добавление группы

Для добавления группы в список контролируемых устройств пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Устройства**, для чего в консоли нажать соответствующую кнопку на панели выбора раздела.

2) В разделе **Устройства** клиентской консоли выбрать при необходимости сервер, для которого необходимо добавить группу (см. п. 2.4.1 «Панель списка устройств»).

3) Выделить группу, в которой будет создана новая группа и в строке меню панели списка устройств нажать кнопку ***Добавить*** (+), выбрать из выпадающего списка значение *Новая группа*, или выбрать пункт контекстного меню выделенной группы *Добавить группу* (рис. 52).

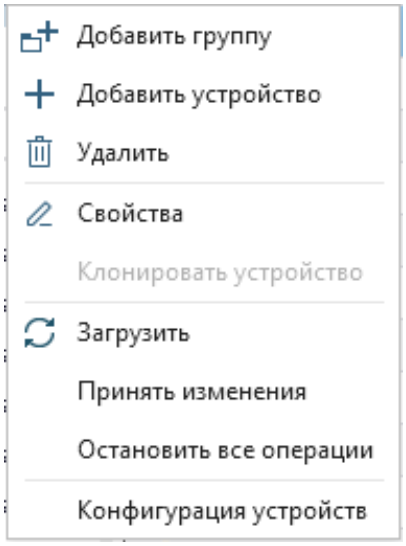


Рисунок 52 – Контекстное меню группы устройств

4) В открывшемся окне **Новая группа** (рис. 53) указать необходимые параметры создаваемой группы во вкладках:
   – *Свойства* в соответствии с п. 2.5.1.2;
   – *Доступ* в соответствии с п. 2.5.1.3;
   – *Расписания* в соответствии с п. 2.5.1.4;
   – *Обработчики событий* в соответствии с п. 2.5.1.5.

5) Нажать кнопку ***Добавить.***

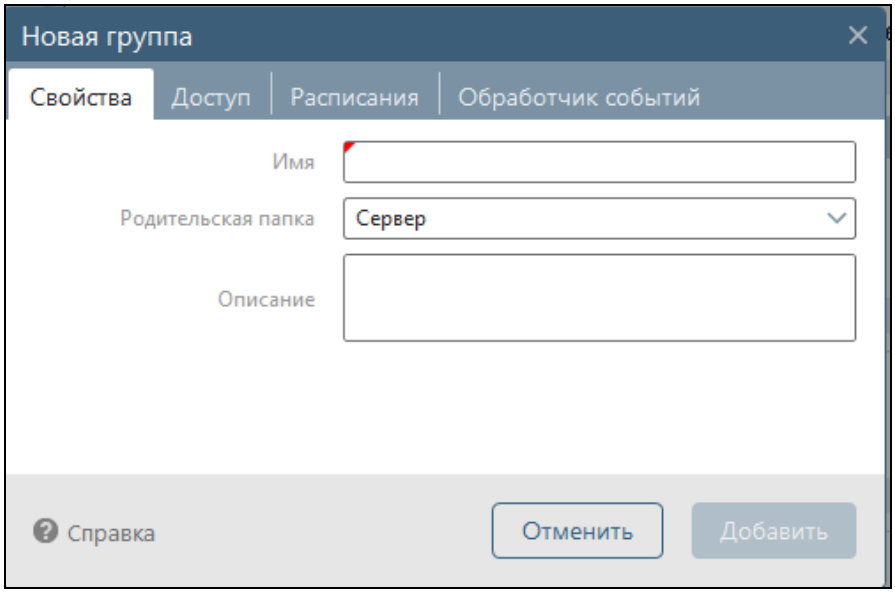


Рисунок 53 – Окно создания новой группы

2.5.1.2. Ввод основных параметров группы устройств

Во вкладке **Свойства**, которая по умолчанию открывается при открытии окна добавления новой группы на сервер ПК, расположены поля ввода, определяющие основные параметры новой группы:

- ***Имя*** – название создаваемой группы;
- ***Родительская папка*** – раскрывающийся список существующих на сервере ПК групп устройств. В указанной в этом поле группе будет создана новая группа;
- ***Описание*** – текстовое поле, в которое можно ввести понятное описание группы.

ВНИМАНИЕ: В комплексе отсутствует ограничение на уникальность имени группы устройств. Если при создании группы в поле ***Имя*** введено значение, уже используемое на сервере ПК, то рамка поля будет выделена желтым цветом, решение о создании группы с указанным именем или переименовании принимается пользователем!

2.5.1.3. Настройка доступа пользователей к группе устройств

Во вкладке ***Доступ*** окна добавления новой группы (рис. 54) отображен список всех групп пользователей (пиктограмма) и пользователей (пиктограмма) с назначенными им правами доступа к родительской группе. По умолчанию переключатели ***Наследовать*** () для всех групп/пользователей включены и права доступа пользователей к новой группе будут полностью унаследованы от родительской группы. Выделенные серым цветом фона кнопки ***Нет доступа***, ***Чтение*** и ***Полный доступ*** соответствуют назначенным пользователям правам на доступ к группе.

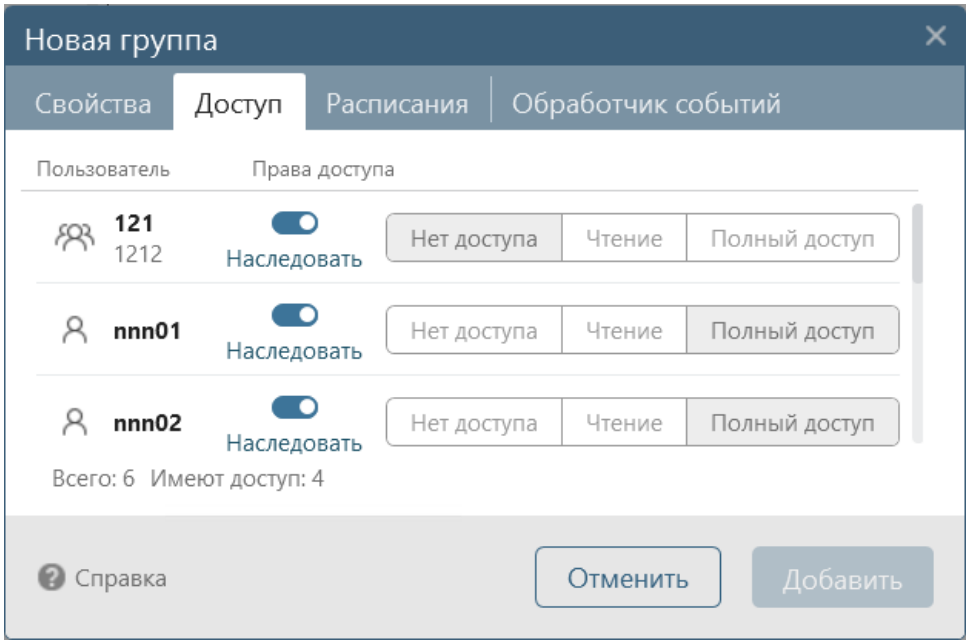


Рисунок 54 – Вкладка ***Доступ*** окна создания новой группы

Для изменения унаследованных от родительского каталога прав доступа пользователей к новой группе необходимо отключить переключатель ***Наследовать***

( ) и и выбрать требуемый уровень доступа пользователей к создаваемой группе, нажав соответствующую кнопку ***Нет доступа***, ***Чтение*** или ***Полный доступ***.

Примечание – Список пользователей не доступен для изменения в окне создания группы.

2.5.1.4. Настройка использования расписаний для группы устройств

Во вкладке ***Расписания*** окна добавления новой группы (рис. 55) отображен список расписаний, имеющихся на сервере ПК. В нижней части окна приведены общее количество и количество активных расписаний.

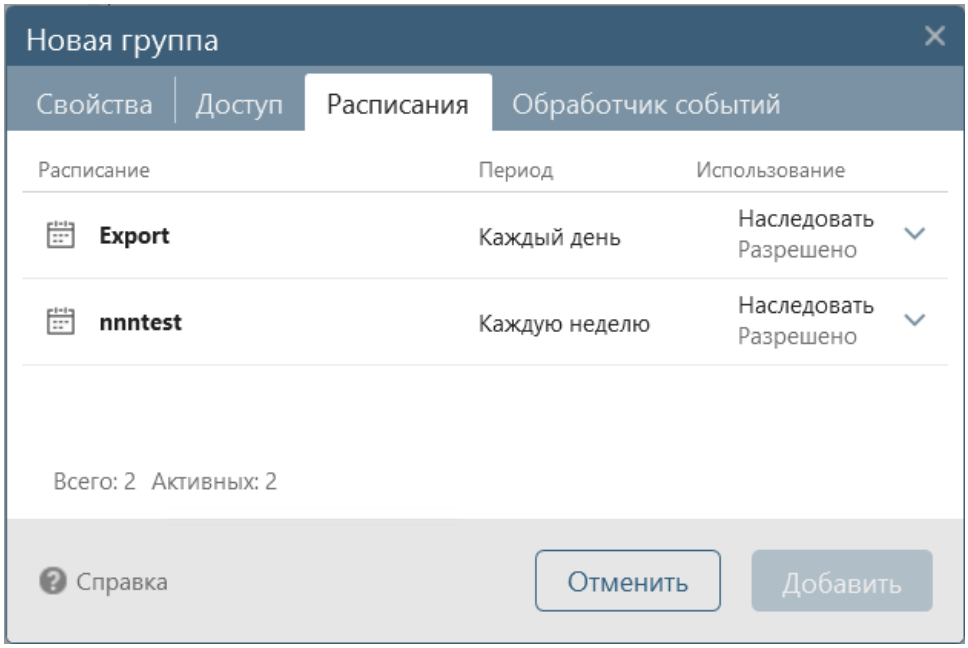


Рисунок 55 – Вкладка ***Расписания*** окна создания новой группы

Во вкладке ***Расписания*** можно настроить режим использования расписаний для создаваемой группы (правила и последовательность действий по настройке аналогичны правилам настройки использования расписаний для устройств (см. п. 2.7.3 «Настройка режима использования расписаний для устройств»)).

2.5.1.5. Настройка использования триггеров для группы устройств

Во вкладке ***Обработчик событий*** окна добавления новой группы (рис. 56) отображен список триггеров, существующих на сервере ПК. В нижней части окна приведены общее количество и количество активных обработчиков событий.

Во вкладке ***Обработчик событий*** можно настроить режим использования обработчиков событий для создаваемой группы (правила и последовательность действий по настройке аналогичны правилам настройки использования триггеров для устройств (см. п. 2.7.2 «Настройка режима использования обработчиков событий для устройств»)).

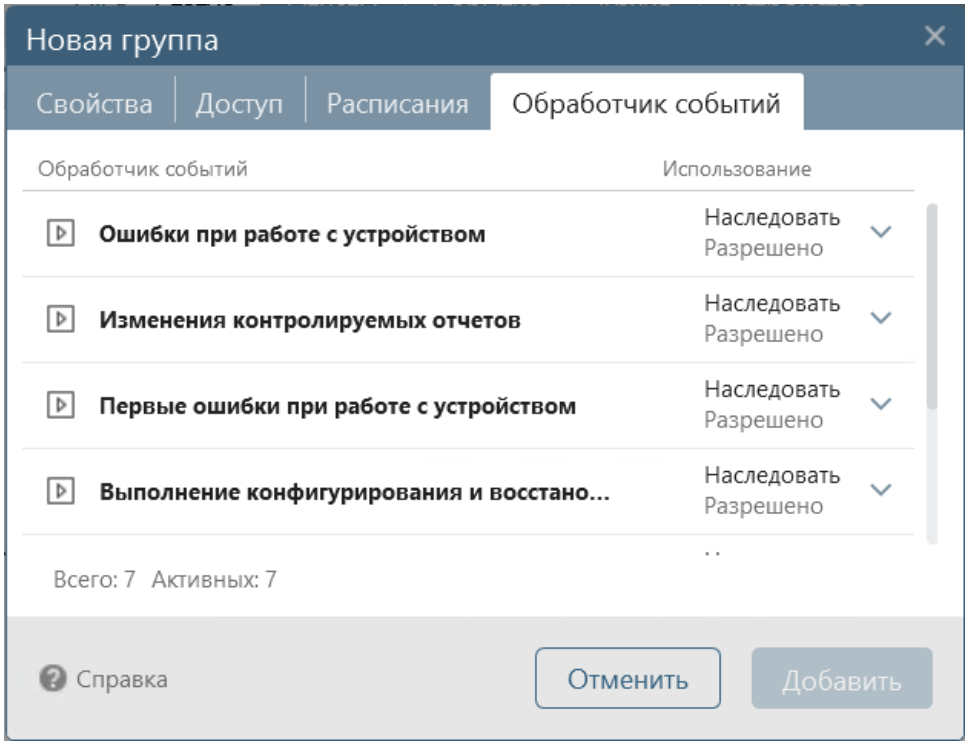


Рисунок 56 – Вкладка ***Обработчик событий*** окна создания новой группы

2.5.1.6. Изменение параметров группы

Для изменения параметров группы пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Устройства**, для чего в консоли нажать соответствующую кнопку на панели выбора раздела.

2) В панели списка устройств выделить изменяемую группу и нажать в строке меню списка устройств кнопку ***Свойства*** () или выбрать пункт ***Свойства*** в контекстном меню группы (см. рис. 52).

3) В открывшемся окне во вкладках: ***Свойства, Доступ, Расписания, Обработчики событий*** изменить необходимые параметры группы.

4) По окончании редактирования параметров группы для сохранения внесенных изменений нажать кнопку ***Сохранить***.

2.5.1.7. Удаление группы

Для удаления группы из списка устройств на сервере ПК пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Устройства**, для чего в консоли нажать соответствующую кнопку в панели выбора раздела.

2) В панели списка устройств выделить удаляемую группу и нажать в строке меню списка устройств кнопку ***Удалить*** () или выбрать пункт ***Удалить*** в контекстном меню группы (см. рис. 52).

3) В открывшемся окне подтвердить удаление группы, нажав кнопку ***Удалить***.

ВНИМАНИЕ: Вместе с группой с сервера ПК будут удалены и все устройства, которые находились в удаляемой группе. Для того чтобы устройства остались в

списке контролируемых на сервере ПК, необходимо перед удалением выбранной группы переместить их в другую группу!

2.5.2. Ведение списка устройств

2.5.2.1. Добавление устройства

Для добавления устройства в список контролируемых на текущем сервере ПК пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Устройства**, для чего в консоли нажать соответствующую кнопку на панели выбора раздела.

2) В разделе **Устройства** клиентской консоли:

– выбрать сервер, для которого необходимо добавить устройство (см. п. 2.4.1 «Панель списка устройств»);

– выделить группу, в которую будет добавлено новое устройство;

– в строке меню панели списка устройств нажать кнопку ***Добавить*** (+) и в раскрывшемся списке выбрать значение ***Новое устройство***, или выбрать пункт контекстного меню выделенной группы ***Добавить устройство*** (см. рис. 52).

3) В открывшемся окне **Новое устройство** (рис. 57) во вкладках:

– ***Свойства*** – указать необходимые параметры добавляемого устройства (см. таблицу 6);

– ***Доступ*** – установить права доступа к добавляемому устройству пользователей комплекса;

– ***Расписания*** – настроить параметры использования расписаний для добавляемого устройства;

– ***Обработчик событий*** – настроить параметры обработчиков событий для добавляемого устройства.

Примечание – Параметры доступа пользователей комплекса к новому устройству, настройки использования расписаний и обработчиков событий полностью совпадают с соответствующими параметрами группы на сервере ПК, их описание и рисунки приведены в описании вкладок окна добавления группы устройств ***Доступ***, ***Расписания***, ***Обработчик событий*** в настоящем Руководстве (п. 2.5.1 «Ведение списка групп устройств»).

ВНИМАНИЕ: Установленные в окне **Новое устройство** параметры доступа пользователей и настройки использования расписаний и триггеров распространяются только на добавляемое устройство!

4) После завершения ввода параметров нового устройства нажать кнопку ***Добавить***.

Для добавления некоторых типов устройств в список контролируемых на сервере ПК необходимо предварительно выполнить создание или подключение внешнего модуля, обеспечивающего взаимодействие устройств соответствующего типа с комплексом (необходимо обратиться к администратору комплекса). В противном случае в поле ***Тип*** вкладки ***Свойства*** будет отсутствовать необходимый тип подключаемого устройства.

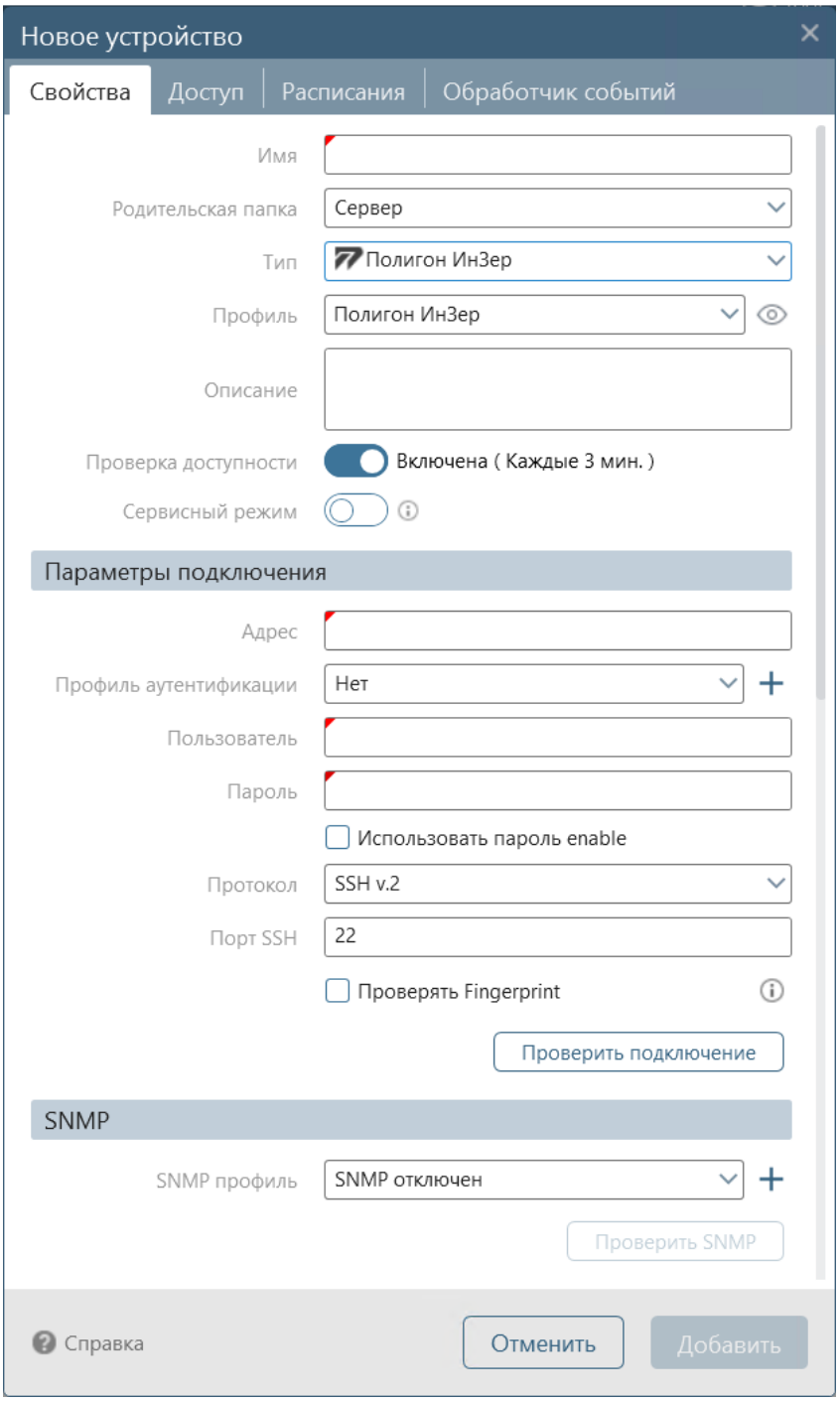


Рисунок 57 – Окно **Новое устройство**

Таблица 6 – Параметры устройства

Параметр	Описание
Имя	Понятное имя добавляемого устройства (оборудования). Данное имя отображается только в клиентской консоли и никак не связано с реальным именем устройства
Родительская папка	Раскрывающийся список существующих на сервере ПК групп устройств
Тип	Раскрывающийся список доступных для добавления на сервер ПК типов устройств (например, *SunOS, Windows, Linux, AIX* и др.).

Параметр	Описание
	Зависит от состава подключенных к серверу ПК внешних модулей
Профиль	Раскрывающийся список поля содержит наименования профилей, имеющихся на сервере ПК для выбранного типа устройства. Справа расположена кнопка ***Просмотреть*** (), по нажатию которой открывается окно просмотра списка отчетов и проверок выбранного профиля, доступных для применения к устройству с заданными для них параметрами контроля (без возможности настройки). По умолчанию выбран профиль, соответствующий имени типа устройства в списке профилей формы редактирования профилей
Описание	Текстовое поле, в которое можно ввести понятное описание устройства. Например, место размещения оборудования, инвентарный/серийный номер и т.д.
Проверка доступности	Переключатель для включения/отключения проверки доступности устройства с указанной периодичностью. Для устройств типа *Универсальное устройство SCADA* переключатель не отображается.
Сервисный режим	Переключатель для включения/отключения для устройства сервисного режима. В сервисном режиме устройство не опрашивается по заданному расписанию и не проверяется в автоматическом режиме его доступность, обновление данных выполняется только по запросу пользователя
Дополнительно для устройств ***Универсальное устройство SCADA***	
Папка установки	Поле для ввода пути к каталогу[1)] установки контролируемого ПО SCADA
Папка проекта	Поле для ввода пути к каталогу хранения контролируемых проектов ПО SCADA
Блок полей ***Параметры подключения*** (состав полей зависит от типа устройства, для устройств типа *Универсальное устройство SCADA* блок отсутствует)	
Адрес	IP-адрес или доменное имя устройства
Профиль аутентификации	Раскрывающийся список поля содержит значение *Нет* и наименования профилей аутентификации, имеющихся на сервере ПК. В списке необходимо выбрать профиль аутентификации (имя учетной записи (логин) и пароль), которые будут использоваться при

[1)] Каталог может быть введен вручную или выбран в окне, которое открывается по нажатию справа в поле кнопки *Выбрать каталог* (). Если с родительским устройством отсутствует связь, то в окне выбора каталога будет отображаться сообщение ***Данные не получены*** и кнопка *Показать лог* для перехода в окно просмотра подробных сведений. Расширения контролируемых файлов выбранного каталога задаются при настройке отчетов ***Файлы SCADA*** и ***Файлы проекта*** устройства.

Параметр	Описание
	аутентификации на контролируемом устройстве. Для устройств типа *Универсальное устройство SCADA* поле не заполняется. Если требуемого профиля нет, то пользователь может добавить его, выбрав значение *Нет,* нажав справа в поле кнопку ***Добавить*** (+), заполнив поля открывшегося окна добавления на сервер ПК профиля аутентификации (рис. 58) и нажав кнопку ***Сохранить***. Пользователь также имеет возможность внести изменения в выбранный в поле профиль, для чего необходимо после выбора профиля нажать справа в поле кнопку ***Редактировать*** (✎), внести изменения в открывшемся окне параметров профиля аутентификации и нажать кнопку ***Сохранить***. Примечание – Создать новый профиль аутентификации и внести изменения в имеющийся из формы создания устройства могут только пользователи, имеющие права доступа к настройкам контроля устройств
Пользователь	Логин пользователя для аутентификации на устройстве
Пароль	Пароль пользователя для аутентификации на устройстве
Использовать пароль enable	При наличии в поле флага, включается возможность входа пользователя на устройство в привилегированном режиме. По умолчанию флаг в поле не установлен, возможность доступа в привилегированном режиме отсутствует
Пароль enable (super, expert, администратора)	Пароль пользователя для осуществления входа на устройство в привилегированном режиме. Поле отображается во вкладке только при наличии флага в поле *Использовать пароль enable*
Протокол	Используемый для соединения с устройством сетевой протокол (*Telnet*, *SSH*)
Порт Telnet/SSH	Для *Windows*-устройств – номер порта подключения Windows-агента; для устройств типа *3COM*, *Huawei*, *Dionis NX* – номер порта для соединения с устройством по протоколу SSH
Проверять Fingerprint ключа устройства	При наличии в поле флага, устанавливается необходимость проверки подлинности открытого ключа при SSH-соединении с устройством. Поле отображается во вкладке только при выборе в поле *Протокол* значения *Telnet.* По умолчанию флаг не установлен
Кнопка Проверить подключение	По нажатию кнопки выполняется проверка подключения устройства. После завершения проверки слева от кнопки отображается результат проверки: *Успешно* или *Ошибка*. Текст результата является ссылкой, при выборе которой открывается окно с логом выполнения команды
Блок полей ***SNMP***	
SNMP профиль	Раскрывающийся список поля по умолчанию содержит значения *SNMP отключен* и *public* (предустановленный профиль для

Параметр	Описание
	подключения по SNMPv2). После добавления SNMP профилей содержит также их названия. При выборе значения *SNMP отключен* справа в поле отображается кнопка ***Добавить*** (+) для перехода в окно добавления профиля SNMP (см. рис. 59). Добавление профиля возможно как *snmpv2* с указанием *community* для подключения, так и *snmpv3* с указанием алгоритмов защиты и учетными данными. Пользователь также имеет возможность внести изменения в выбранный в поле профиль (*SNMP* или *public*), для чего необходимо после выбора профиля нажать справа в поле кнопку ***Редактировать*** (✎), внести изменения в открывшемся окне параметров профиля и нажать кнопку ***Сохранить***. Примечание – Создать новый SNMP профиль и внести изменения в имеющийся из формы создания устройства могут только пользователи, имеющие права доступа к настройкам контроля устройств
Кнопка Проверить SNMP	По нажатию кнопки выполняется проверка подключения к устройству по выбранному профилю SNMP. После завершения проверки слева от кнопки отображается результат проверки: *Успешно* или *Ошибка*
Для устройств ***AD Domain*** блок ***Параметры подключения*** содержит поля	
Контроллер домена	Полное имя домена
Использовать имя и пароль	Переключатель открытия/закрытия полей ввода имени и пароля пользователя, от имени которого будет происходить авторизация на указанном контроллере домена
Для устройств ***CheckPoint SmartCenter*** блок ***Параметры подключения*** дополнительно содержит поля	
Application CN	*Domain Name* используемого OPSEC приложения
Management CN	*Domain Name Check Point SmartCenter*
Сертификат OPSEC Application	Сертификат используемого OPSEC приложения, для создания защищенного соединения между сервером ПК и устройством
Для устройств ***CheckPoint R80 Management Server*** окно дополнительно содержит	
Блок Параметры подключения по REST API	Поля для ввода/изменения параметров подключения к устройству по REST API: порт, логин и пароль пользователя
Для устройств ***CISCO UCM*** блок ***Параметры подключения*** содержит только поле *Адрес* и окно дополнительно содержит	
Блок Пользователь AXL API	Логин и пароль пользователя для аутентификации на устройстве с помощью сервиса AXL API
Блок Параметры подключения по SSH	Поля для ввода параметров для подключения по протоколу SSH. Состав полей аналогичен составу полей блока ***Параметры подключения*** (см. выше общее описание блока), без поля *Адрес*

Параметр	Описание
Для устройств ***Dionis-NX 2.0*** блок ***Параметры подключения*** содержит вместо поля *Использовать пароль enable* поле *Для входа в режим enable использовать другую учетную запись*	
Для входа в режим enable использовать другую учетную запись	Поле для флага, при установке флага в котором дополнительно отображается поле *Учетная запись для входа в режим enable.* Используется для обеспечения возможности доступа к устройству администраторов с разными ролями
Учетная запись для входа в режим enable	Поля для ввода логина пользователя, иеющего привилегию аутентификации на устройстве в режиме enable

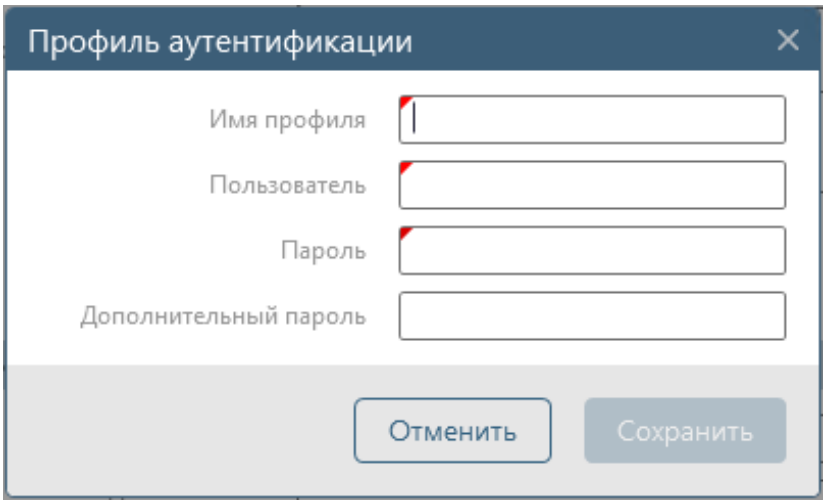


Рисунок 58 – Окно добавления профиля аутентификации

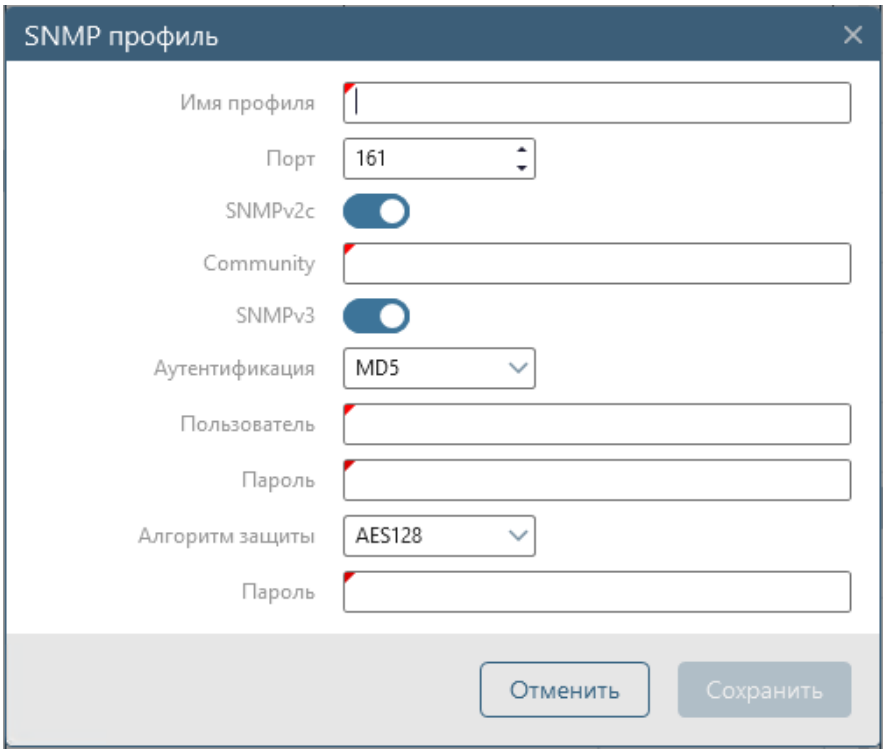


Рисунок 59 – Окно добавления SNPM профиля

Для устройств, поддерживающих два типа подключения (например, API и SSH) блок ***Параметры подключения*** содержит поле *Адрес* и две группы полей с параметрами подключения (***API*** и ***SSH*** соответственно) (рис. 60). В каждой группе полей есть возможность выбрать профиль аутентификации соответствующего типа из числа имеющихся на сервере ПК или создать новый профиль аутентификации. Состав полей групп зависит от типа устройств.

ВНИМАНИЕ: Изменение выбора профилей аутентификации в дальнейшем для таких устройств возможно только в карточке устройства, при настройке профилей подключения в разделе **Настройки** изменение использования профилей для таких устройств не доступно!

Для устройств, поддерживающих выполнение операций, блок ***Параметры подключения*** содержит поле ***Задать дополнительные настройки***, при установке в котором флага отображаются дополнительные поля (рис. 61) для задания тайм-аутов в секундах для подключения, выполнения команды и ожидания ответа (состав полей зависит от поддерживаемых устройством операций).

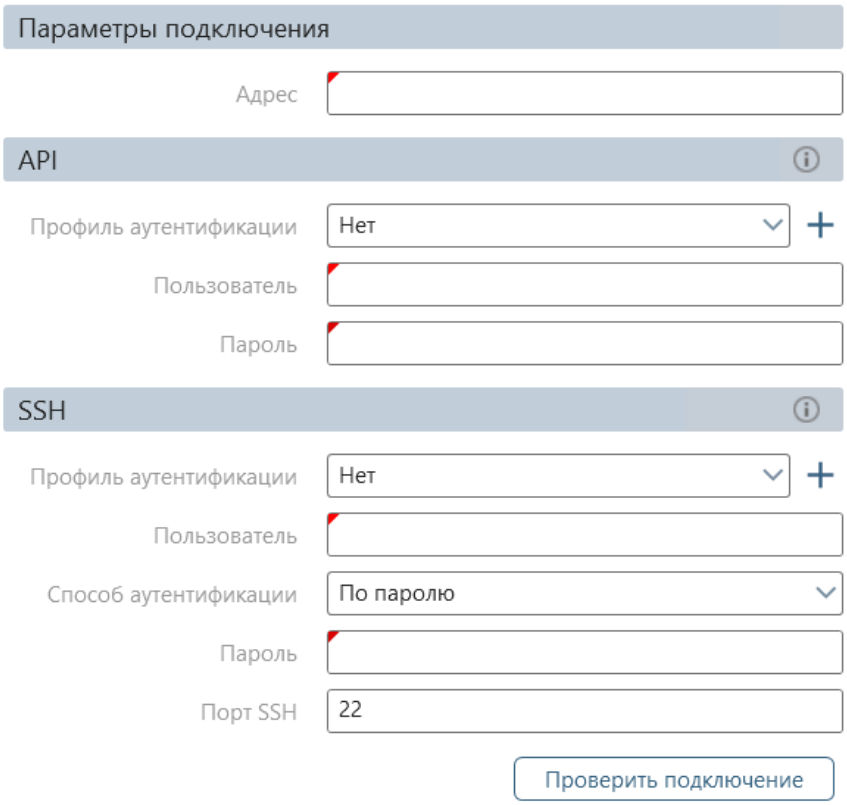


Рисунок 60 – Блок ***Параметры подключения*** для устройств, поддерживающих два типа подключения

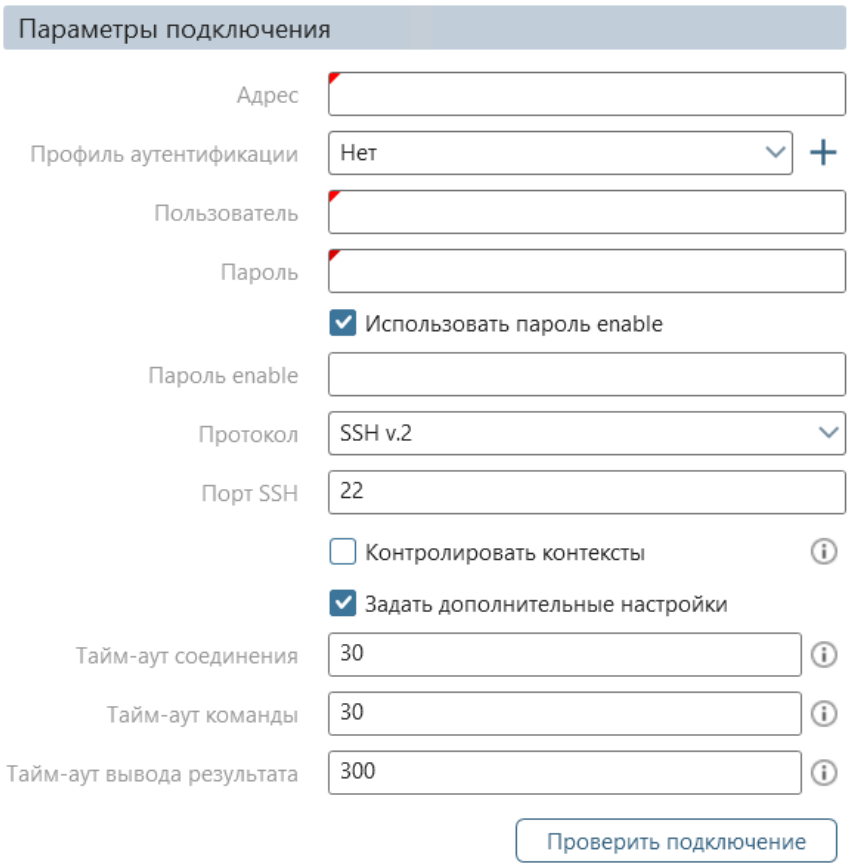


Рисунок 61 – Блок ***Параметры подключения*** с полями настройки тайм-аутов выполнения операций

2.5.2.2. Изменение параметров устройства

Для изменения параметров устройства пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Устройства**, для чего в консоли нажать соответствующую кнопку на панели выбора раздела.

2) В панели списка устройств выделить изменяемое устройство и нажать в строке меню списка устройств кнопку ***Свойства*** () или выбрать пункт ***Свойства*** в контекстном меню устройства.

3) В открывшемся окне изменить свойства устройства (см. рис. 57) и, при необходимости, параметры доступа к устройству пользователей комплекса. Описание полей окна свойств устройства приведено в таблице 6.

4) По окончании редактирования параметров устройства – нажать кнопку ***Сохранить***.

2.5.2.3. Удаление устройства

Для удаления устройства из списка контролируемых на текущем сервере ПК пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Устройства**, для чего в консоли нажать соответствующую кнопку на панели выбора раздела.

2) В панели списка устройств выделить удаляемое устройство и нажать в строке меню списка устройств кнопку ***Удалить*** () или выбрать пункт ***Удалить*** в контекстном меню устройства.

3) В открывшемся окне подтвердить операцию удаления устройства, нажав кнопку ***Удалить***.

2.5.2.4. Доступность устройств

В ПК «Efros Config Inspector» v.4 существует возможность просмотра доступности устройств в сети. Доступность устройств проверяется с помощью ICMP Ping и учитывает последние данные о работе комплекса с устройством (подключение и задачи по выбранным протоколам).

Настройку проверки доступности устройств в сети (включена/отключена, периодичность проверки, список проверяемых устройств) могут выполнить только пользователи с правами *Управление* в категории *Настройки контроля* (подробнее см. документ 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»).

Результаты проверок доступности отображаются в разделе **Устройства,** в панели списка устройств. На пиктограмме устройства, в случае его недоступности по результатам проверки, отображается символ  . В случае, если проверка доступности устройства прошла успешно после ошибки при выполнении последней операции, пиктограмма устройства отображается без символа недоступности устройства.

2.6. Настройка отчетов устройств

Для анализа работы оборудования и обеспечения контроля его конфигурации на сервер ПК загружаются отчеты, содержащие значения параметров контролируемого оборудования. Для загрузки параметров конфигурации контролируемого оборудования на сервер ПК служит механизм ***Отчеты***. Каждый ***Отчет*** содержит в себе команду, которая выполняется на устройстве, или список файлов контролируемого устройства, целостность которых контролируется на сервере ПК.

Существует три типа отчетов, загружаемых с устройств:

- ***Общий (встроенный)*** – добавляются на сервер ПК одновременно с подключением к нему внешнего модуля и содержат в себе команды для контроля и анализа конфигураций, поддерживаемых этим модулем устройств;
- ***Пользовательский*** – формируются пользователями комплекса на основе шаблонов, которые также добавляются на сервер ПК при подключении к нему внешнего модуля;
- ***Фильтр*** – формируются пользователями комплекса на основе загруженного с устройства отчета путем фильтрации отображаемых в отчете параметров конфигурации устройства.

Для МЭ кроме встроенных отчетов при настройке проверок МЭ могут быть созданы стандарты безопасности, содержащие требования для контроля наличия/отсутствия правил МЭ по заданным параметрам, и назначены устройства, в списке отчетов которых в разделе **Устройства** будет доступен отчет по созданному стандарту безопасности.

ВНИМАНИЕ: Добавлять, изменять и клонировать отчеты на сервере ПК, а также изменять их настройки в существующих на сервере ПК профилях могут только пользователи с правами *Управление* в категории *Настройки контроля*!

Настройка отчетов на сервере ПК заключается в:

1) Настройке отчетов в имеющихся профилях комплекса (доступно пользователям с правами *Управление* в категории *Настройки контроля*):
   - разрешение/запрет загрузки отчетов с контролируемых устройств, которые используют настройки редактируемого профиля;
   - необходимость отслеживания изменений в загружаемых с устройств отчетах (расчет контроля целостности загруженных на сервер ПК отчетов);
   - изменение параметров дополнительных настроек отчетов (доступно для некоторых типов отчетов, например, для отчета ***Linux Файлы*** могут быть изменены настройки масок файлов для загрузки контрольных сумм и исключаемых файлов из списка контролируемых, для отчетов типа ***Файлы SCADA*** и ***Файлы проекта*** – расширения контролируемых файлов, для отчетов типа ***События журнала безопасности Windows*** могут быть заданы идентификаторы событий для их отбора в отчет и период загрузки событий).
2) Настройке отчетов для устройств, подключенных к комплексу (доступно всем пользователям):
   - разрешение/запрет использования (загрузки) отчетов;
   - необходимость отслеживания изменений в загружаемых с устройств отчетах (расчет контроля целостности загруженных на сервер ПК отчетов);
   - настройка сравнения версий отчетов, загруженных с устройств на сервер ПК.

2.6.1. Настройка одного отчета для одного устройства

Для настройки отчета для одного устройства пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Устройства**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.

2) В панели списка устройств выделить требуемое устройство и перейти на вкладку ***Отчеты***.

3) Во вкладке ***Отчеты*** (рис. 62) выделить требуемый отчет, в контекстном меню отчета выбрать пункт ***Настройки отчета*** или нажать в его строке кнопку ***Настройка*** ().

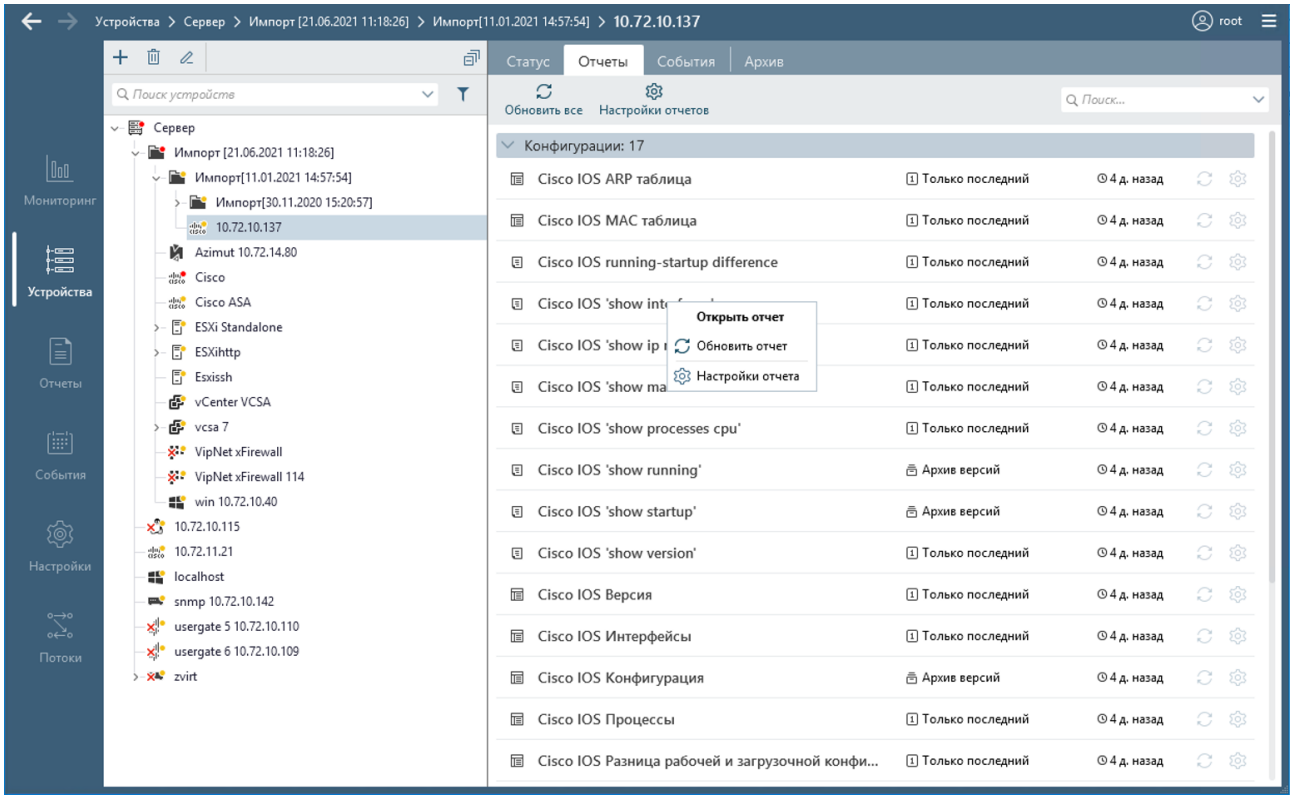


Рисунок 62 – Вкладка ***Отчеты*** выбранного устройства

4) В открывшемся окне настройки отчета из раскрывающегося списка поля *Использование* выбрать необходимое значение (рис. 63, состав и описание значений полей окна приведено в таблице 7).

5) Изменить, при необходимости, дополнительные параметры (при их наличии в отчете), предварительно выключив переключатель ***Наследовать настройки*** (см. рис. 63).

6) Нажать кнопку ***Применить***. Окно настройки отчета закроется, внесенные изменения будут сохранены.

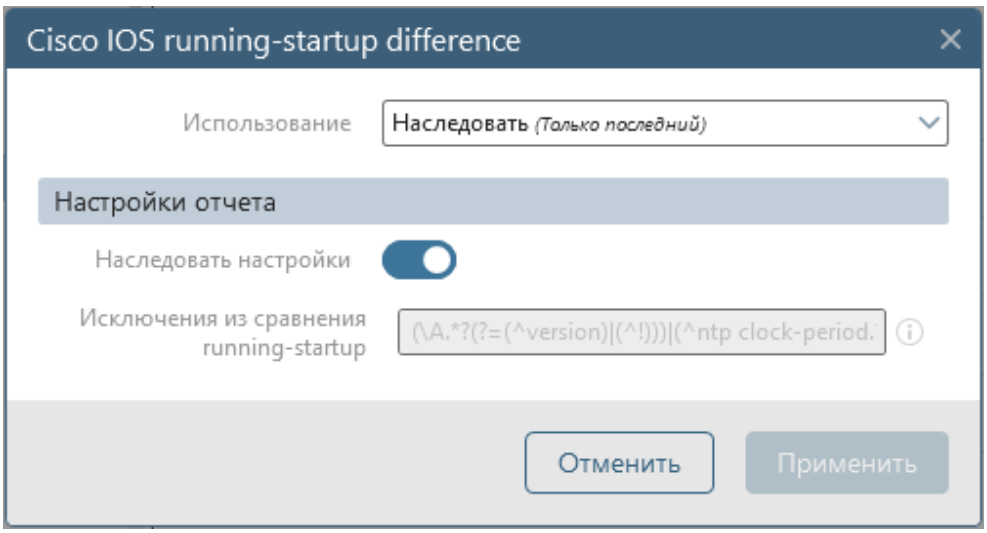


Рисунок 63 – Окно настройки отчета

Таблица 7 – Состав и описание полей окна настройки отчета для устройства

Настройка	Описание/Назначение
Использование	Выбор режима использования отчета. Возможные значения для отчетов типа ***Конфигурации***: – *Контроль изменений* – вне зависимости от настроек базового профиля будет выполняться контроль целостности загруженного с устройства отчета; – *Архив версий* – в базе данных сервера ПК будут храниться все измененные версии отчета, загруженного с устройства; – *Только последний* – в базе данных сервера ПК хранится только последняя измененная версия отчета, загруженного с устройства; – *Запрещено* – загрузка отчета с устройств запрещена вне зависимости от настроек базового профиля; – *Наследовать (XXXX)* – применить настройки базового профиля. В скобках отображается значение, установленное для отчета в базовом профиле. Возможные значения для отчетов типа ***Проверки***: – *Разрешено* – разрешить проверку вне зависимости от настроек базового профиля; – *Запрещено* – запретить проверку вне зависимости от настроек базового профиля; – *Наследовать (XXXX)* – применить настройки базового профиля. В скобках отображается значение, установленное для проверки в базовом профиле
Наследовать настройки	Переключатель режима применения настроек используемого устройством базового профиля для дополнительных настроек отчета
Группы полей дополнительных настроек	Для настройки дополнительных параметров (например, масок контролируемых файлов, параметров выполнения команд и т.д.). Поля доступны для редактирования после перевода переключателя в поле ***Наследовать настройки*** в положение *Выключен* ()

2.6.2. Настройка всех отчетов для одного устройства

Для настройки всех отчетов одного устройства пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Устройства**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.

2) В панели списка устройств выделить требуемое устройство и перейти на вкладку ***Отчеты***.

3) В заголовке вкладки ***Отчеты*** (см. рис. 62) нажать кнопку ***Настройки отчетов*** ().

4) Откроется окно настройки отчетов выбранного устройства (рис. 64), в котором в поле *Профиль устройства* отображается наименование профиля устройства, далее список всех отчетов профиля во всех состояниях. В нижней части окна отображается строка с общим количеством отчетов в профиле и количеством активных отчетов (не в статусе *Запрещено*) для выбранного устройства.

5) Из раскрывающегося списка поля *Использование* выбрать необходимое значение для каждого отчета (состав и описание значений полей окна приведено в таблице 7).

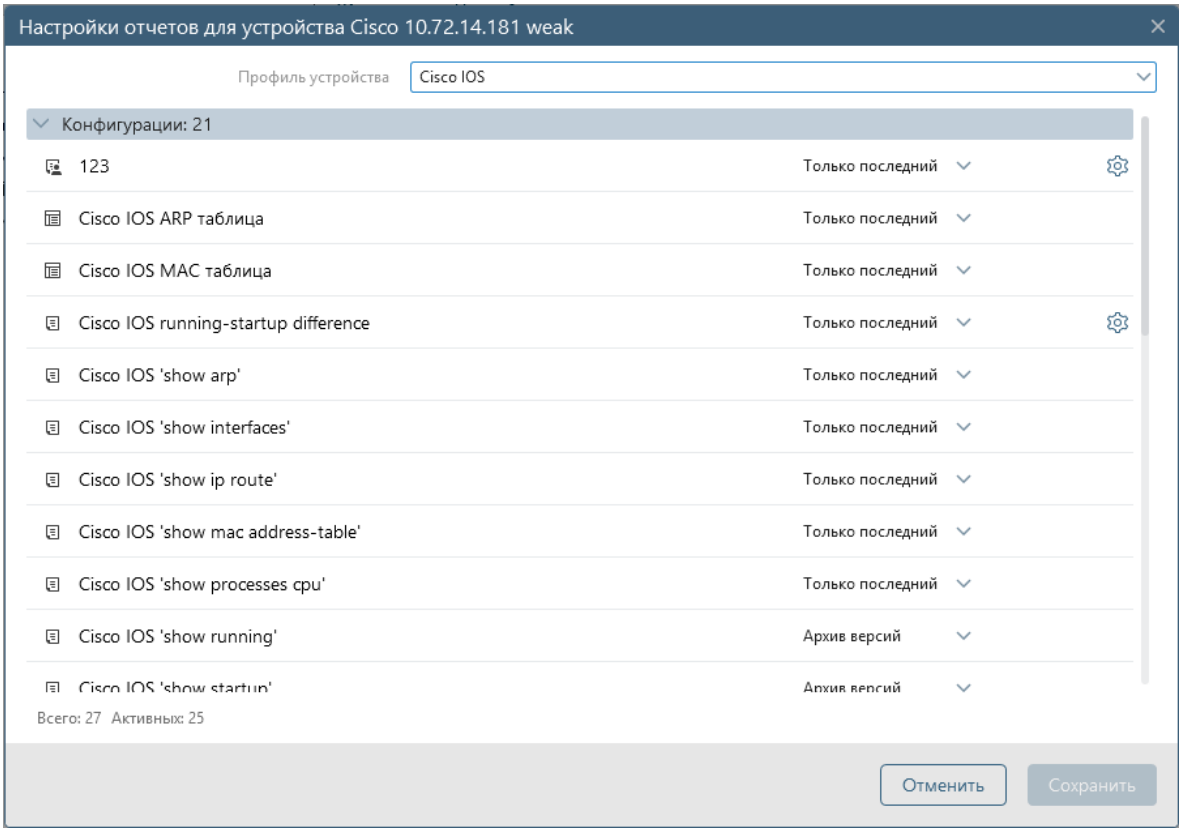


Рисунок 64 – Окно настройки всех отчетов устройства

6) Для изменения дополнительных параметров отчетов (при их наличии для отчета):

- нажать кнопку ***Параметры*** ⚙ в строке отчета;
- в открывшемся окне настройки дополнительных параметров отчета (см. пример на рис. 63, состав и описание значений полей окна приведено в таблице 7) выключить переключатель в поле ***Наследовать настройки***, внести требуемые изменения;
- нажать кнопку ***Применить***.

7) В окне настройки отчетов нажать кнопку ***Сохранить***. Окно настройки отчетов устройства закроется, внесенные изменения будут сохранены.

2.6.3. Настройка правил сравнения версий отчетов

В ПК «Efros Config Inspector» v.4 существует возможность определения правил игнорирования изменений в версиях загруженных с устройств текстовых отчетов. Для текстовых отчетов, с установленными правилами игнорирования изменений, в зависимости от режима использования, не будут возникать ошибки контроля целостности, они не будут сохраняться в архив версий, если изменения, которые произошли на контролируемом оборудовании, были указаны в правилах.

Для настройки правил сравнения версий текстовых отчетов пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Устройства**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.

2) В панели списка устройств выбрать устройство и перейти на вкладку ***Отчеты***.

3) В открывшейся вкладке ***Отчеты***, в контекстном меню настраиваемого отчета выбрать пункт ***Открыть отчет***.

4) В открывшемся окне просмотра отчета нажать кнопку ***Исключения*** ().

5) В открывшейся области настройки правил игнорирования изменений (рис. 65) нажать ссылку ***Добавить правило*** и в открывшееся поле ввести имя параметра, изменение которого на устройстве контролировать нет необходимости.

Примечание – Для корректной работы правила игнорирования изменений в отчете необходимо в поле ввода ввести символ звездочки (*) перед и/или после имени указанного параметра. При необходимости, добавить еще правила, повторив действия, описанные в перечислении 5.

6) В области настройки правил игнорирования изменений нажать кнопку ***Сохранить***. Внесенные изменения будут сохранены, и при следующей загрузке отчета изменения параметров, указанных в правилах, будут игнорироваться.

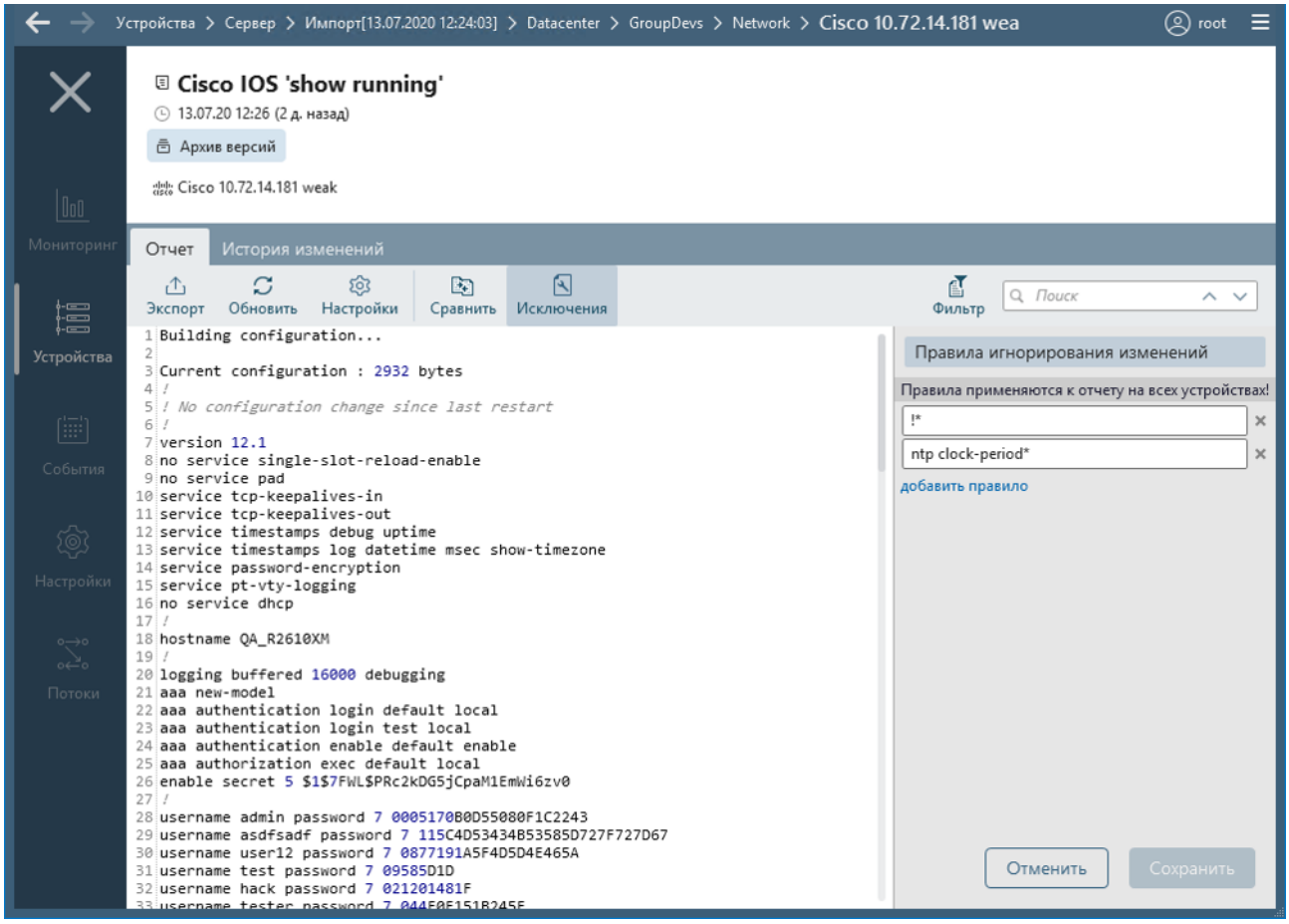


Рисунок 65 – Окно просмотра отчета с открытой областью настройки правил игнорирования изменений в отчетах

2.7. Настройка параметров контроля устройств

Настройка параметров контроля устройств заключается в:

1) Настройке отчетов, загружаемых с устройств:

– разрешение/запрет загрузки отчетов;

– необходимость отслеживания изменений в загружаемых с устройств отчетах (расчет контроля целостности отчетов);

– изменение параметров дополнительных настроек отчетов (доступно для некоторых типов отчетов, например, для отчета *Linux Файлы* могут быть изменены настройки масок файлов для постановки на контроль и масок файлов, исключаемых из списка контролируемых).

2) Настройке параметров выполнения проверок на устройствах:

– включение/отключение проверки;

– включение/отключение правила из проверки;

– задание исключений для правил проверки (например, исключение пользователя из правила *Защита пароля пользователя*).

3) Настройке использования обработчиков событий для устройства.

4) Настройке использования расписаний для устройства.

2.7.1. Настройка параметров загрузки отчетов

Изменять параметры загрузки отчетов с устройств могут пользователи комплекса с правами *Управление* в категории *Настройки контроля* и пользователи с правами доступа *Полный доступ* к изменяемым устройствам.

Для просмотра и внесения изменений в параметры загрузки отчетов с выбранного устройства пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Устройства**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.

2) В открывшемся разделе **Устройства,** в панели списка устройств выделить устройство и выбрать вкладку ***Отчеты.***

3) В заголовке открывшейся вкладки ***Отчеты*** нажать кнопку ***Настройки отчетов*** (⚙)**.** Откроется окно настройки отчетов для выбранного устройства (рис. 66), в котором в поле ***Использование,*** в выпадающем меню выбрать необходимый режим использования соответствующего отчета (состав и описание полей окна настройки отчетов для устройства приведены в таблице 8).

4) Для изменения дополнительных параметров выбранного отчета нажать в окне настройки отчетов в строке отчета кнопку ***Настройки*** (⚙).

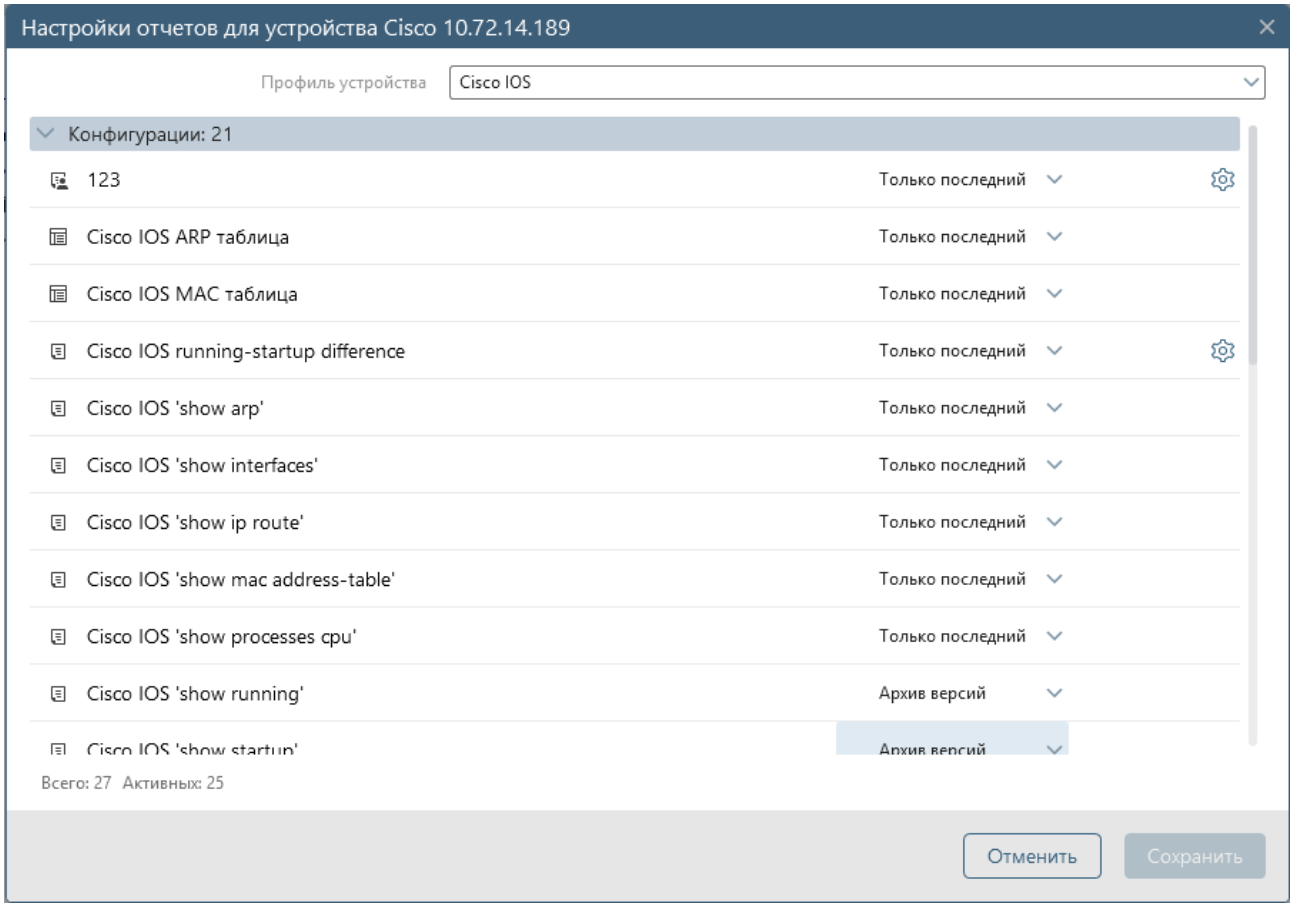


Рисунок 66 – Окно настройки всех доступных для устройства отчетов

Таблица 8 – Состав и описание полей окна настройки отчетов для устройства

Поле	Описание/Назначение
Профиль устройства	Наименование профиля устройства
Конфигурации/Проверки	Наименование отчета
Использование	Выбор режима использования отчета. Возможные значения для отчетов типа ***Конфигурации***: – *Контроль изменений* – вне зависимости от настроек базового профиля будет выполняться контроль целостности загруженного с устройства отчета; – *Архив версий* – в базе данных сервера ПК будут храниться все измененные версии отчета, загруженного с устройства; – *Только последний* – в базе данных сервера ПК хранится только последняя измененная версия отчета, загруженного с устройства; – *Запрещено* – загрузка отчета с устройств запрещена вне зависимости от настроек базового профиля; – *Наследовать (XXXX)* – применить настройки базового профиля. В скобках отображается значение, установленное для отчета в базовом профиле. Возможные значения для отчетов типа ***Проверки***: – *Разрешено* – разрешить проверку вне зависимости от настроек базового профиля; – *Запрещено* – запретить проверку вне зависимости от настроек

Поле	Описание/Назначение
	базового профиля; – *Наследовать (XXXX)* – применить настройки базового профиля. В скобках отображается значение, установленное для проверки в базовом профиле
Без названия	Содержит кнопку дополнительных параметров ⚙. Щелчок по кнопке открывает окно настройки дополнительных параметров выбранного отчета

5) В открывшемся окне настройки дополнительных параметров отчета (рис. 67 состав и описание значений полей окна приведено в таблице 9) выключить переключатель в поле ***Наследовать настройки***, внести требуемые изменения и нажать кнопку ***Применить***.

Примечание – При наведении курсора на пиктограмму, расположенную рядом с изменяемым параметром, появляется всплывающая подсказка со справочной информацией по этому параметру.

6) Нажать кнопку ***Сохранить***. Окно настройки отчетов для устройства закроется, внесенные изменения будут сохранены.

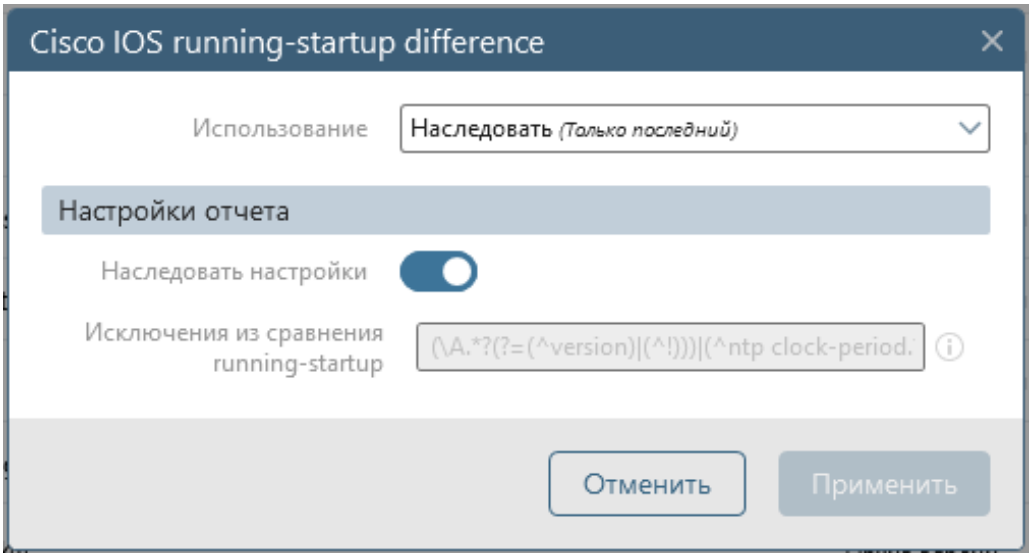


Рисунок 67 – Окно настроек отчета для устройства

Таблица 9 – Состав и описание полей окна настроек отчета для устройства

Поле	Описание/Назначение
Использование	Выбор настройки использования отчета. Возможные значения перечислены в таблице 8
Наследовать настройки	Переключатель режима применения настроек используемого устройством базового профиля для дополнительных настроек отчета
Группы полей дополнительных настроек	Для настройки дополнительных параметров (например, масок контролируемых файлов, параметров выполнения команд и т.д.). Поля доступны для редактирования после перевода переключателя в поле ***Наследовать настройки*** в положение *Выключен* (⬭)

2.7.2. Настройка режима использования обработчиков событий для устройств

Список обработчиков событий ведется в разделе **Настройки** пользователями с правами *Управление* в категории *Настройки контроля.*

Изменять режим использования обработчиков событий для устройств могут пользователи комплекса с правами *Управление* в категории *Настройки контроля* и пользователи с правами доступа *Полный доступ* к изменяемым устройствам.

Для просмотра и внесения изменений в режим использования триггеров для выбранного устройства пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Устройства**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.

2) В панели списка устройств выбрать устройство, для которого необходимо настроить режим использования обработчиков событий.

3) В панели кнопок списка устройств нажать кнопку ***Свойства*** (✎) или выбрать пункт ***Свойства*** в контекстном меню устройства.

4) В открывшемся окне свойств выбранного устройства (рис. 68) перейти на вкладку ***Обработчик событий*** (рис. 69).

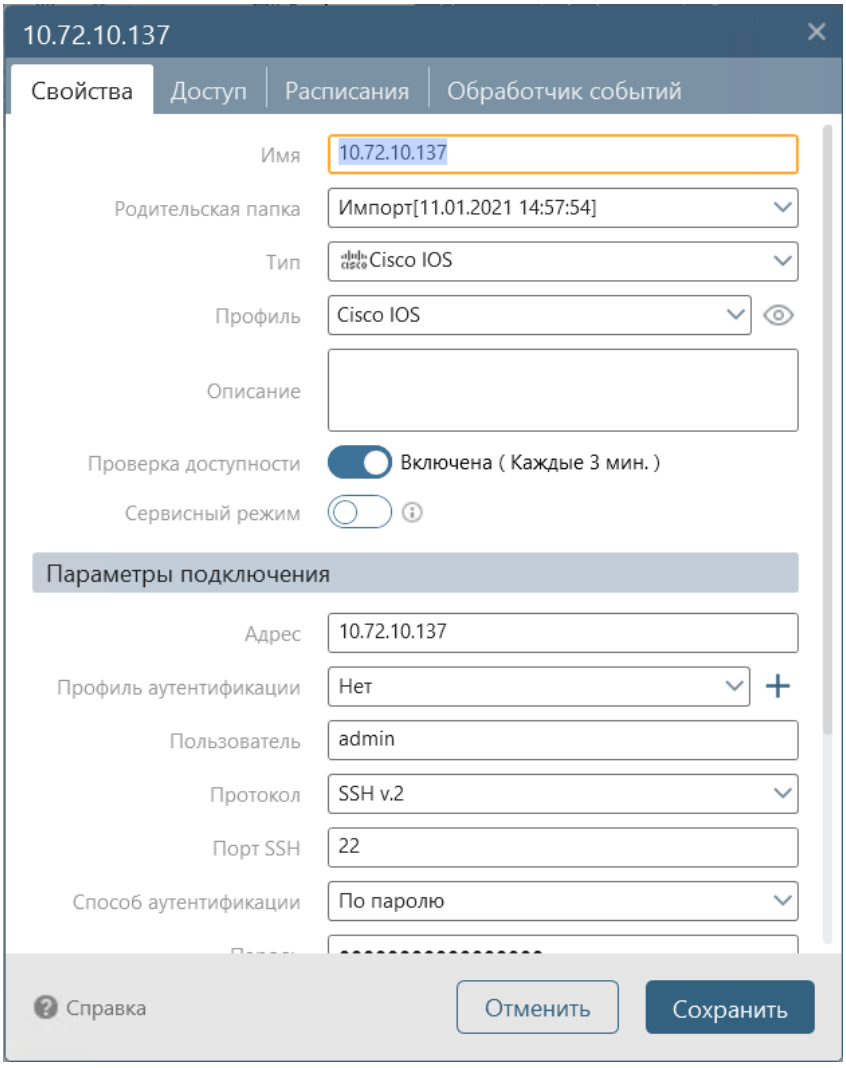


Рисунок 68 – Окно свойств устройства

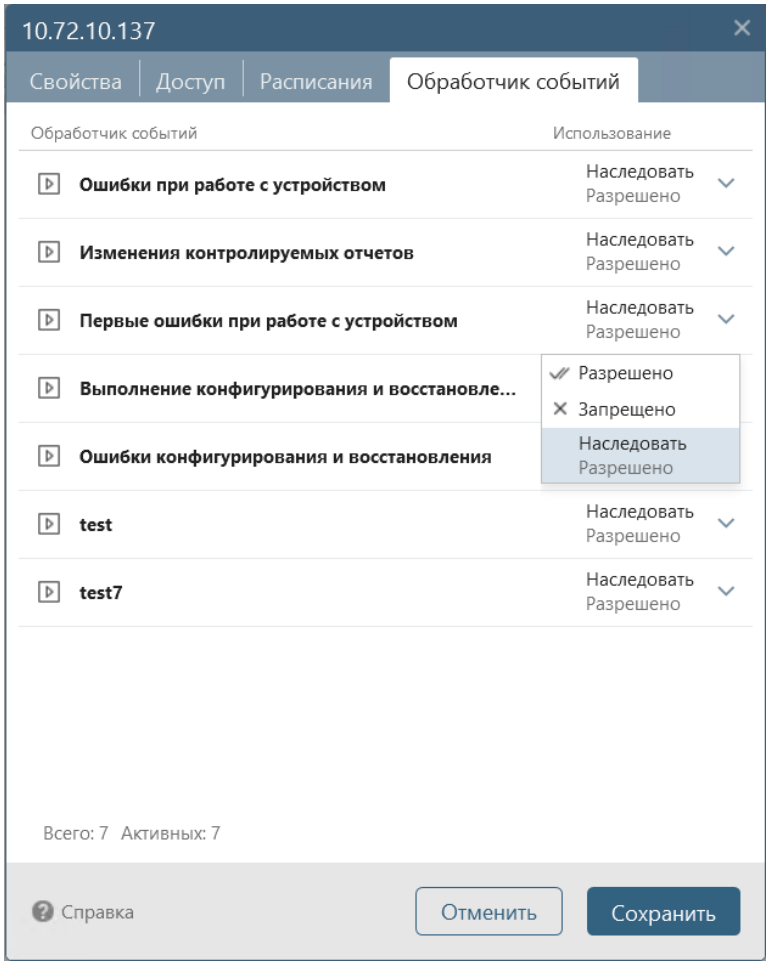


Рисунок 69 – Вкладка ***Обработчик событий***

5) В строке настраиваемого обработчика событий выбрать из перечня значений раскрывающегося списка поля *Использование* требуемое значение варианта использования триггера для выбранного устройства (см. рис. 69, состав и описание значений полей окна приведено в таблице 10).

6) Нажать кнопку ***Сохранить***. Окно свойств устройства закроется, внесенные изменения будут сохранены.

Таблица 10 – Состав и описание полей вкладки ***Обработчик событий*** для устройства

Поле	Описание/Назначение
Обработчик событий	Наименование обработчика событий
Использование	Выбор режима использования триггера. Возможные значения: – *Разрешено* – разрешить выполнение триггера вне зависимости от настроек, заданных для группы устройств, в которую входит устройство; – *Запрещено* – запретить выполнение триггера вне зависимости от настроек, заданных для группы устройств, в которую входит устройство; – *Наследовать (XXXX)* – применить настройки, заданные для группы устройств, в которую входит устройство. В скобках отображается значение, установленное для группы устройств

2.7.3. Настройка режима использования расписаний для устройств

Список расписаний ведется в разделе **Настройки** пользователями с правами *Управление* в категории *Настройки контроля.*

Изменять режим использования расписаний для устройств могут пользователи комплекса с правами *Управление* в категории *Настройки контроля* и пользователи с правами доступа *Полный доступ* к изменяемым устройствам

Для внесения изменений в настройки расписаний для выбранного устройства (группы) пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Устройства**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) В панели списка устройств выбрать устройство (группу), для которого необходимо настроить режим использования расписаний.
3) В панели кнопок списка устройств нажать кнопку ***Свойства*** () или выбрать пункт ***Свойства*** в контекстном меню устройства (группы).
4) В открывшемся окне свойств выбранного устройства (группы) перейти на вкладку ***Расписания*** (рис. 70).

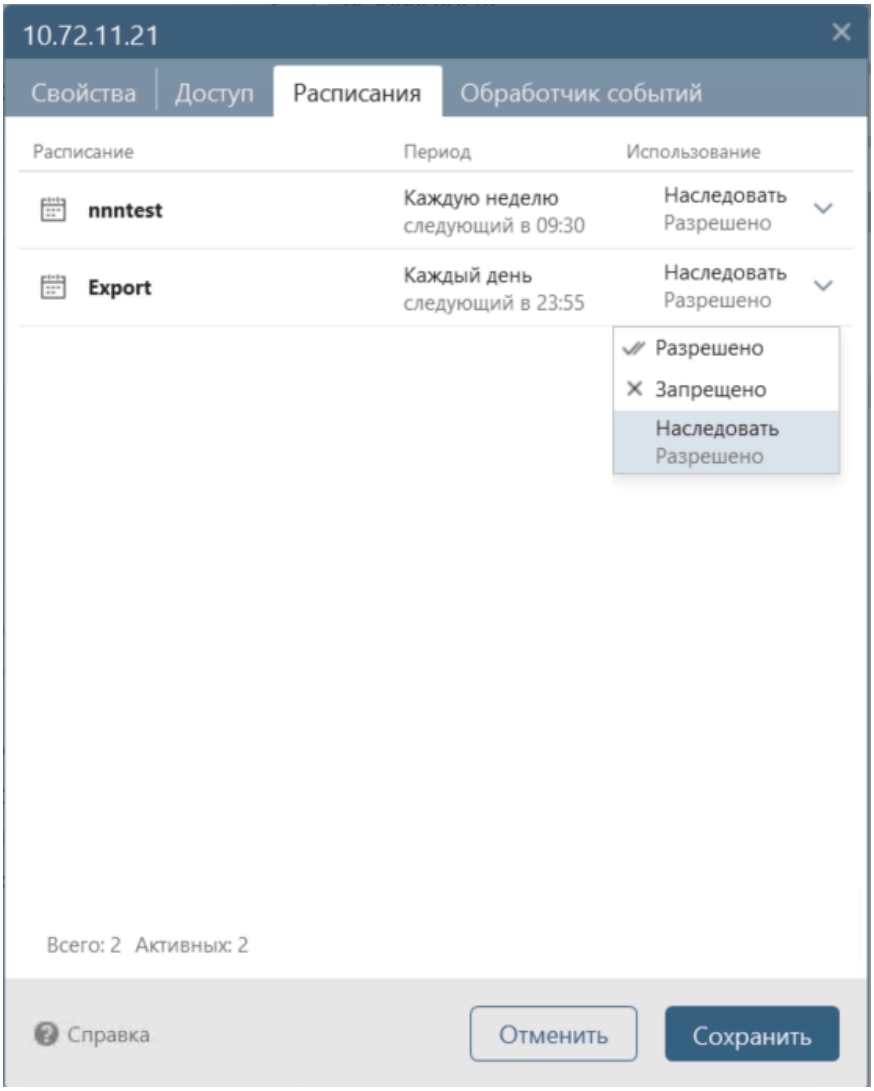


Рисунок 70 – Вкладка ***Расписания***

5) Выбрать необходимое расписание и из перечня значений раскрывающегося списка поля ***Использование*** установить требуемое значение варианта использования расписания для выбранного устройства (см. рис. 70, состав и описание значений полей окна приведено в таблице 11).

6) Нажать кнопку ***Сохранить***. Окно свойств устройства закроется, внесенные изменения будут сохранены.

Примечание – Периодичность запуска расписания настраивается в разделе **Настройки** пользователями с правами *Управление* в категории *Настройки контроля.*

Таблица 11 – Состав и описание полей вкладки настройки расписаний для устройства

Поле	Описание/Назначение
Расписание	Наименование расписания
Период	Информация о периодичности запуска расписания и времени очередного старта
Использование	Выбор режима использования расписания. Возможные значения: – *Разрешено* – разрешить выполнение расписания вне зависимости от настроек базового профиля; – *Запрещено* – запретить выполнение расписания вне зависимости от настроек базового профиля; – *Наследовать (XXXX)* – применить настройки базового профиля, используемого устройством. В скобках отображается значение, установленное для расписания в базовом профиле

2.8. Работа с устройствами

Работа пользователя комплекса с контролируемым на сервере ПК оборудованием заключается в анализе содержимого загруженных с устройств отчетов и результатов выполнения проверок устройств.

Работа с контролируемым на сервере ПК оборудованием осуществляется в разделе **Устройства** клиентской консоли (описание интерфейса раздела приведено в п. 2.4 «Просмотр и управление списком устройств в разделе **Устройства**»).

2.8.1. Загрузка отчетов

Загрузка всех отчетов, доступных для контролируемого на сервере ПК устройства, может быть выполнена:

- автоматически при проверке устройства по расписанию;
- автоматически в результате выполнения триггера (например, при получении Syslog-сообщения);
- автоматически при выводе устройства из сервисного режима;
- вручную по команде ***Загрузить*** из контекстного меню устройства (группы) в панели списка устройств или из панели ***Действия с устройством*** вкладки ***Статус*** раздела **Устройства**.

Загрузка одного типа отчета (и автоматически связанных с ним других типов отчетов) выполняется вручную по команде ***Обновить отчет*** из контекстного меню загруженного отчета, или нажатием кнопки ***Обновить*** (🔄) в строке выбранного отчета, во вкладке ***Отчеты*** раздела **Устройства.**

ВНИМАНИЕ: Операции загрузки и обновления отчетов вручную доступны пользователям, имеющим права доступа к устройствам только «чтение (просмотр, загрузка отчетов)», только при отключенном режиме *Запретить загрузку конфигураций для пользователей с правами «чтение»* (см. п. 2.4.8 «Настройка параметров безопасности учетных записей пользователей комплекса» документа 643.72410666.00082-01 96 01-01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование»)!

В зависимости от варианта использования, отчеты, загруженные с устройства впервые, могут быть автоматически приняты за эталон для проведения проверок с версиями отчетов, загружаемыми с устройства в последующем. Проверка заключается в сравнении содержания вновь загруженных версий отчетов и принятых ранее эталонных значений.

После повторной загрузки выполняется проверка каждого отчета на равенство эталону (предыдущей версии отчета соответствующего типа). В случае обнаружения различий на вкладке ***Отчеты*** отобразится соответствующая информация (рис. 71).

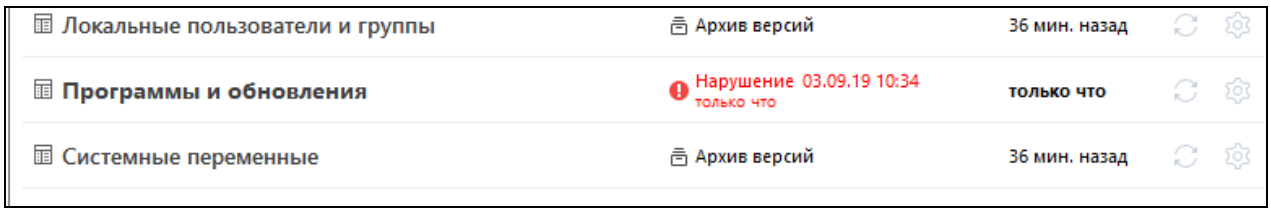


Рисунок 71 – Сообщения о нарушении при загрузке отчета

Также на вкладке ***События*** можно просмотреть сообщение о характере нарушения (рис. 72).

ЭВМ2	03.09.2019 10:34:59	Загрузка отчета	Загружен отчет "Программы и обновления"
ЭВМ2	03.09.2019 10:34:59	Запуск действий по триггеру	Запуск действий по триггеру "Check Integrity"
ЭВМ2	03.09.2019 10:34:59	Нарушение целостности	Отчет "Программы и обновления" не соответствует эталону
ЭВМ2	03.09.2019 10:34:59	Изменение отчета	Отчет "Программы и обновления" изменен и помещен в архив
ЭВМ2	03.09.2019 10:34:59	Запуск действий по триггеру	Запуск действий по триггеру "Изменения контролируемых отчетов"

Рисунок 72 – Сообщения о неэквивалентности версий отчетов

Для просмотра отчета с изменениями необходимо открыть отчет с уведомлением о нарушении, дважды щелкнув левой кнопкой «мыши» по наименованию отчета во вкладке ***Отчеты.***

Проверка версий отчетов выполняется с учетом регулярных выражений[1)], определяющих маски для контролируемых и неконтролируемых строк отчета. Настройка правил игнорирования изменения параметров устройств в отчетах выполняется в форме настройки отчетов (подробнее см. п. 2.6.3 «Настройка правил сравнения версий отчетов»).

Настройка режима использования отчетов выполняется в форме настройки отчетов (подробнее см. п. 2.6.1 «Настройка одного отчета для одного устройства»).

В разделе **Отчеты** ПК «Efros Config Inspector» v.4 пользователю доступен функционал создания на основе отчетов, загруженных с устройств, пользовательских отчетов типов *Выборка* и *История изменений* по заданным параметрам: для выбранных устройств, выбранных типов отчетов, за выбранный период (см. п. 2.12 «Просмотр отчетов в разделе **Отчеты**»)

2.8.2. Загрузка отчетов для устройства/группы устройств

Для загрузки всех доступных и разрешенных (при настройке) для устройства/группы устройств отчетов (см. п. 2.4.3 «Вкладка Отчеты») пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Устройства**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выделить в панели списка устройств устройство или группу, отчеты с которого необходимо загрузить на сервер ПК.
3) Выполнить одно из двух действий:
   - в контекстном меню устройства/группы выбрать пункт ***Загрузить***;
   - в области **Действия с устройством** вкладки ***Статус*** нажать ссылку ***Загрузить*** (для устройства) или ***Обновить устройства*** (для группы устройств).

Будет запущен процесс загрузки отчетов, в ходе которого в области ***Последняя операция*** вкладки ***Статус*** для выбранного устройства/устройств группы будет последовательно отображаться информация о результатах загрузки на сервер ПК каждого отчета.

ВНИМАНИЕ: Операции загрузки и обновления отчетов вручную доступны пользователям, имеющим права доступа к устройствам только «чтение (просмотр, загрузка отчетов)», только при отключенном режиме *Запретить загрузку конфигураций для пользователей с правами «чтение»* (см. п. 2.4.8 «Настройка параметров безопасности учетных записей пользователей комплекса» документа 643.72410666.00082-01 96 01-01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование»)!

[1)] Описание регулярных выражений стандарта PCRE, допустимых к применению в ПК «Efros Config Inspector» v.4, приведено в Приложении 1.

2.8.3. Получение отчета о состоянии контролируемых устройств

На сервере ПК существует возможность получения отчета со сведениями о состоянии доступных пользователю для контроля устройств.

Экспорт списка устройств группы из раздела **Устройства** может выполнить любой пользователь комплекса. Для экспорта списка устройств группы пользователю необходимо выполнить следующие действия:

- перейти в раздел **Устройства**;
- выбрать в списке устройств панели списка требуемую группу устройств;
- выбрать в рабочей области раздела вкладку ***Устройства*** (см. п. 2.4.6 «Вкладка Устройства»);
- нажать над таблицей списка устройств, входящих в группу, кнопку ***Экспорт*** ( );
- указать в открывшемся окне **Экспорт списка устройств** установкой флагов тип выгружаемых данных и установкой переключателя – формат файла отчета (рис. 73);
- нажать кнопку ***Экспортировать***;
- в открывшемся стандартном окне ОС **Сохранить как** указать имя и месторасположение файла отчета и нажать кнопку ***Сохранить***.

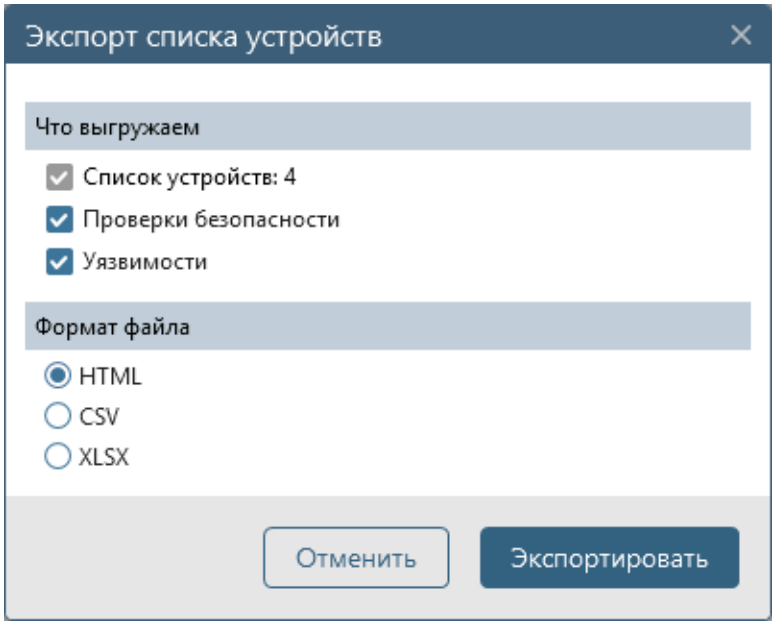


Рисунок 73 – Окно **Экспорт списка устройств**

В файле отчета содержится список объектов (устройств и каталогов/групп), включенных в группу, с учетом заданных параметров фильтрации, параметры каждого из этих устройств, результат выполнения последней операции для каждого устройства и сведения о результатах выполнения проверок каждого устройства.

2.8.4. Контроль целостности файловых объектов ОС устройств

Проверка целостности поставленных на контроль файловых объектов ОС устройств может быть выполнена на сервере ПК тремя способами.

СПОСОБ 1.

Проверка целостности файловых объектов, поставленных на контроль, запускается автоматически при загрузке ОС устройства. В этом случае предварительно пользователю с правами *Управление* в категории *Настройки контроля* следует:

- на контролируемом устройстве (кроме рабочих станций и серверов, с установленной ОС Windows) настроить автоматический запуск задания отправки сообщения по протоколу Syslog на сервер ПК по событию загрузки/перезагрузки ОС;
- в клиентской консоли создать триггер (обработчик события), который в ответ на получение сервером ПК Syslog-сообщения о запуске ОС или запуске Windows агента, выполнит загрузку отчетов с устройств.

При получении соответствующего сообщения:

1) Сервер ПК фиксирует событие получения Syslog-сообщения и подключается к контролируемому устройству.

2) Выполняется автоматическая загрузка отчетов (конфигурационных файлов) с устройства в БД комплекса и обработка загруженных данных (например, подсчет контрольных сумм).

3) По результатам обработки загруженных отчетов формируются производные отчеты устройства. Далее производится контроль целостности загруженных и сформированных в процессе обработки отчетов согласно установленным параметрам отчетов для данного типа устройств.

4) При несоответствии отчета эталонной версии формируется уведомление о нарушении целостности контролируемых объектов, содержащее ссылку на форму просмотра отчета с отображением выявленных изменений.

СПОСОБ 2.

Проверка целостности файловых объектов, поставленных на контроль, запускается автоматически в соответствии с заданным на сервере ПК расписанием. Во втором случае:

1) В соответствии с заданным расписанием сервер ПК подключается к контролируемому устройству.

2) Выполняются приведенные выше для способа 1 шаги 2 – 4 контроля целостности.

СПОСОБ 3.

Проверка целостности файловых объектов, поставленных на контроль, запускается пользователем вручную активацией команды ***Загрузить*** в панели списка устройств раздела **Устройства**. В третьем случае:

1) Пользователю следует:
   - выполнить запуск клиентской консоли;
   - перейти в раздел **Устройства**;
   - выбрать в контекстном меню требуемого устройства пункт ***Загрузить***.

2) Далее сервер ПК автоматически подключается к контролируемому устройству.

3) Выполняются приведенные выше для способа 1 шаги 2 – 4 контроля целостности.

Если устройство не доступно (выключено или отсутствует связь с устройством), то после запуска операции загрузки отчетов формируется уведомление об ошибке загрузки отчета.

2.8.5. Конфигурирование устройства

Вкладка ***Статус*** раздела **Устройства** содержит блок полей ***Действия с устройством,*** в котором доступен перечень операций для выполнения на выбранном устройстве/группе с сервера ПК (рис. 74). Список доступных операций в области ***Действия с устройством*** зависит от типа устройства.

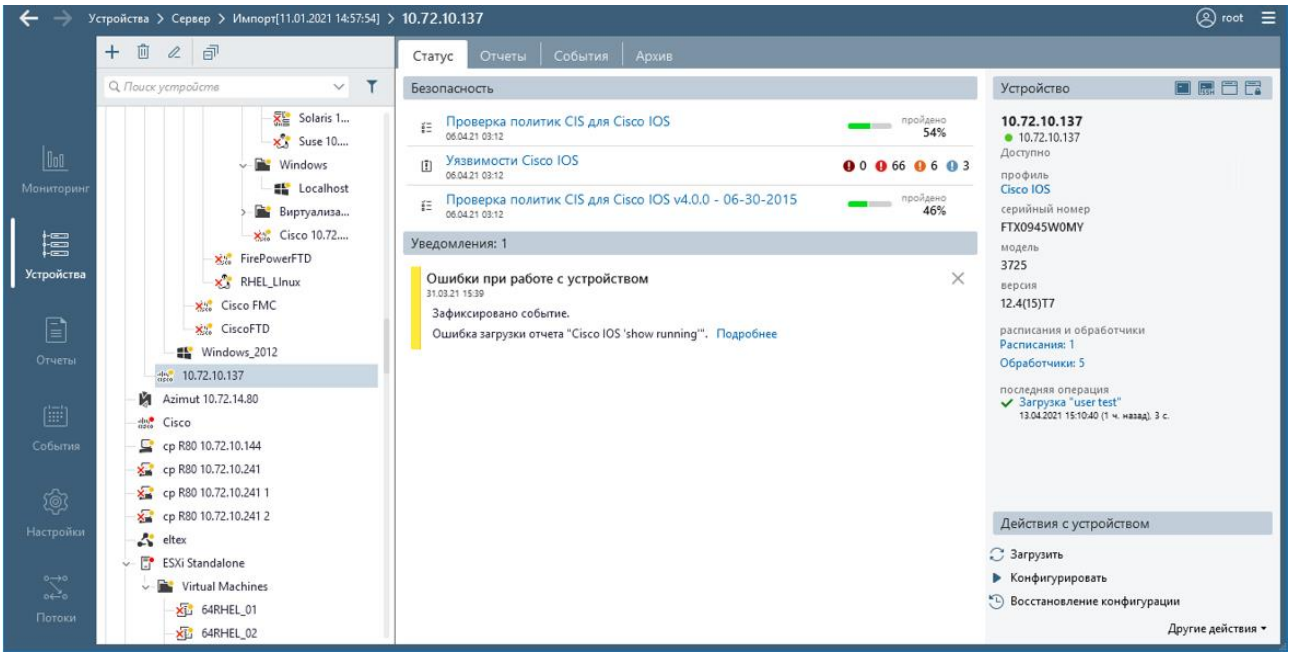


Рисунок 74 – Вкладка ***Статус*** раздела **Устройства** с раскрытым списком ***Действия с устройством***

ВНИМАНИЕ: Операции изменения и восстановления конфигурации устройств доступны только после подключения сервисного модуля «Управление устройствами» (см. п. 3.2.4 «Настройка параметров внешних модулей» документа 643.72410666.00082-01 96 01-01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование») и только для устройств, поддерживающих возможность выполнения этих операций!

Для изменения конфигурации устройства необходимо выполнить следующие действия:

1) Перейти в раздел **Устройства**, для чего нажать соответствующую кнопку в панели выбора раздела консоли. В списке устройств выбрать необходимое устройство для изменения его конфигурации.

2) В открывшейся вкладке ***Статус*** в блоке полей ***Действия с устройством*** выбрать ссылку ***Конфигурировать.***

3) В открывшемся окне ***Конфигурирование оборудования*** (рис. 75, таблица 12) заполнить поле *Команды конфигурирования* одним из способов***:***

- способ 1 – выбрать набор команд в поле *Сохраненные наборы команд* из списка сохраненных шаблонов наборов команд;
- способ 2 – ввести набор команд в поле *Команды конфигурации* вручную;

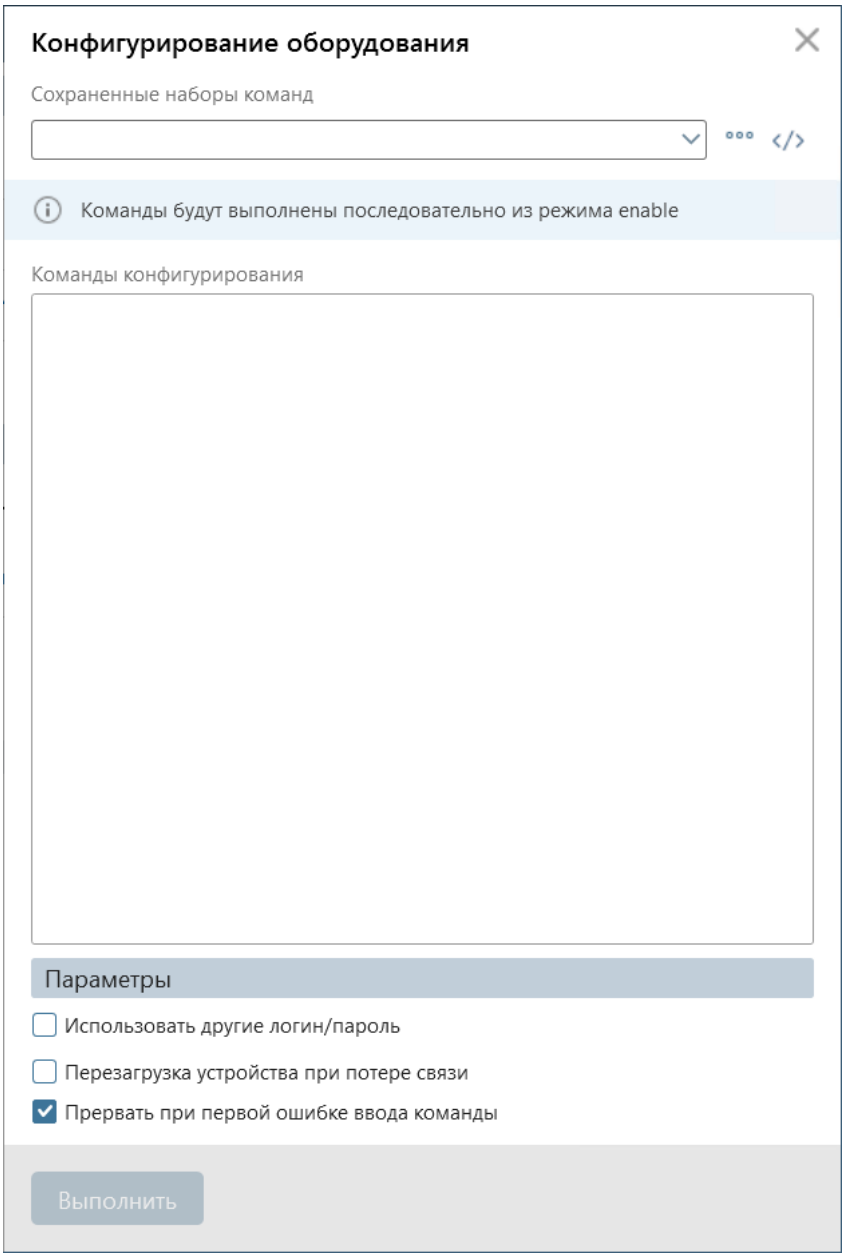


Рисунок 75 – Окно **Конфигурирование оборудования**

Таблица 12 – Состав и описание полей окна **Конфигурирование оборудования**

Поле	Описание/Назначение
Сохраненные наборы команд	Поле со списком ранее созданных и сохраненных шаблонов наборов команд конфигурирования устройств соответствующего типа. Поддерживается сохранение/изменение/удаление шаблонов наборов команд конфигурирования. По нажатию кнопки ***Меню*** (⁰⁰⁰) раскрывается контекстное меню к полю, содержащее пункты

Поле	Описание/Назначение
	Сохранить, *Сохранить как*, *Переименовать* и *Удалить* для выполнения с выбранным (или вновь созданным) шаблоном соответствуего действия. Справа содержит кнопку ***Генерация скрипта AAA*** (</>), по нажатию которой открывается окно ввода параметров, на основе которых далее автоматически будет сгенерирован шаблон. Набор команд шаблона доступен пользователю в поле *Команды конфигурирования* (см. ниже) для внесения изменений и сохранения в новом шаблоне. Примечание – Возможность генерации шаблона набора команд в окне ввода параметров (для настройки AAA модели) 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 и Mikrotik (RouterOS)
Команды конфигурирования	Поле для отображения и редактирования набора команд, выбранного в поле *Сохраненные наборы команд* шаблона или сформированного на основе параметров, заданных в окне **Скрипт настройки AAA**, или для ввода нового набора команд
Область *«Параметры»* (рис. 76)	
Использовать другие логин и пароль	Поле для флага. По умолчанию флаг в поле не установлен. При установке флага в окне отображаются дополнительные поля для ввода данных пользователя (логин, пароль и дополнительный пароль) для доступа к устройству при выполнении действий по конфигурированию устройства
Перезагрузка устройства при потере связи	Поле для флага. По умолчанию флаг в поле не установлен. При установке флага в окне дополнительно отображается поле для ввода времени задержки (от 1 до 99 минут) до перезагрузки устройства при потере связи с ним
Прервать при первой ошибке ввода команды	Поле для флага. По умолчанию флаг в поле установлен. При фиксировании первой ошибки ввода команды конфигурирования операция конфигурирования устройства будет прервана

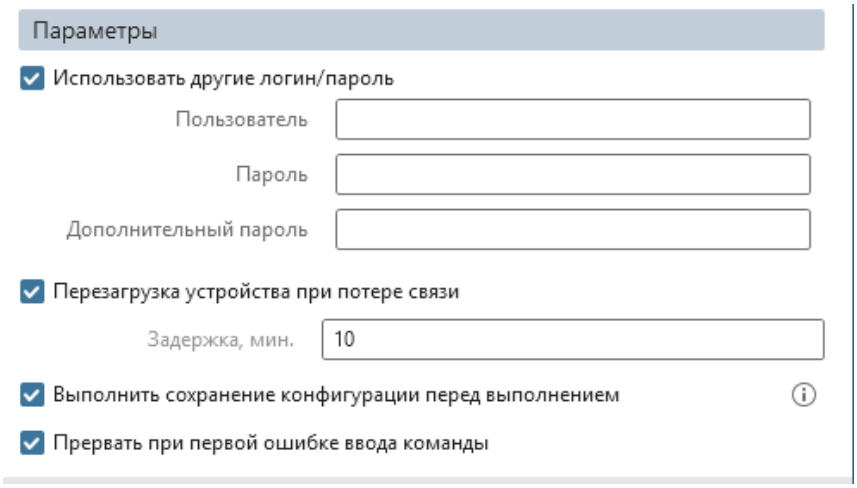


Рисунок 76 – Область ***Параметры*** с выбранными параметрами

– способ 3 – нажать кнопку ***Генерация скрипта ААА*** (</>), выбрать в открывшемся окне **Скрипт настройки ААА (<тип устройства>)** (рис. 77, таблица 13) параметры генерации набора команд и нажать кнопку ***Применить***.

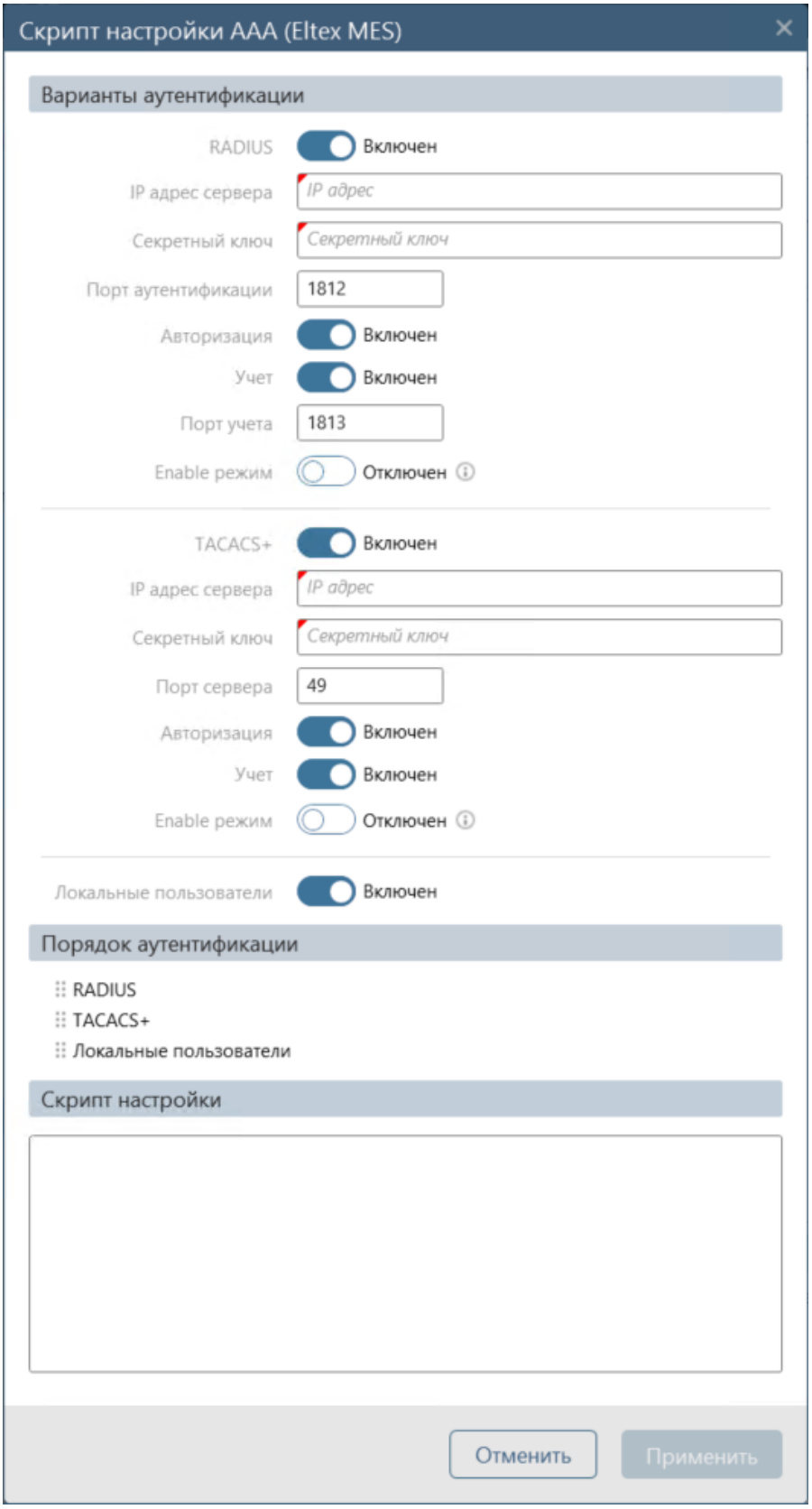


Рисунок 77 – Окно **Скрипт настройки ААА (<тип устройства>)**

Таблица 13 – Состав и описание полей окна **Скрипт настройки AAA (<тип устройства>)**

Поле	Описание/Назначение
Варианты аутентификации	Предназначена для выбора вариантов аутентификации на устройстве – через сервер RADIUS, TACACS и/или в качестве локального пользователя. При выключении переключателей ***RADIUS***, ***TACACS*** и ***Локальные пользователи*** отключается и возможность аутентификации соответствующего типа, скрываются поля параметров соответствующего типа аутентификации. По умолчанию включены все три типа аутентификации с параметрами: 1. Тип аутентификации ***RADIUS***: – *IP адрес сервера* – адрес текущего сервера ПК; – *Порт аутентификации* – 1812; – *Порт учета* – 1813; – *Авторизация* – переключатель включен; – *Учет* – переключатель включен; – *Enable режим* – переключатель выключен. 2. Тип аутентификации ***TACACS***: – *IP адрес сервера* – адрес текущего сервера ПК; – *Порт сервера* – 49; – *Порт учета* – 49 (используется только для устройств типа Huawei VRP); – *Авторизация* – переключатель включен; – *Учет* – переключатель включен; – *Enable режим* – переключатель выключен. При включении переключателя ***Enable режим***, будет выполняться автоматический переход в привилегированный режим. Примечание – Для устройств типа Cisco ASA (рис. 78) может быть включен только один из вариантов аутентификации ***RADIUS*** или ***TACACS*** и порядок аутентификации не доступен для изменения – тип аутентификации ***Локальные пользователи*** в поле *Порядок аутентификации* (см. ниже) всегда расположен на второй позиции
Порядок аутентификации	Поле содержит строки с включенными в поле *Варианты аутентификации* типами аутентификации, предназначено для настройки порядка выполнения аутентификации. Настройка выполняется путем «перетаскивания» (drag&drop) строк
Скрипт настройки	Поле для отображения скрипта аутентификации AAA, сгенерированного в соответствии с заданными в полях *Варианты аутентификации* и *Порядок аутентификации* настройками. Внесение изменений вручную в текст скрипта в этом поле не доступен

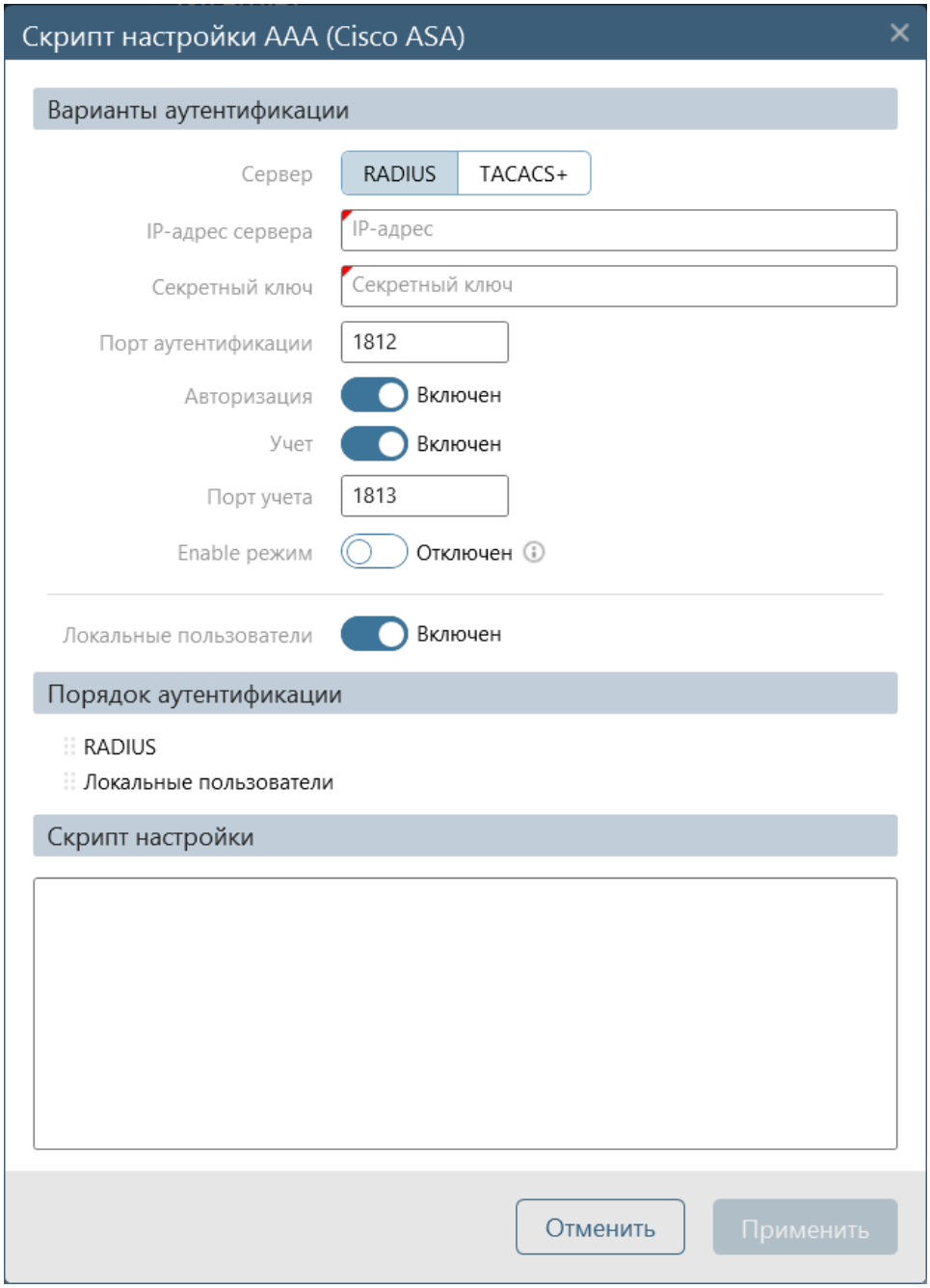


Рисунок 78 – Окно **Скрипт настройки AAA (Cisco ASA)**

4) В области ***Параметры*** выбрать установкой флагов требуемые параметры конфигурирования.

5) Указать, при необходимости, значения выбранных параметров: другие логин и пароль для доступа к устройству при выполнении действий по конфигурированию устройства, динамические настройки выполнения конфигурирования (характерные для выбранного типа устройств).

6) Нажать кнопку ***Выполнить***.

Доступна для выполнения также команда по восстановлению загрузочной конфигурации сетевого оборудования с использованием ранее сохраненной настройки конфигурации (в случае необходимости восстановления работоспособности устройства). При выборе в блоке полей ***Действия с устройством*** ссылки ***Восстановление конфигурации*** после подключения к

устройству и загрузки его конфигурации открывается окно **Восстановление конфигурации** (рис. 79).

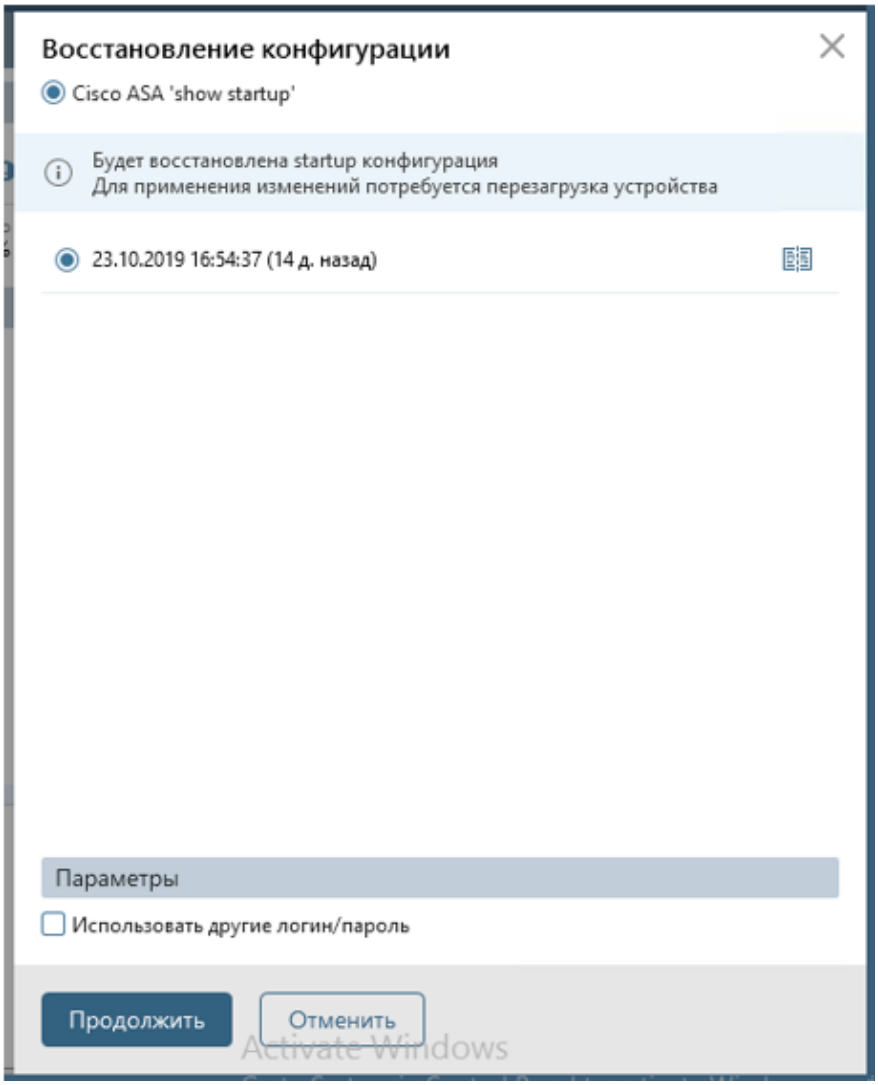


Рисунок 79 – Окно **Восстановление конфигурации**

Для восстановления конфигурации устройства необходимо выполнить следующие действия:

1) В окне **Восстановление конфигурации** выбрать сохраненную ранее конфигурацию.

При необходимости можно просмотреть выбранную для восстановления конфигурацию, нажав кнопку ***Сравнение*** ( ). В открывшемся окне **Сравнение отчетов** можно сравнить архивную версию отчета, выбранного для восстановления конфигурации, и текущую версию конфигурации (рис. 80).

2) В области ***Параметры*** указать, при необходимости, другие логин и пароль для доступа к устройству при выполнении действий по конфигурированию устройства.

3) Нажать кнопку ***Продолжить***.

В результате произойдет обновление конфигурации выбранного устройства.

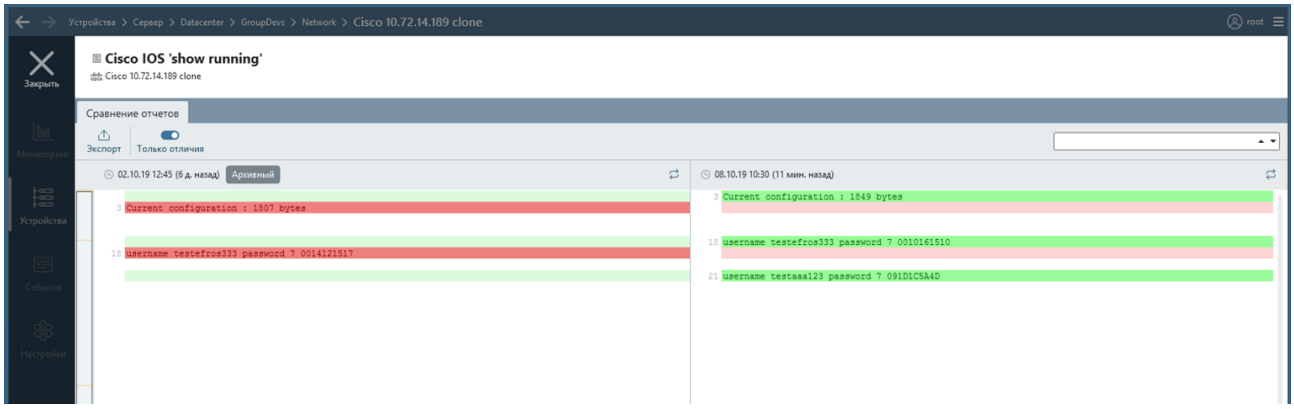


Рисунок 80 – Окно **Сравнение отчетов**

2.8.6. Конфигурирование группы устройств

На сервере ПК существует возможность изменения конфигурации группы устройств.

ВНИМАНИЕ: Операции изменения и восстановления конфигурации устройств доступны только после подключения сервисного модуля **Управление устройствами** (см. п. 2.3.2 «Подключение внешних модулей» документа 643.72410666.00082-01 96 01-01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование») и только для устройств, поддерживающих возможность выполнения этих операций!

Для изменения конфигурации группы устройств пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Устройства**, для чего нажать соответствующую кнопку в панели выбора раздела консоли. В списке устройств выбрать группу для изменения конфигураций входящих в нее устройств.

2) В открывшейся вкладке ***Статус*** в блоке полей ***Действия с устройством*** выбрать ссылку ***Конфигурация устройств.***

3) В открывшемся окне ***Конфигурирование оборудования*** (рис. 81) выбрать тип доступного для выполнения действия устройства из предлагаемого перечня в поле ***Тип устройства.***

4) Заполнить поле ***Команды конфигурирования*** одним из способов***:***

- способ 1 – выбрать набор команд в поле *Сохраненные наборы команд* из списка сохраненных шаблонов наборов команд;
- способ 2 – ввести набор команд в поле *Команды конфигурации* вручную;
- способ 3 – нажать кнопку «Генерация скрипта AAA» (</>), выбрать в открывшемся окне **Скрипт настройки AAA (<тип устройства>)** (см. п. 2.8.5 «Конфигурирование устройства») параметры генерации набора команд и нажать кнопку ***Применить***.

Примечание – В версии 4.14.100 ПК «Efros Config Inspector» v.4 заполнение поля ***Команды конфигурирования*** способом 3 доступно только для устройств следующих типов: Eltex MES, Eltex ESR, Cisco ASA, Cisco IOS, Huawei VRP и Mikrotik (RouterOS).

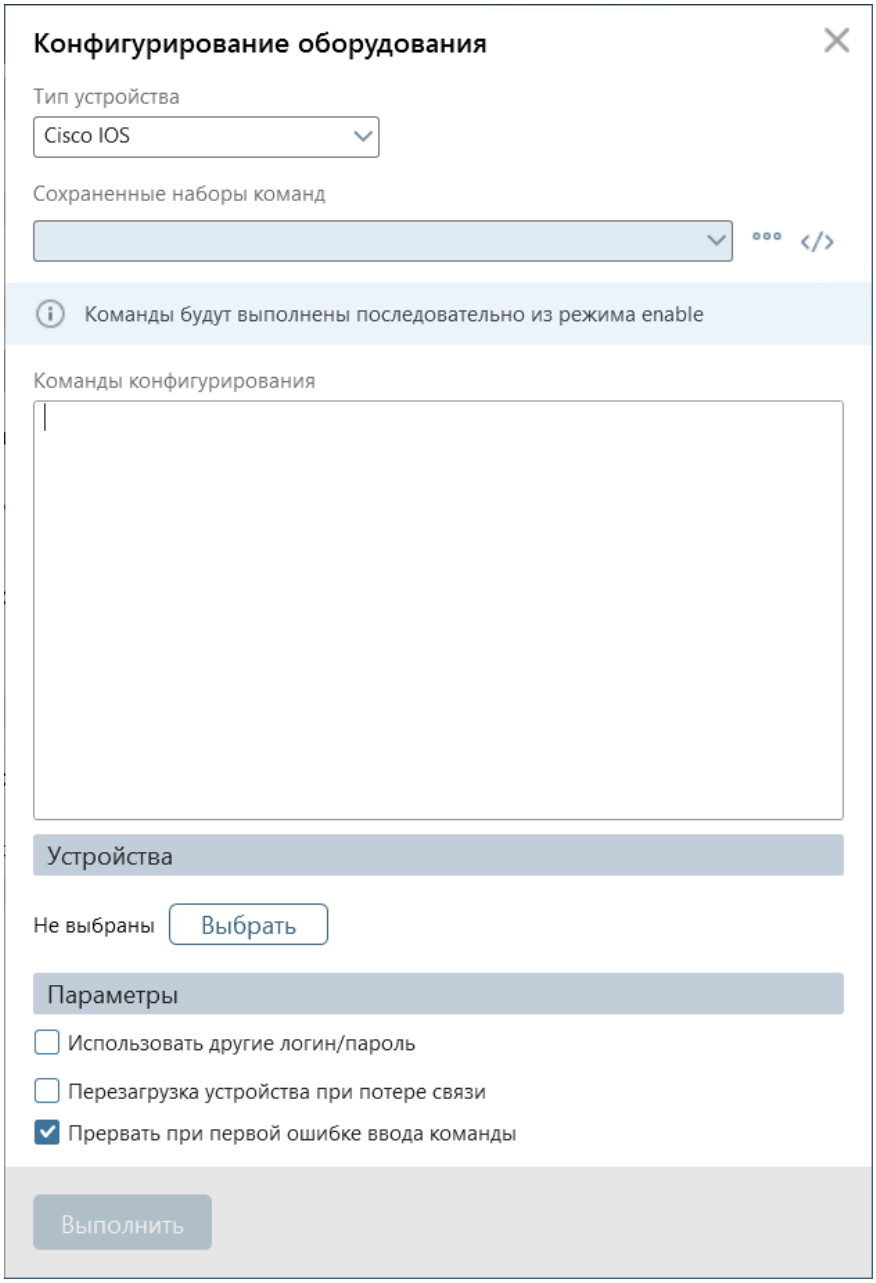


Рисунок 81 – Окно **Конфигурирование оборудования** для группы устройств

5) В области ***Устройства*** нажать кнопку ***Выбрать*** и в открывшемся окне **Выбор устройств** отметить устройства в соответствии с выбранным типом для изменения конфигурации.

Примечание – Правила поиска, фильтрации и выбора устройств в окне выбора устройств приведены п. 2.2.5.4 «Настройка виджетов».

6) В области ***Параметры*** (см. рис. 81) выбрать установкой флагов требуемые параметры конфигурирования. Указать, при необходимости, значения выбранных параметров: другие логин и пароль для доступа к устройству при выполнении действий по конфигурированию устройства, динамические настройки выполнения конфигурирования (характерные для выбранного типа устройств).

7) Нажать кнопку ***Выполнить***.

2.8.7. Перевод устройства в сервисный режим

На сервере ПК есть возможность перевода устройства в сервисный режим. В сервисном режиме устройство не опрашивается по заданному расписанию и не проверяется в автоматическом режиме его доступность, обновление данных выполняется только по запросу пользователя.

Для перевода устройства в сервисный режим пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Устройства**, для чего нажать соответствующую кнопку в панели выбора раздела консоли. В списке устройств выбрать устройство для перевода его в сервисный режим.

2) Выбрать в контекстном меню устройства пункт ***Включить сервисный режим*** либо нажать в строке меню панели списка устройств кнопку ***Свойства*** (), в открывшемся окне (рис. 82) перевести переключатель ***Сервисный режим*** в положение ***Включен*** () и нажать кнопку ***Сохранить***.

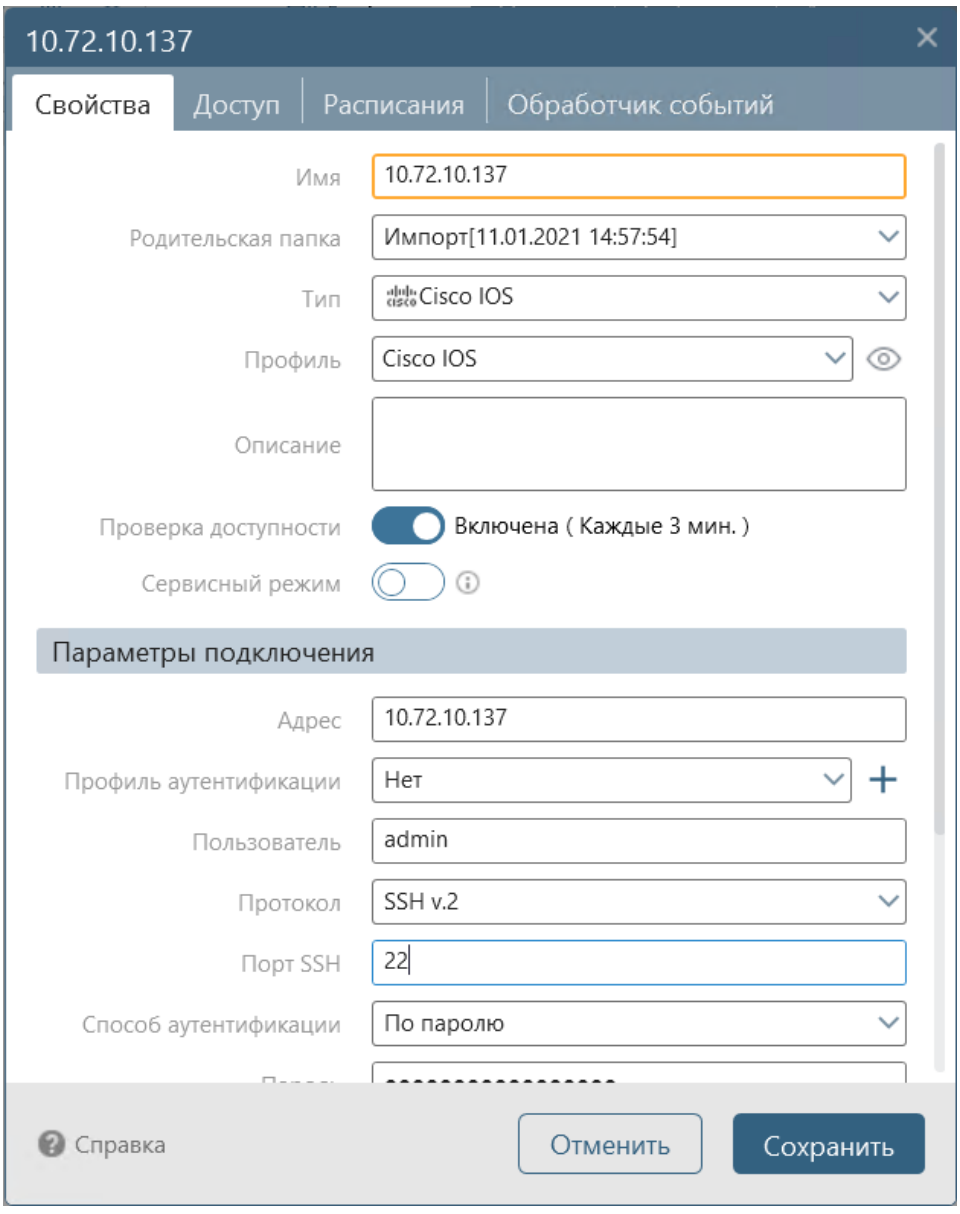


Рисунок 82 – Окно настройки свойств устройства

В левой части пиктограммы устройства отобразится оранжевый ключ, в заголовке вкладки ***Статус*** устройства отобразится соответствующее сообщение и команда отключения сервисного режима (рис. 83).

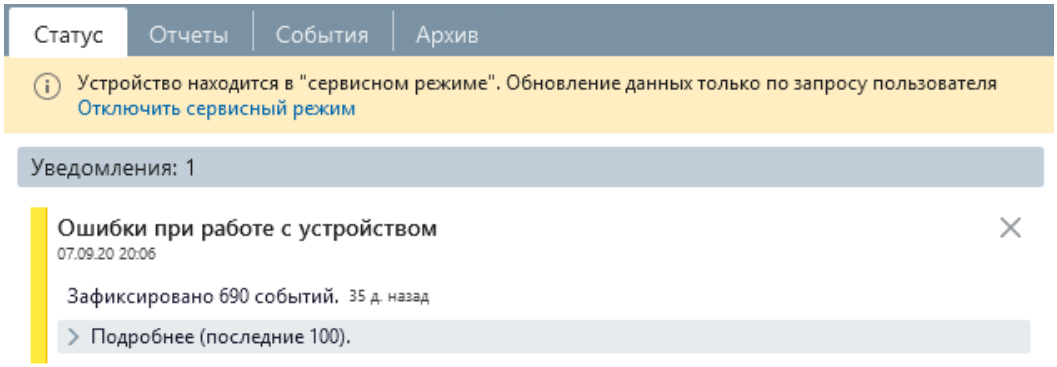


Рисунок 83 – Сообщение о нахождении устройства в сервисном режиме

Для отключения для устройства сервисного режима пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Устройства**, для чего нажать соответствующую кнопку в панели выбора раздела консоли. В списке устройств выбрать устройство для вывода его из сервисного режима.
2) Выбрать в контекстном меню устройства пункт ***Отключить сервисный режим*** либо нажать в заголовке вкладки ***Статус*** ссылку ***Отключить сервисный режим***, либо нажать в строке меню панели списка устройств кнопку ***Свойства*** (), в открывшемся окне (см. рис. 82) перевести переключатель ***Сервисный режим*** в положение ***Отключен*** () и нажать кнопку ***Сохранить***.

В левой части пиктограммы устройства перестанет отображаться оранжевый ключ, автоматически запустится загрузка всех включенных для него при настройке отчетов.

2.9. Работа с последними загруженными версиями отчетов

2.9.1. Просмотр отчета

Для просмотра последней загруженной версии отчета в разделе **Устройства** из списка во вкладке ***Отчеты*** необходимо дважды щелкнуть левой кнопкой «мыши» на строке с требуемым отчетом или выбрать в контекстном меню отчета пункт ***Открыть отчет***. В результате откроется форма просмотра отчета (пример формы просмотра отчета приведен на рис. 84).

В заголовке формы просмотра отчета указаны название отчета, дата и время последнего обновления отчета (в скобках указан прошедший интервал времени), установленный для отчета режим использования (***Архив версий*** или ***Только последний***), имя устройства в ПК «Efros Config Inspector» v.4. Имя устройства является ссылкой, при нажатии которой открывается карточка устройства (см. рис. 81).

Примечание – Пользователь имеет возможность в карточке выделить и скопировать данные устройства: имя устройства, адрес, описание (при его наличии в карточке), модель, версию.

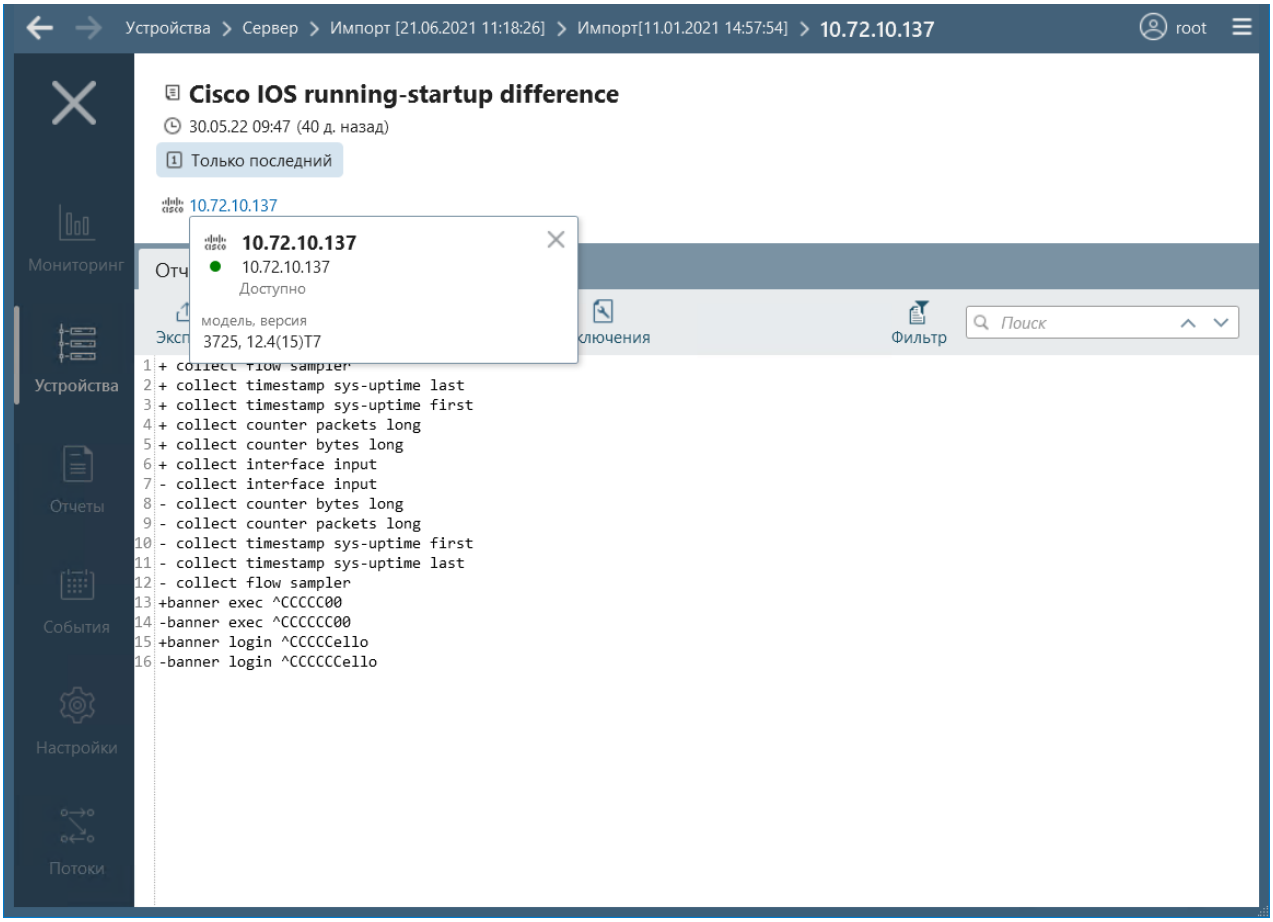


Рисунок 84 – Пример формы просмотра отчета с раскрытой карточкой устройства

При открытии на просмотр отчета проверок МЭ (отчет оптимизации правил, отчеты зонного анализа и отчет стандартов МЭ) после внесения изменений в настройки проверок МЭ и до обновления отчета отображается сообщение *Настройки проверки изменились, для получения актуальных данных обновите отчет* с кнопкой ***Обновить***. После нажатия кнопки будет выполнено обновление отчета с учетом измененных настроек.

Примечание – Если требующий обновления отчет открыт одним пользователем, а другой одновременно с этим запустил операцию обновления отчета, то текст сообщения изменится на *Доступна свежая версия текущего отчета*.

Формы просмотра отчетов содержат вкладку ***Отчет*** с данными отчета и, если для отчета установлен режим использования ***Архив версий*** или ***Контроль изменений,*** вкладку ***История изменений*** со списком версий отчета.

Во вкладке ***История изменений*** заголовок каждого измененного отчета содержит дату и время его изменения, обобщенные количественные данные изменений, а также кнопку ***Меню*** (⋯), по нажатию которой пользователь имеет возможность:

- перейти к просмотру соответствующего отчета;
- сравнить отчет с текущим отчетом;

- добавить/редактировать комментарий к отчету.

Если для отчета включен контроль целостности (установлен режим использования ***Контроль изменений***) и установлен эталонный отчет, то во вкладке ***История изменений*** эталонный отчет отмечен знаком (✔) с указанием логина пользователя, установившего эталон версии, и даты и времени установки эталона.
Если ранее для отчета внесен комментарий, то текст комментария отображается под заголовком версии отчета.

Изменения, зафиксированные в отчете, выделяются цветом шрифта:

- красным цветом – удаленные и старые значения версии отчета;
- зеленым цветом – добавленные и новые значения версии отчета.

Примечание – Если отчет пустой, то во вкладке ***Отчет*** отображается сообщение *Данные отсутствуют,* также, если для отчета не зафиксированы изменения, то во вкладке ***История изменений*** отображается сообщение *Изменения отсутствуют*.

В отчетах доступны:

- выбор периода – по нажатию кнопки ***Выберите период*** (📅) открывается окно выбора начальной и конечной дат периода, за который отображаются данные отчета. В окне также могут быть выбраны преднастроенные периоды *Сегодня*, *Вчера*, *Последние 7/14/30 дней*. Настройка применяется по нажатию кнопки ***Применить***, отменяется – по нажатию кнопки ***Очистить***;
- фильтрация данных – по нажатию кнопки ***Фильтр*** (📋) открывается окно фильтрации с полями для выбора требуемых параметров фильтрации (выбор осуществляется установкой флагов) и кнопкой сброса настройки фильтра;
- поиск данных – после ввода в поле поиска последовательности символов и нажатия кнопки ENTER, найденная в отчете последовательность будет выделена желтым цветом фона.

Количество отображаемых версий отчетов во вкладке ***История изменений*** ограничено. Если версий более 100, то выводятся первые 100 записей в соответствии с заданными настройками периода и фильтрации, в нижней части окна отображается сообщение *Показаны первые 1000 записей*. Для просмотра требуемой версии отчета, не попавшей в число отображаемых, необходимо выбрать другой временной период и/или параметры фильтрации списка.

2.9.1.1. Просмотр структурированных отчетов

В форме просмотра структурированных отчетов, используя кнопки меню вкладки, пользователь может выполнить следующие действия:

1) Во вкладке ***Отчет*** (рис. 85):

- сохранить отчет в файл формата XML или HTML;
- обновить отчет;
- настроить использование отчета для устройства (выбор из значений: *Контроль изменений, Архив версий, Только последний, Запрещено* или *Наследовать* (XXXX), где XXXX – настройки базового отчета);

- сравнить с любой из ранее загруженных на сервер ПК версией этого отчета;
- настроить представление отчета: в табличном виде или в виде дерева (с раскрытыми или свернутыми уровнями дерева);
- задать фильтрацию отчета с возможностью создания нового типа отчета.

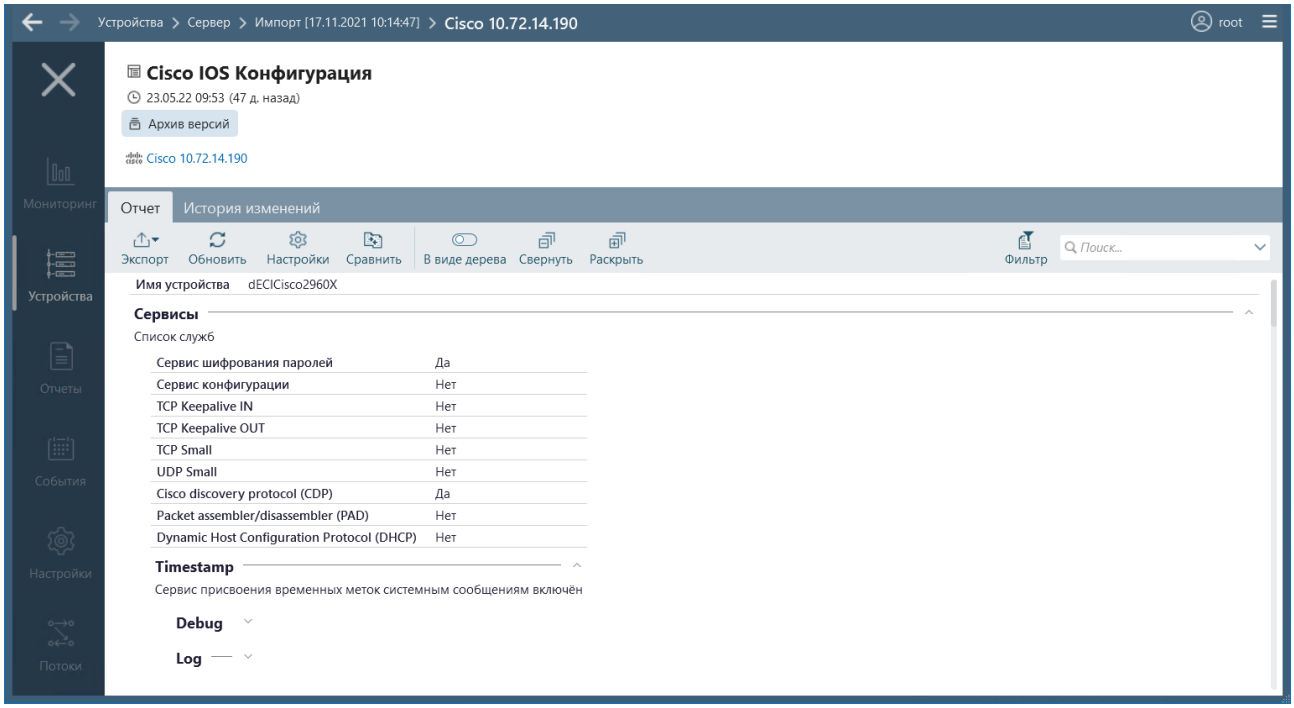


Рисунок 85 – Форма просмотра структурированного отчета. Вкладка ***Отчет***

2) Во вкладке ***История изменений*** (рис. 86):

- сохранить историю изменений отчета в файл формата HTML;
- настроить представление изменений с раскрытыми или свернутыми уровнями данных (только заголовок изменения отчета (дата и время; количество добавленных, измененных и удаленных элементов) или с описанием изменений);
- для каждого измененного отчета отдельно по кнопке ***Меню*** (⋯):
  а) перейти к просмотру соответствующего отчета;
  б) сравнить отчет с текущим отчетом;
  в) добавить/редактировать комментарий к отчету.

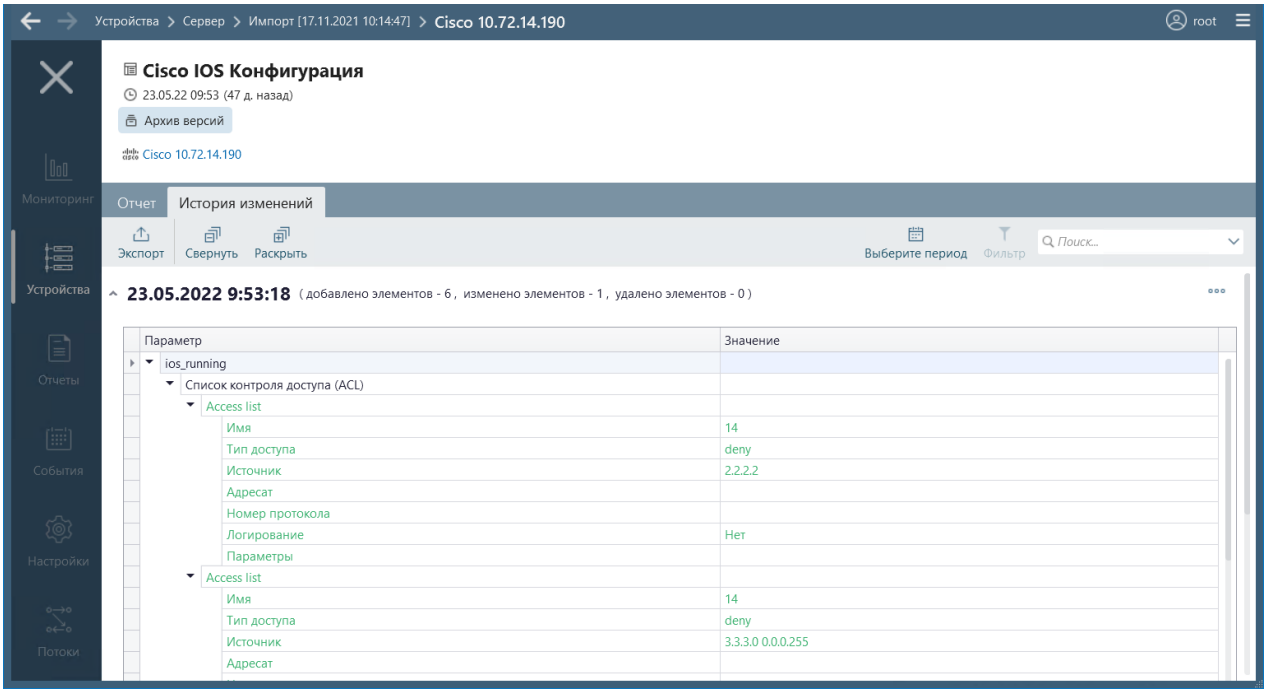


Рисунок 86 – Форма просмотра структурированного отчета. Вкладка ***История изменений***

2.9.1.2. Просмотр текстовых отчетов

В форме просмотра текстовых отчетов, используя кнопки меню вкладки, пользователь может выполнить следующие действия:

1) Во вкладке ***Отчет*** (рис. 87):
- сохранить отчет в формате TXT;
- обновить отчет;
- настроить использование отчета для устройства (выбор из значений: *Контроль изменений, Архив версий, Только последний, Запрещено* или *Наследовать (XXXX), где XXXX – настройки базового отчета*);
- сравнить с любой из ранее загруженных на сервер ПК версией этого отчета;
- просмотреть и установить (при наличии прав *Управление* в категории *Настройки контроля*) правила игнорирования изменений параметров устройства в загружаемом на сервер ПК отчете;
- задать фильтрацию отчета с возможностью создания нового типа отчета (при наличии прав *Управление* в категории *Настройки контроля*).

2) Во вкладке ***История изменений*** (рис. 88):
- сохранить историю изменений отчета в файл формата HTML;
- настроить представление изменений с раскрытыми или свернутыми уровнями данных (только заголовок изменения отчета (дата и время; количество добавленных, измененных и удаленных элементов) или с описанием изменений);
- для каждого измененного отчета отдельно по кнопке ***Меню*** (⋯):
  а) перейти к просмотру соответствующего отчета;
  б) сравнить отчет с текущим отчетом;
  в) добавить/редактировать комментарий к отчету.

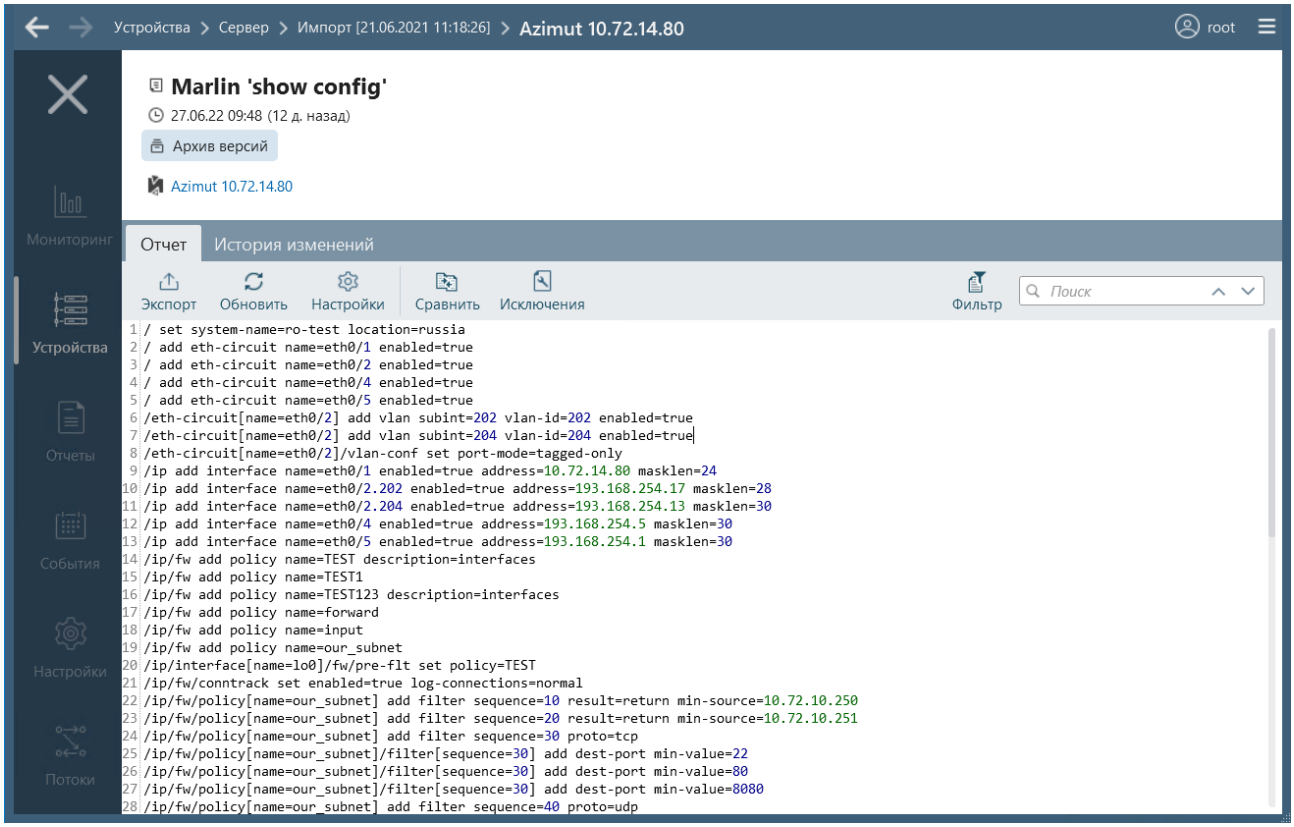


Рисунок 87 – Форма просмотра текстового отчета. Вкладка ***Отчет***

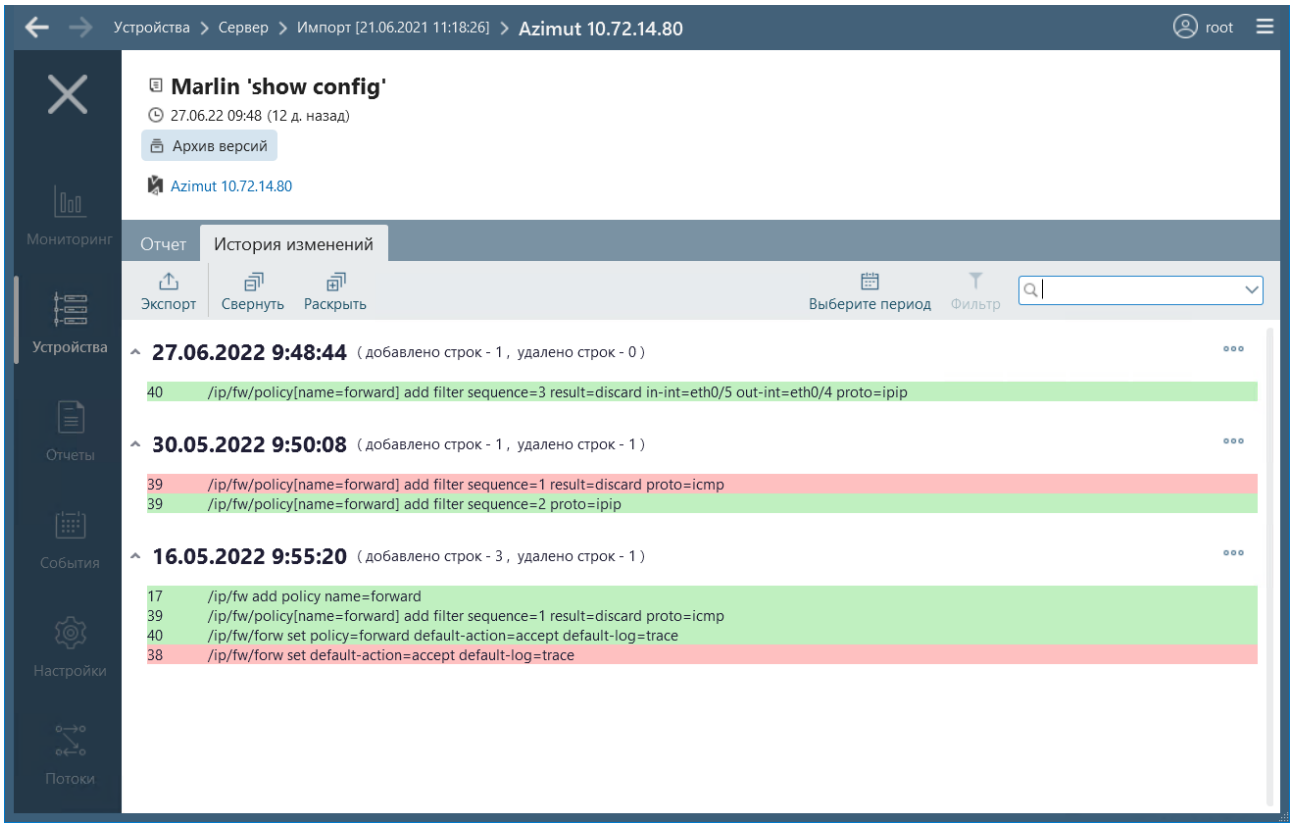


Рисунок 88 – Форма просмотра текстового отчета. Вкладка ***История изменений***

2.9.1.3. Особенности просмотра отчетов

При просмотре отчетов дополнительно:

1) В заголовке форм просмотра отчетов типа ***Отчет о проверке*** (рис. 89) дополнительно отображается индикатор защищенности устройства. Во вкладке ***Отчет*** пользователь может:

- используя переключатель ***Только нарушения***, выполнить фильтрацию результатов проверок для просмотра;
- используя раскрывающееся меню кнопки ***Экспорт,*** выбрать для выгрузки в файл формата HTML все проверки, только нарушенные или только пройденные успешно.

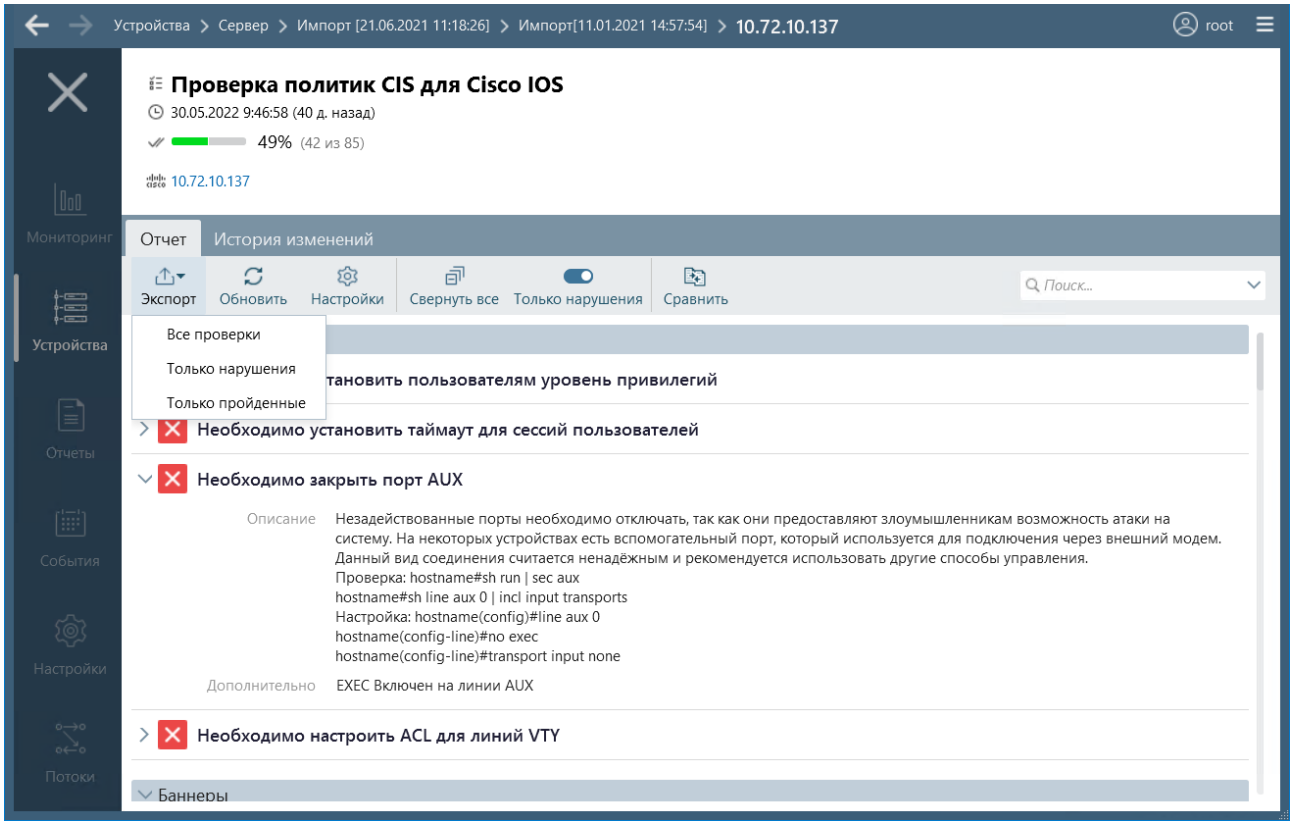


Рисунок 89 – Форма просмотра отчета типа ***Отчет о проверке***

2) В заголовке форм просмотра отчетов типа ***Отчет о проверке на наличие уязвимостей*** (рис. 90) дополнительно отображаются результаты выполнения проверок на наличие уязвимостей***.*** Во вкладке ***Отчет*** пользователь может выполнить фильтрацию списка уязвимостей по уровням критичности и состоянию (*Активные*, *Скрытые*), осуществить переход на сайт с подробным описанием выявленной уязвимости. Для перехода доступны следующие сайты (при наличии на них описания выявленной уязвимости):

- ФСТЭК России (bdu.fstec.ru);
- официальный сайт базы уязвимостей «Common Vulnerabilities and Exposures» (cve.mitre.org);
- производитель оборудования.

Также во вкладке ***Отчет*** пользователь может скрыть уязвимости на устройствах (подробнее см. пункт 2.9.1.4 «Скрытие уязвимостей»).

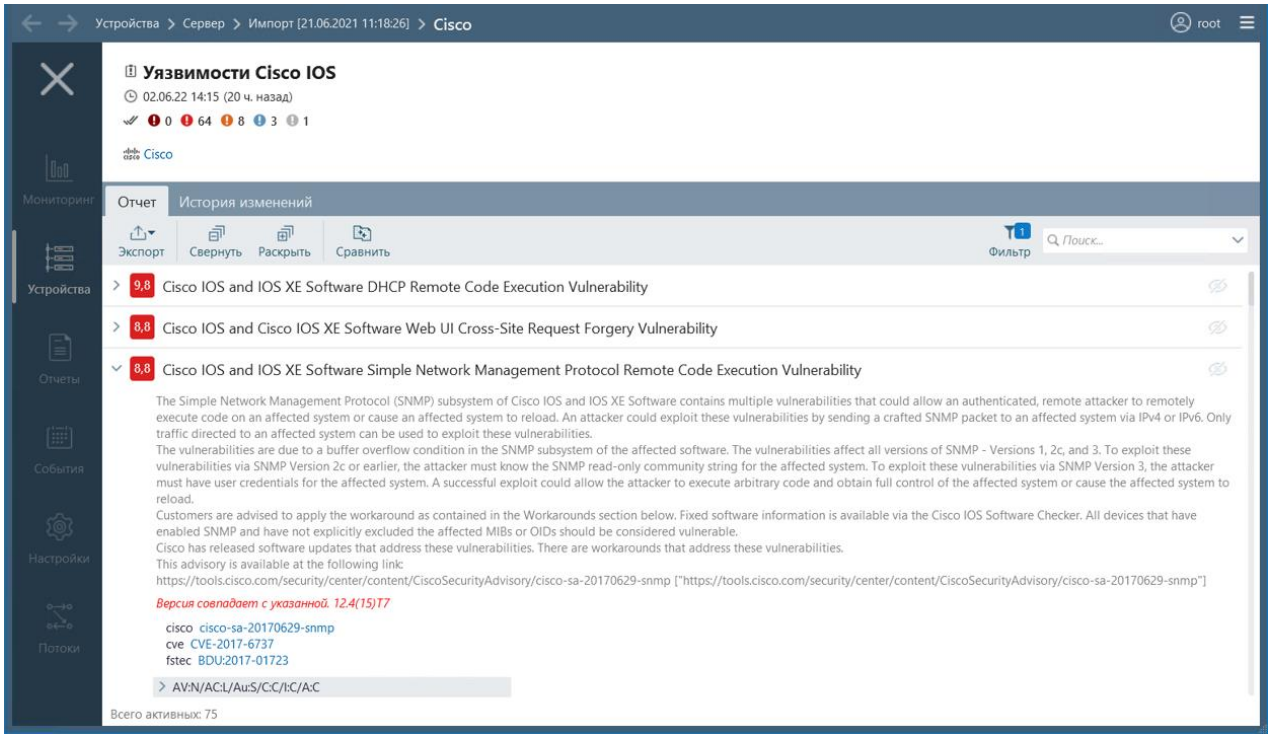


Рисунок 90 – Форма просмотра отчета типа ***Отчет о проверке на наличие уязвимостей***. Вкладка ***Отчет***

Примечание – Используемые в ПК графические обозначения уровня критичности уязвимости:

- «» – *Критический*;
- «» – *Высокий*;
- «» – *Средний*;
- «» – *Низкий*;
- «» – *Скрытые уязвимости*.

Во вкладке ***История изменений*** (рис. 91) отчета пользователь может просмотреть списки новых выявленных и измененных уязвимостей. Уязвимости сгруппированы по датам обновления БДУ комплекса и категориям:

- *Найдено* – обнаруженные после обновления БДУ;
- *Исправленные/удаленные* – пропавшие из списка после обновления БДУ;
- *Измененные* – были изменены какие-либо поля после обновления БДУ:
- *Скрытые* – скрыты пользователем средствами сервера ПК.

В заголовке каждой группы отображается дата и время изменения, количественные показатели изменения уязвимостей для каждого типа уязвимостей в формате «<графическое обозначение типа уязвимости> +/- <количество>».

Для скрытых уязвимостей отображаются логин пользователя, скрывшего уязвимость, дата скрытия и введенный пользователем комментарий.

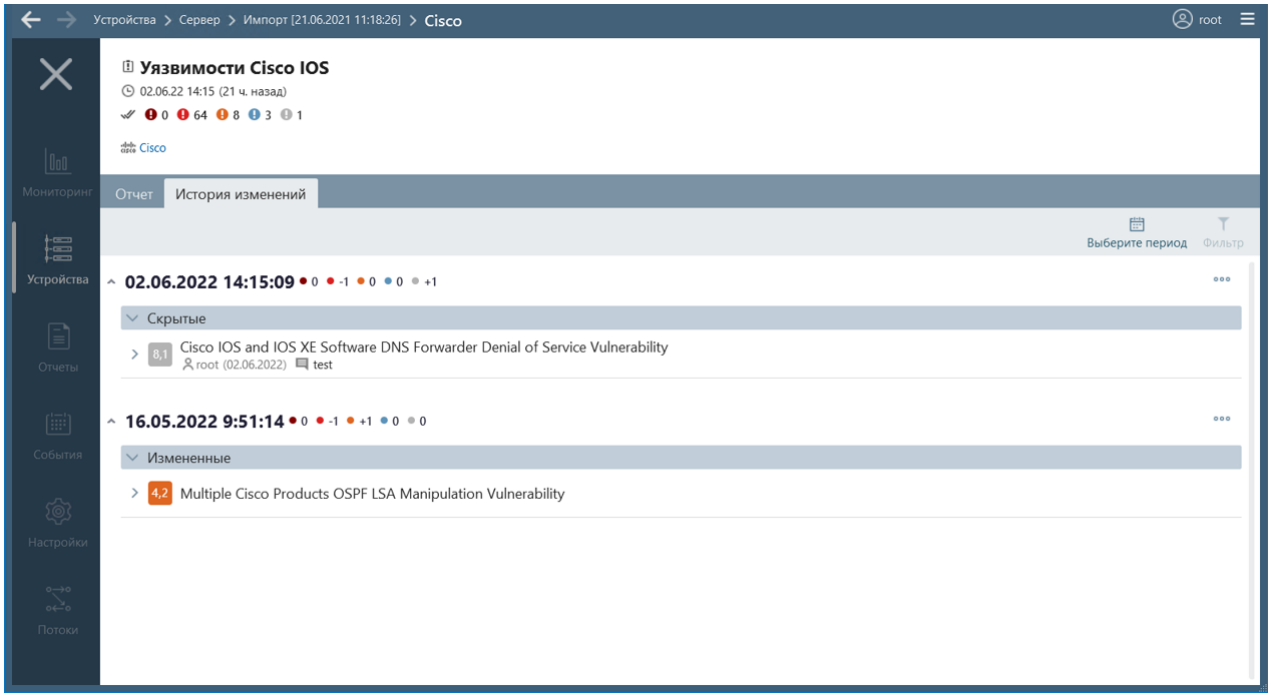


Рисунок 91 – Форма просмотра отчета типа ***Отчет о проверке на наличие уязвимостей***. Вкладка ***История изменений***

3) В заголовке форм просмотра отчетов типа ***Оптимизация правил*** (рис. 92) дополнительно отображается количество теневых, избыточных, а также неиспользуемых и нулевых правил, если устройством поддерживается подсчет срабатываний правил (подробнее о типах правил см. п. 1.1.1 «Обработка отчетов»).

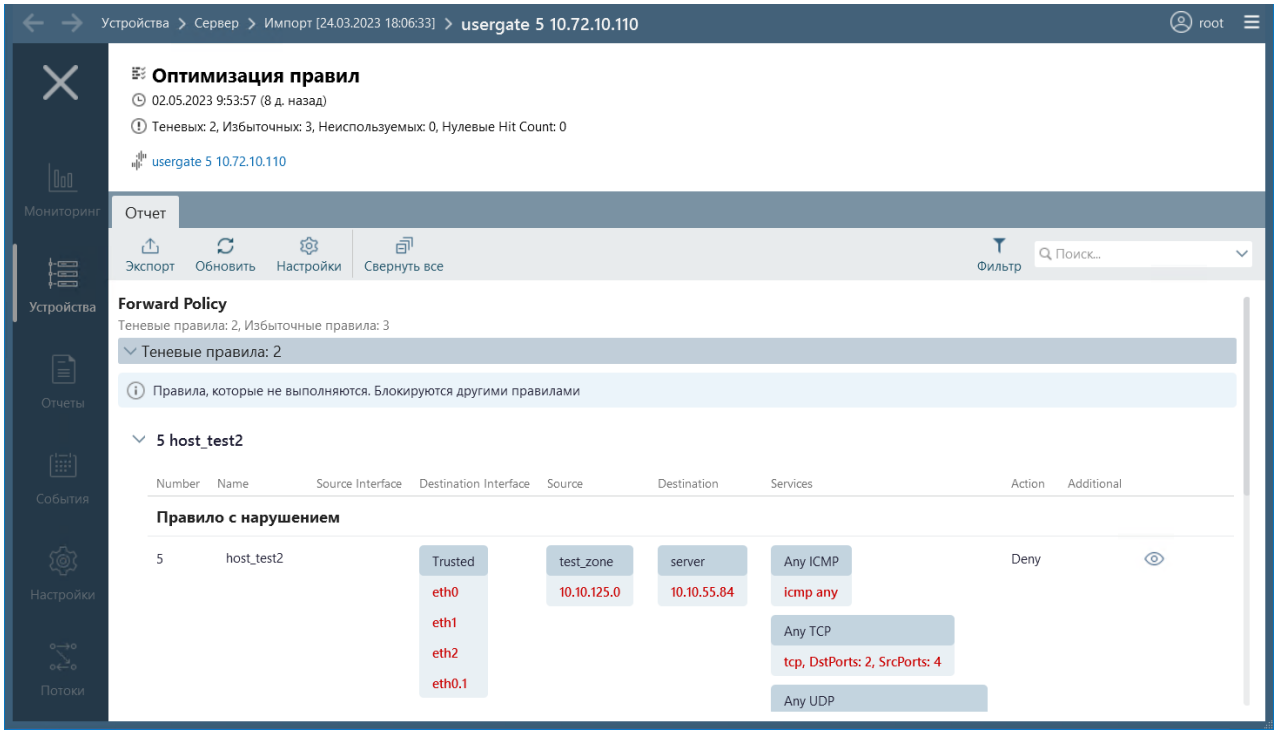


Рисунок 92 – Форма просмотра отчета типа ***Оптимизация правил***

Во вкладке ***Отчет*** пользователь может выполнить фильтрацию данных отчета по наборам правил (по кнопке ***Фильтр*** (

)), а также перейти по нажатию в строке правила кнопки ***Просмотр*** () из ***Отчета по оптимизации*** в форму просмотра ***Отчета по ACL*** устройства с позиционированием на соответствующем правиле.

4) В форме просмотра отчетов типа ***Правила межсетевых экранов*** пользователь может во вкладке ***Отчет*** выполнить фильтрацию данных отчета по наборам правил (по кнопке ***Фильтр*** (

)), а также просмотреть для каждого правила расписание его работы (если оно задано) в столбце ***Additional***, количество его срабатываний в столбце ***HitCount*** (столбец отображается в отчете только, если устройством поддерживается подсчет срабатываний правил). В отчетах для некоторых типов устройств под заголовком политики (например, для Check Point и Fortinet) или правила (например, для Cisco ASA), если в него внесены изменения, могут отображаться данные менявшего ACL пользователя и время изменения (данные берутся из последнего syslog, примененного к политике).

5) В форме просмотра отчетов типа ***Правила NAT*** пользователь может во вкладке ***Отчет*** просмотреть основную таблицу NAT (таблица без заголовка) и дополнительные таблицы с заголовками. В основной таблице реализованы ссылки на дополнительные таблицы в формате «GOTO <имя дополнительной таблицы>». При выборе ссылки выполняется позиционирование на заголовке соответствующей таблицы.

6) В форме просмотра отчетов, созданных пользователями на основе стандартов безопасности МЭ, пользователь может во вкладке ***Отчет*** выгрузить данные отчета в файл формата HTML, просмотреть для каждого требования стандарта безопасности соответствующего типу устройства:

- его статус (успешно выполнен или с нарушением);
- обнаруженные по требованию правила МЭ, при этом для требований с нарушением прараметры, по которым найдено правило, будут отображены красным цветом шрифта, для успешных требований – зеленым.

Аналогично отчетам типа ***Оптимизация правил*** пользователь может перейти по нажатию в строке правила кнопки ***Просмотр*** () в форму просмотра ***Отчета по ACL*** устройства с позиционированием на соответствующем правиле

Примечание – При просмотре отчетов по проверкам безопасности МЭ, стандартам безопасности МЭ и оптимизации МЭ пользователям доступно выделение и копирование текста в таблицах отчетов, а также копирование значений с использованием контекстного меню.

2.9.1.4. Скрытие уязвимостей

В форме просмотра отчетов типа ***Отчет о проверке на наличие уязвимостей*** (см. рис. 90) пользователь с полными правами на устройстве может во вкладке ***Отчет*** скрыть уязвимости на устройстве.

Для скрытия уязвимости необходимо выполнить следующие действия:

1) Нажать в строке скрываемой уязвимости кнопку ***Скрыть*** ( ).
2) Ввести в открывшемся окне (рис. 93) комментарий.
3) Нажать кнопку ***Скрыть***.

Примечание – Заполнение поля **Комментарий** обязательно.

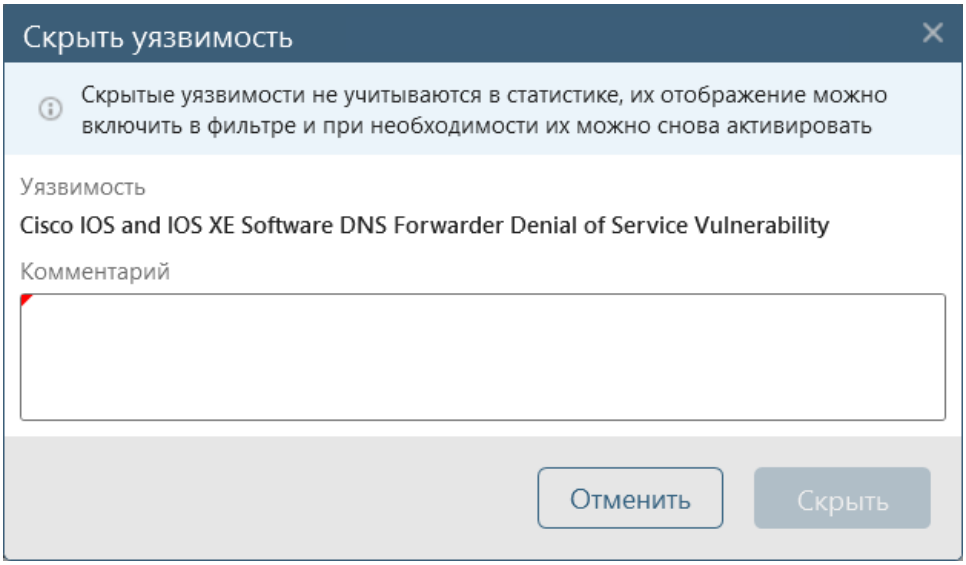


Рисунок 93 – Окно **Скрыть уязвимость**

Скрытые уязвимости по умолчанию не учитываются в статистике и не отображаются в отчетах. Для просмотра скрытых уязвимостей в отчете необходимо выбрать в окне фильтрации списка уязвимостей вкладки ***Отчет*** состояние *Скрытые*.

Скрытые уязвимости доступны во вкладке ***Отчет*** (см п. 2.9.1.3 «Особенности просмотра отчетов») для активации по нажатию в строке уязвимости кнопки ***Активировать*** ( ). При активации окно для ввода комментария не открывается.

Примечание – Уязвимости могут быть также скрыты и активированы в отчетах по уязвимостям в разделе **Отчеты** (см. п. 2.12.1.2 «Ввод параметров отчета и просмотр отчета для типа шаблона *Уязвимости устройств*»).

2.9.2. Просмотр истории изменений конфигурации, проверок устройства

Для просмотра истории изменений конфигурации, проверок контролируемого устройства пользователю необходимо выполнить следующие действия:

- открыть последнюю загруженную версию отчета, для чего дважды щелкнуть левой кнопкой мыши на строке с требуемым отчетом во вкладке **Отчеты** выбранного устройства;
- в открывшейся форме просмотра отчета перейти на вкладку ***История изменений*** (рис. 94).

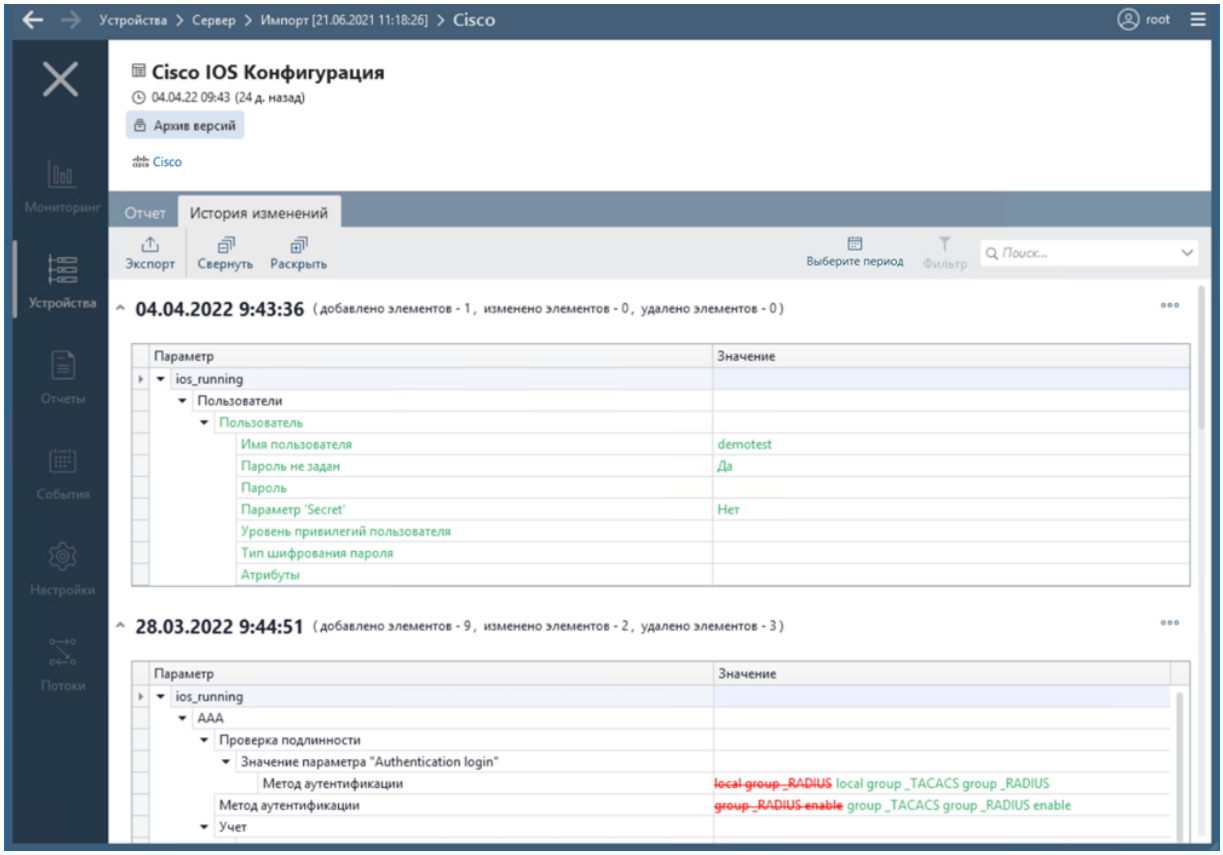


Рисунок 94 – Форма просмотра истории изменений конфигурации в структурированном отчете

При просмотре истории изменений отчета о проверках устройства (рис. 95) в строке каждой измененной проверки отображается индикатор-цветной квадрат и сообщение о выявленных изменениях: *Новое требование*, *Изменено*, *Удалено*. Индикатор отображает текущее(новое) состояние проверки:

- красного цвета – выявлено нарушение (проверка не пройдена);
- зеленого цвета – правило выполняется;
- серого цвета – правило удалено из проверки.

Яркость цвета индикатора зависит от состояния статуса проверки. Если статус менялся, то цвет яркий, если не менялся, то бледный (полупрозрачный).

Все неизмененные данные конфигураций, проверок отображаются без изменений черным цветом шрифта. Изменившиеся данные выделяются:

- красным цветом – старые значения;
- зеленым цветом – новые значения.

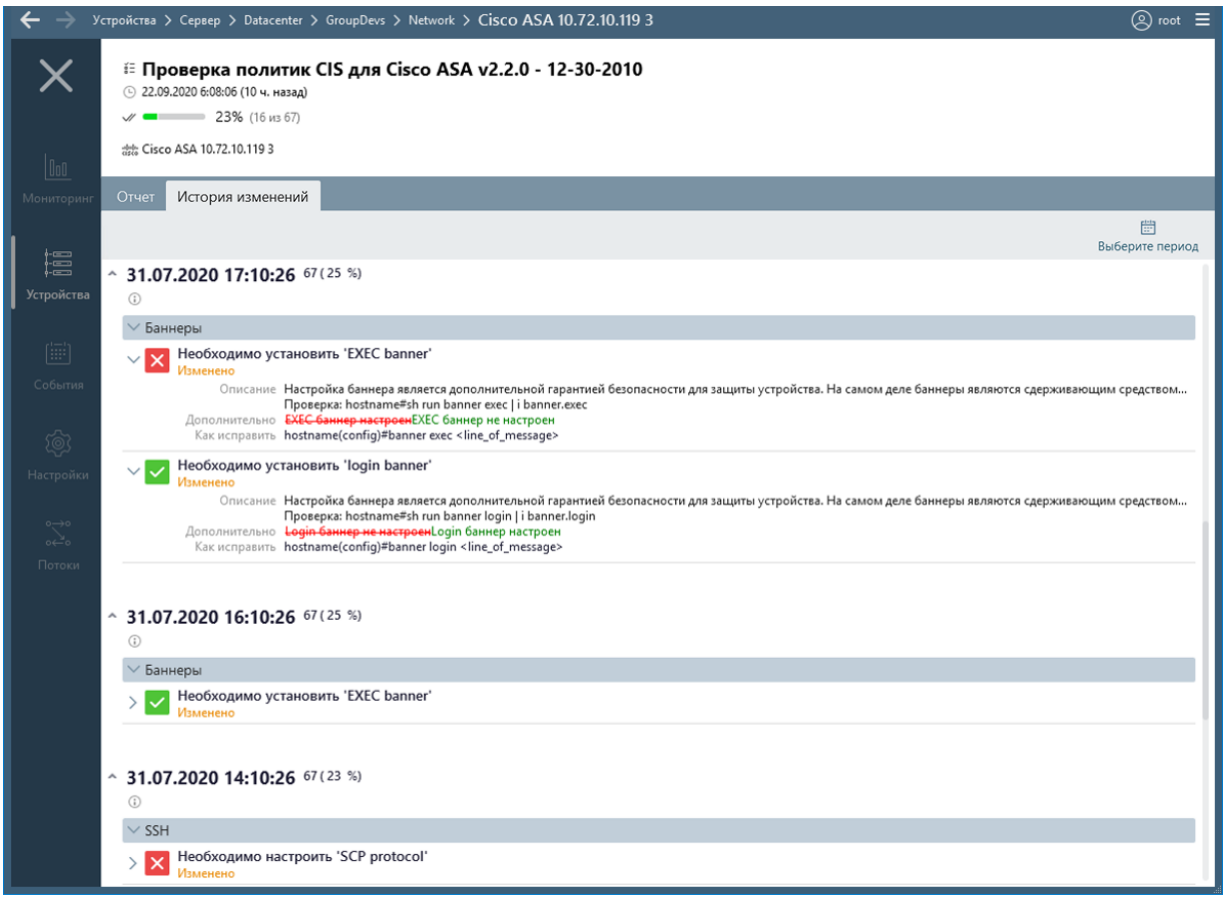


Рисунок 95 – Форма просмотра истории изменений проверок

2.9.3. Обновление (загрузка) отчета

Обновить отчет из вкладки ***Отчеты*** раздела **Устройства** пользователь может несколькими способами:

1) Нажать кнопку ***Обновить*** (***)*** в строке с именем обновляемого отчета (рис. 96).

2) Выделить требуемый отчет в списке и, вызвав контекстное меню, выбрать пункт ***Обновить отчет.***

3) Открыть необходимый отчет для просмотра, дважды щелкнув левой кнопкой «мыши» на строке с его именем, и в открывшейся форме просмотра отчета нажать кнопку ***Обновить*** (***)*** (см. примеры на рис. 85-95).

В результате любого из этих действий будет выполнена операция загрузки выбранного отчета, обновятся данные в таблице отчетов.

После загрузки отчета будет обновлен выбранный отчет, а также обновятся связанные с ним исходный отчет (загружаемый с устройства) и все другие производные отчеты (типа *Фильтр*) из этого исходного отчета.

Для обновления всех отчетов выбранного устройства, необходимо нажать кнопку ***Обновить все*** (***)*** в заголовке вкладки ***Отчеты***.

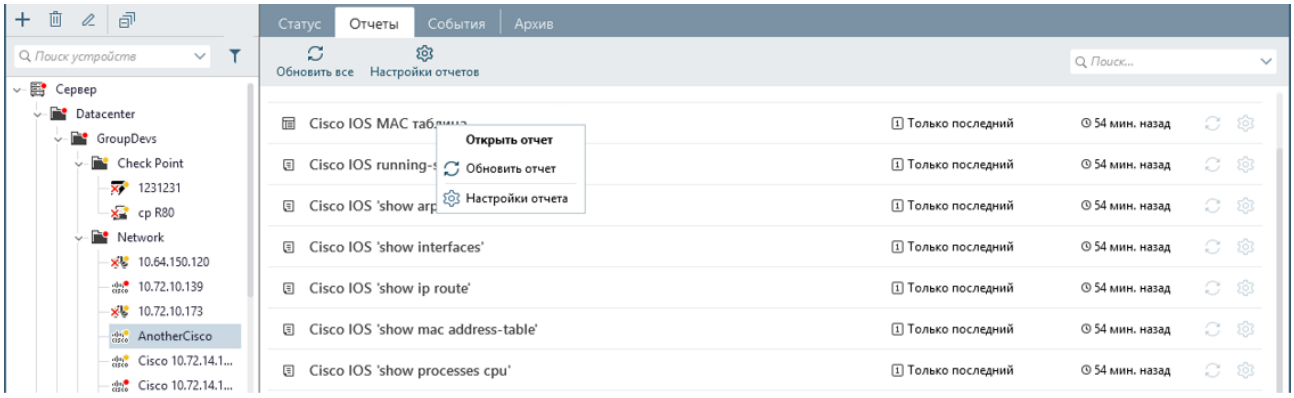


Рисунок 96 – Контекстное меню отчета

2.9.4. Установка эталона отчета

В качестве эталонной можно установить версию отчета, в свойствах которого установлен режим использования - ***Контроль изменений***. Первая загруженная с устройства версия такого отчета автоматически принимается за эталон. В дальнейшем пользователь может изменить эталонную версию отчета.

Есть несколько способов установки версии отчета в качестве эталонной:

а) ***из контекстного меню устройства***. В контекстном меню устройства в разделе **Устройства** выбрать пункт ***Принять изменения***. Все измененные версии загруженных с устройства отчетов будут установлены в качестве эталонных, а изменения конфигурационных файлов и списков устройства подтверждены;

б) ***из заголовка уведомления о фиксации события несоответствия отчета эталону.*** Для установки последней загруженной измененной версии отчета в качестве эталона пользователю необходимо выполнить следующие действия:

- в панели **Уведомления** вкладки ***Статус*** раздела **Устройства** выделить уведомление о несоответствии загруженного отчета его эталонной версии;
- при необходимости, просмотреть отчет с изменениями, перейдя по ссылке в уведомлении **<Имя_измененного_отчета>** – откроется форма просмотра изменений (рис. 97);
- вернуться обратно во вкладку ***Статус***, закрыв просматриваемый отчет, и нажать кнопку ***Принять новую версию за эталон*** (✓), которая расположена в правой части заголовка уведомления о нарушении целостности отчета.

Уведомление пропадет из списка уведомлений вкладки ***Статус*** выбранного устройства, изменение конфигурации устройства будет подтверждено, а последняя загруженная измененная версия отчета будет установлена в качестве эталонной.

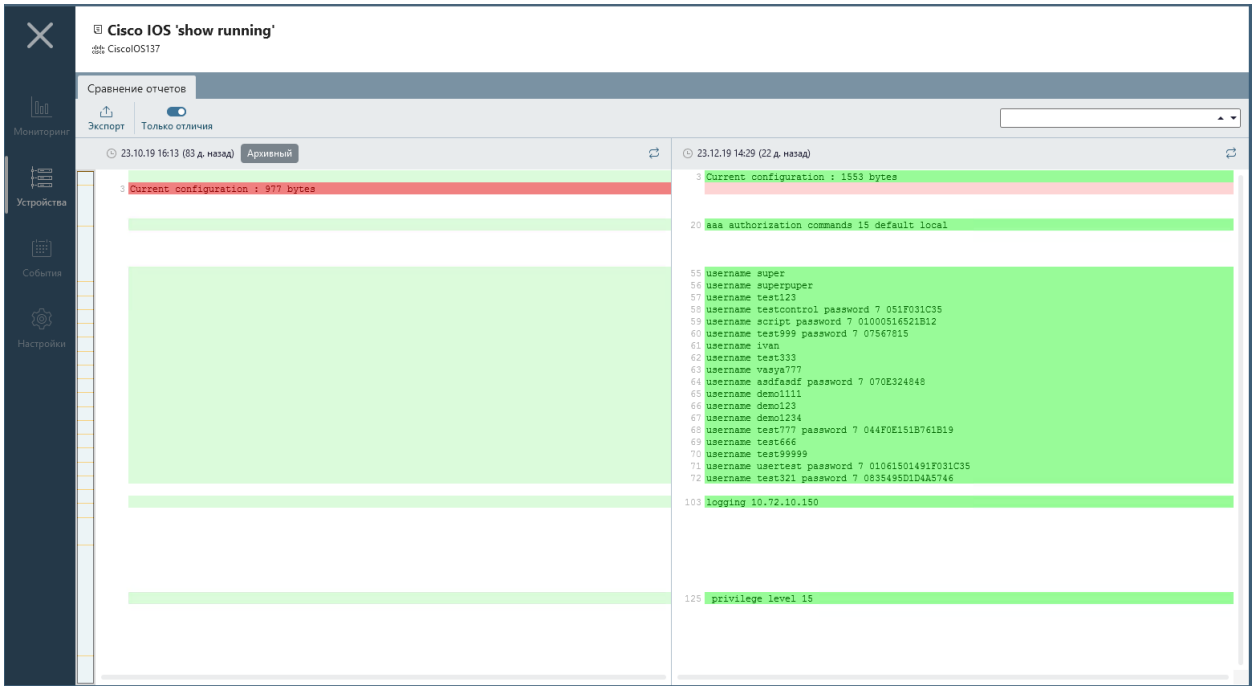


Рисунок 97 – Форма сравнения последней загруженной версии отчета с архивной

в) ***из формы просмотра нарушений в последней загруженной версии отчета.*** Для установки последней загруженной измененной версии отчета в качестве эталона пользователю необходимо выполнить следующие действия:

- во вкладке ***Отчеты*** раздела **Устройства** щелкнуть левой кнопкой «мыши» по ссылке ***Нарушение*** в поле **Состояние** измененного отчета;
- в открывшейся форме сравнения последней загруженной версии отчета с эталоном просмотреть список измененных параметров конфигурации контролируемого устройства и принять эти изменения, нажав кнопку **Принять текущую версию за эталон**.

Последняя загруженная версия отчета будет установлена в качестве эталонной, изменение конфигурации устройства будет подтверждено, а уведомление о нарушении пропадет из списка уведомлений вкладки ***Статус*** выбранного устройства.

2.9.5. Сохранение отчета в формате XML, TXT, HTML

Для сохранения структурированного отчета в файл формата XML, HTML пользователю необходимо выполнить следующие действия:

- открыть необходимый отчет для просмотра, дважды щелкнув левой кнопкой «мыши» на строке с его именем, в открывшейся форме просмотра отчета нажать кнопку ***Экспорт*** () и в открывшемся меню выбрать формат файла, в котором будет сохранен выбранный отчет: ***XML, HTML***;
- в открывшемся стандартном окне ОС Windows **Сохранить как** указать имя и каталог размещения файла, в который будет сохранен выбранный отчет и нажать кнопку ***Сохранить***.

В результате выбранный отчет будет сохранен в указанном файле. Отчет, сохраненный в формате HTML, откроется для просмотра в новом окне используемого по умолчанию web-браузера.

Для сохранения текстового отчета в файл формата TXT, а отчета о проверке в файл формата HTML, пользователю необходимо выполнить следующие действия:

- открыть необходимый отчет для просмотра, дважды щелкнув левой кнопкой «мыши» на строке с его именем, и в открывшейся форме просмотра отчета нажать кнопку ***Экспорт*** ( );
- в открывшемся стандартном окне ОС Windows **Сохранить как** указать имя и каталог размещения файла, в который будет сохранен выбранный отчет, и нажать кнопку ***Сохранить***.

В результате выбранный отчет будет сохранен в указанном файле. Отчет о проверке, сохраненный в формате HTML, откроется для просмотра в новом окне используемого по умолчанию web-браузера.

Примечание – В отчетах о проверках данные выгружаются с учетом заданной фильтрации (с учетом текущего положения переключателя ***Только нарушения***, при включении которого в отчете остаются только правила, которые не выполнены).

2.9.6. Сравнение отчета с эталонной версией

Для сравнения загруженной версии отчета с эталонной версией пользователю необходимо открыть отчет для просмотра, дважды щелкнув левой кнопкой «мыши» на строке с его наименованием, и в открывшейся форме просмотра отчета нажать кнопку ***Сравнить*** ( ). В открывшемся окне выбора версии отчета для сравнения дважды щелкнуть на строке версии отчета, отмеченного как эталон (рис. 98).

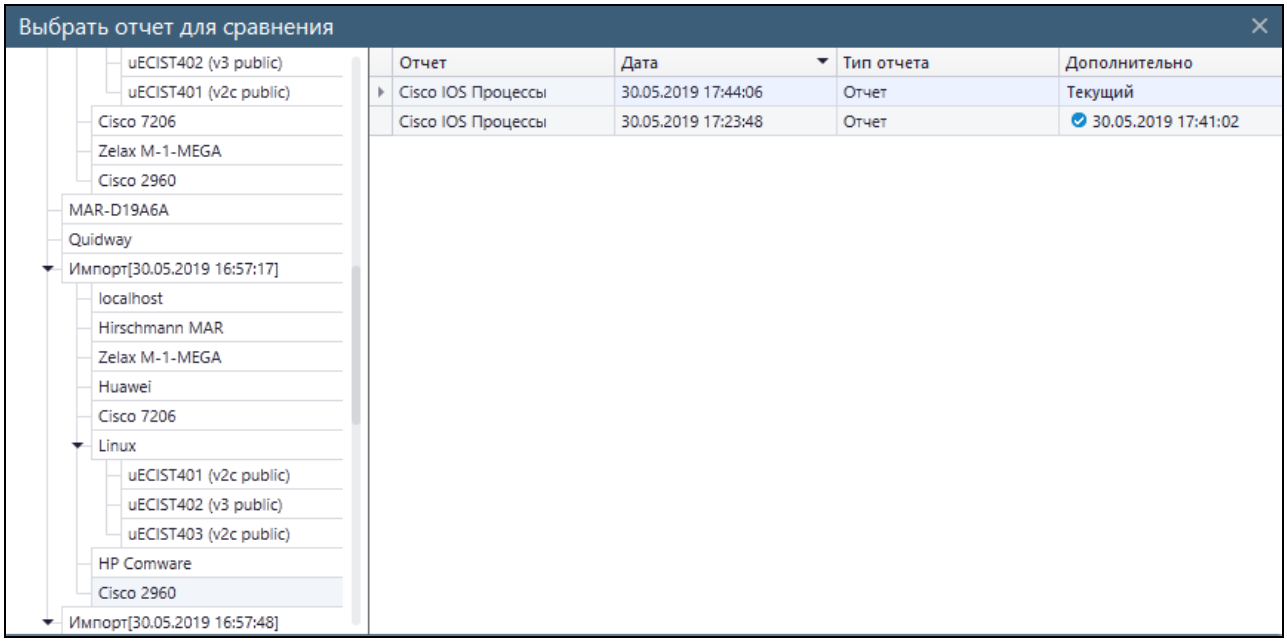


Рисунок 98 – Окно выбора версии отчета для сравнения

В результате откроется форма просмотра выполненного сравнения. Пример формы просмотра результата сравнения версий отчета для текстового отчета приведен на

рис. 97. Все данные проверяемого отчета, совпадающие с эталонным, отображаются без изменений черным цветом шрифта. Изменившиеся данные выделяются:

- красным цветом – значения эталонной версии;
- зеленым цветом – значения проверяемой версии.

В форме просмотра результата сравнения версий с эталоном для структурированного отчета (рис. 99) пользователь имеет возможность:

1) Выбрать режим отображения данных:
- полностью или только данные с изменениями, отметив параметр ***Только отличия***;
- в табличном виде или в виде дерева (с раскрытыми уровнями), отметив параметр ***В виде дерева***;

2) Сохранить результат сравнения выбранной версии отчета с эталоном в файл формата HTML, нажав кнопку ***Экспорт*** ( ).

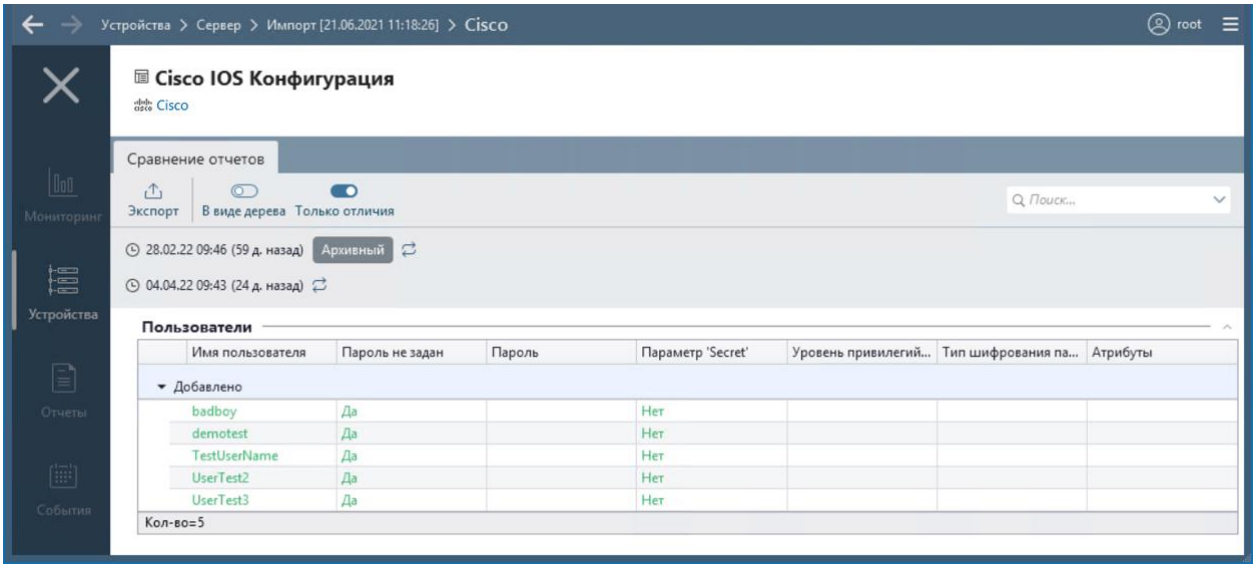


Рисунок 99 – Форма просмотра результата сравнения версий для структурированного отчета

В форме просмотра результата сравнения версий с эталоном для текстового отчета пользователь имеет возможность:

1) Выбрать режим отображения данных: полностью или только данные с изменениями, сняв или отметив, соответственно, параметр ***Только отличия***.

2) Просмотреть отличия в версиях отчета, нажимая кнопки ***Предыдущее***, ***Следующее***.

3) Сохранить результат сравнения выбранной версии отчета с эталоном в файл формата HTML, нажав кнопку ***Экспорт*** ( ).

Примечание – В форме просмотра результата сравнения версий отчета по уязвимостям изменения сгруппированы по категориям *Скрытые* и *Активированные*.

2.9.7. Фильтрация отчета и просмотр данных отфильтрованного отчета

Для определения параметров фильтрации отчета пользователю необходимо выполнить следующие действия:

1) Во вкладке ***Отчеты*** раздела **Устройства** открыть необходимый отчет для просмотра, дважды щелкнув левой кнопкой «мыши» на строке с его именем, и в открывшейся форме просмотра отчета нажать кнопку ***Фильтр*** ().

2) В открывшемся окне **Фильтр содержимого** настроить условия отбора данных выбранного отчета. Для структурированных отчетов в соответствии с пунктом 2.9.7.1 «Настройка условий фильтрации для структурированных отчетов» и для текстовых отчетов – с пунктом 2.9.7.2 «Настройка условий фильтрации для текстовых отчетов» и нажать кнопку ***Применить***.

В консоли откроется форма просмотра отчета в соответствии с указанными настройками фильтрации (рис. 100).

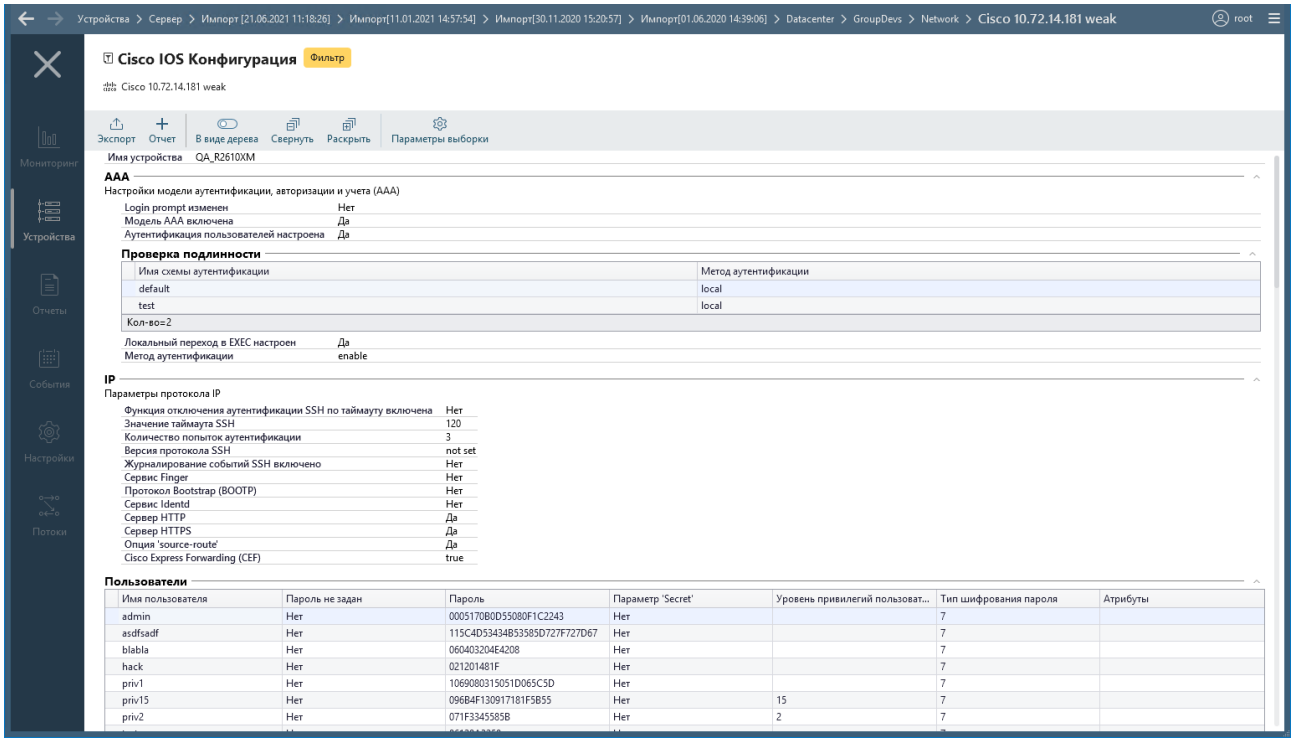


Рисунок 100 – Отображение структурированного отчета с заданными параметрами фильтра

В форме просмотра отчета пользователь может выполнить следующие действия:

- сохранить полученный отчет в файле формата HTML или TXT;
- сохранить полученный тип отчета, с учетом заданных значений фильтра (доступно только пользователям с правами *Управление* в категории *Настройки контроля*);
- настроить представление структурированного отчета: в табличном виде или в виде дерева (с раскрытыми или свернутыми уровнями дерева);
- изменить параметры формирования отчета, нажав кнопку ***Параметры выборки*** (), изменив настройки условия отбора данных в открывшемся окне **Фильтр содержимого** и нажав кнопку ***Применить***.

Для сохранения отфильтрованного отчета в файл формата HTML (для структурированных отчетов) или формата TXT (для текстовых отчетов) пользователю необходимо выполнить следующие действия:

- нажать в форме просмотра отчета кнопку ***Экспорт*** ();
- в открывшемся стандартном окне ОС Windows **Сохранить как** указать имя и каталог размещения файла, в который будет сохранен выбранный отчет, из раскрывающегося списка поля ***Тип файла*** выбрать необходимое расширение и нажать кнопку ***Сохранить***. Отчет будет сохранен в указанном файле и сразу же откроется для просмотра в окне программы просмотра отчетов, используемой по умолчанию: web-браузер (для структурированных отчетов) или текстовый редактор, например, **Блокнот** (для текстовых отчетов).

2.9.7.1. Настройка условий фильтрации для структурированных отчетов

Для настройки условий отбора данных для структурированных отчетов пользователю необходимо выполнить следующие действия:

1) В окне **Фильтр содержимого** (рис. 101) выбрать установкой/отменой установки флагов параметры, которые должны отображаться в отчете. Состав доступных для выбора параметров отчета зависит от его типа.

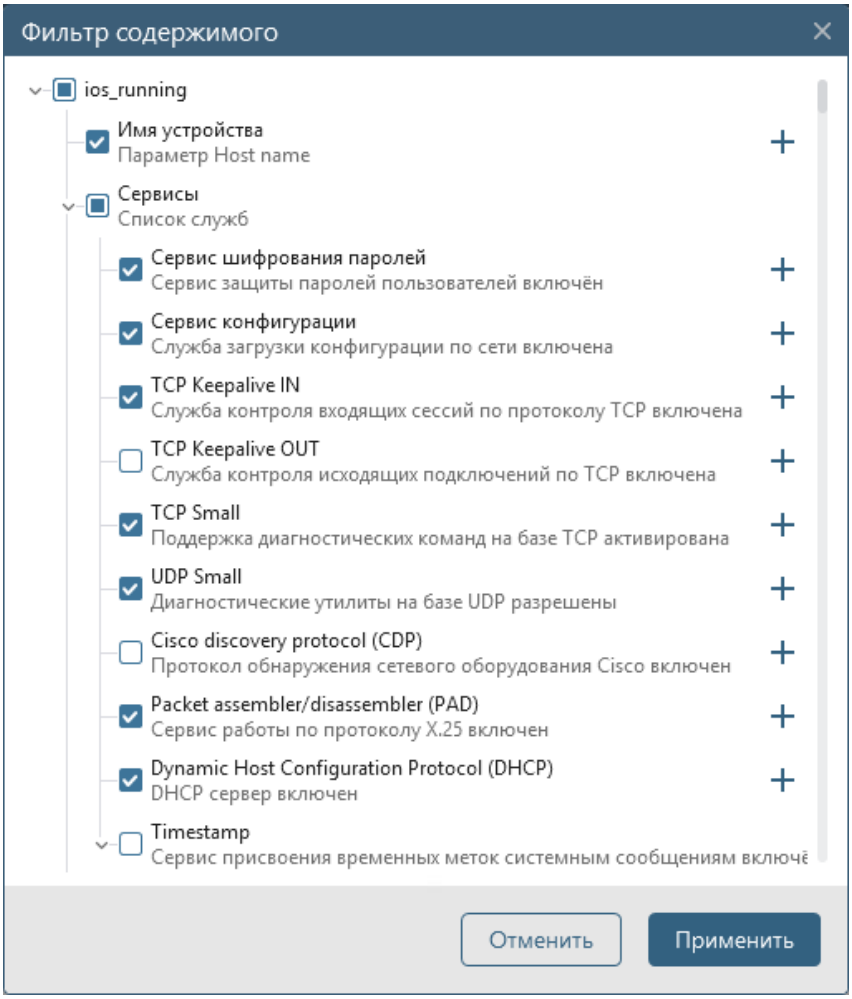


Рисунок 101 – Окно **Фильтр содержимого**

2) В строке параметра, для которого будет задаваться условие отбора, нажать кнопку ***Добавить условие*** (+).

3) Для логического параметра фильтра – выбрать значение *Да* или *Нет* (выполняется или не выполняется), для текстового параметра – выбрать из раскрывающегося списка типов условий требуемое условие (рис. 102), ввести в текстовое поле значение для проверки.

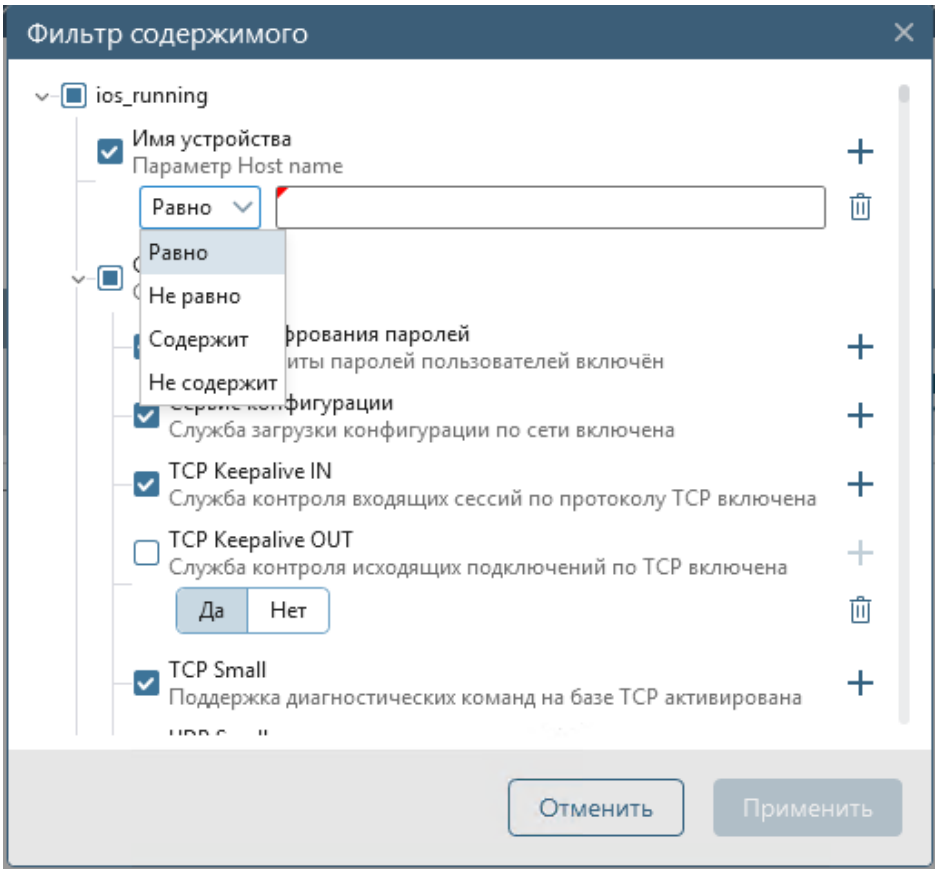


Рисунок 102 – Добавление условий для параметров

4) Добавить, при необходимости для текстового параметра другие условия отбора, повторив действия шага 3, и выбрав для заданных типов условий логические операции «*И*»/«*ИЛИ*» (рис. 103).

5) При необходимости добавить условия отбора для остальных выбранных параметров отчета, повторив действия шагов 2 – 4.

6) Нажать кнопку ***Применить***. В результате отчет в форме просмотра будет отображен в соответствии с введенными критериями отбора.

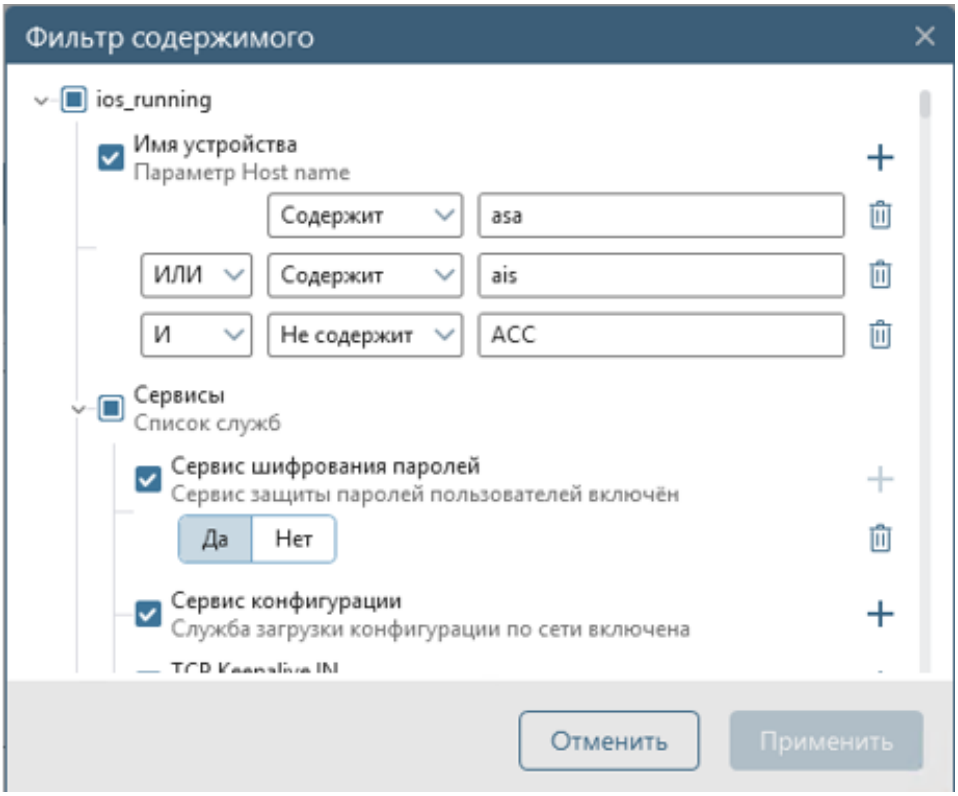


Рисунок 103 – Добавление нескольких условий для текстового параметра

2.9.7.2. Настройка условий фильтрации для текстовых отчетов

Для настройки условий отбора данных для текстовых отчетов пользователю необходимо выполнить следующие действия в окне **Фильтр содержимого** (рис. 104):

1) Выбрать тип фильтрации:
   - ***Простой поиск*** – для выборки строк данных в тексте отчета в соответствии с введенными критериями отбора;
   - ***Регулярные выражения (Поиск)*** – для выполнения поиска введенных данных в тексте отчета;
   - ***Регулярные выражения (Замена)*** – для выполнения поиска введенных данных с заменой на другое значение.

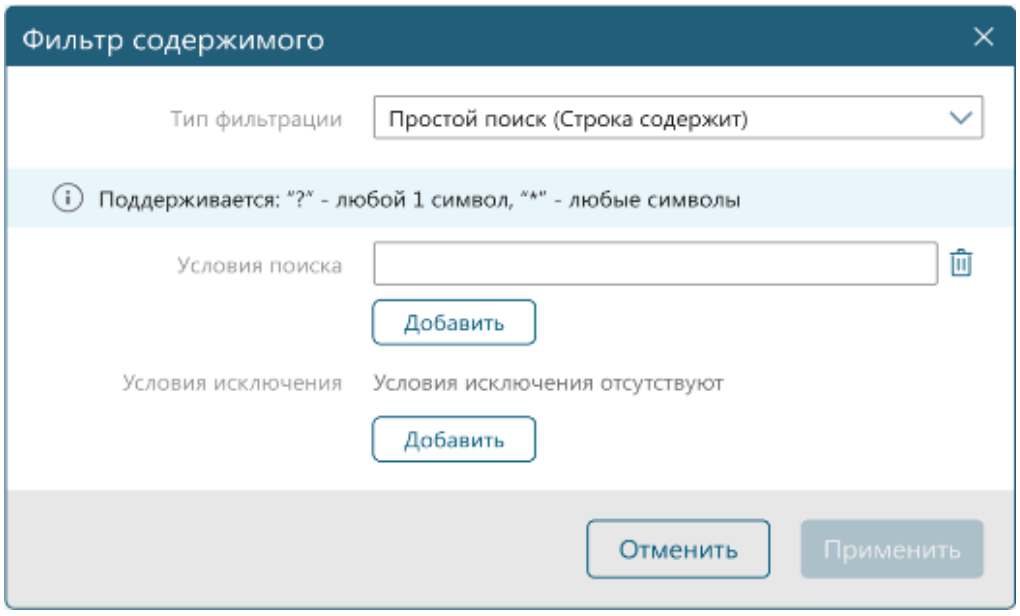
Примечание – Описание регулярных выражений стандарта PCRE, допустимых к применению в ПК «Efros Config Inspector» v.4, приведено в Приложении 1.

2) Ввести необходимые критерии отбора для фильтрации отчета:
   а) при выборе параметра ***Простой поиск*** (рис. 104, а) ввести ключевое значение в поле ***Условие поиска*** (для ввода нескольких значений – нажимать кнопку ***Добавить*** и вводить новые значения); для исключения строк из отчета, в которых содержатся определенные значения, нажать кнопку ***Добавить*** в области *Условия исключения* и ввести необходимое значение в открывшееся поле ввода (для ввода нескольких значений – нажимать кнопку ***Добавить*** и вводить новые значения). Для удаления ошибочно добавленных условия и/или исключений – нажать соответствующую им кнопку ***Удалить*** ().

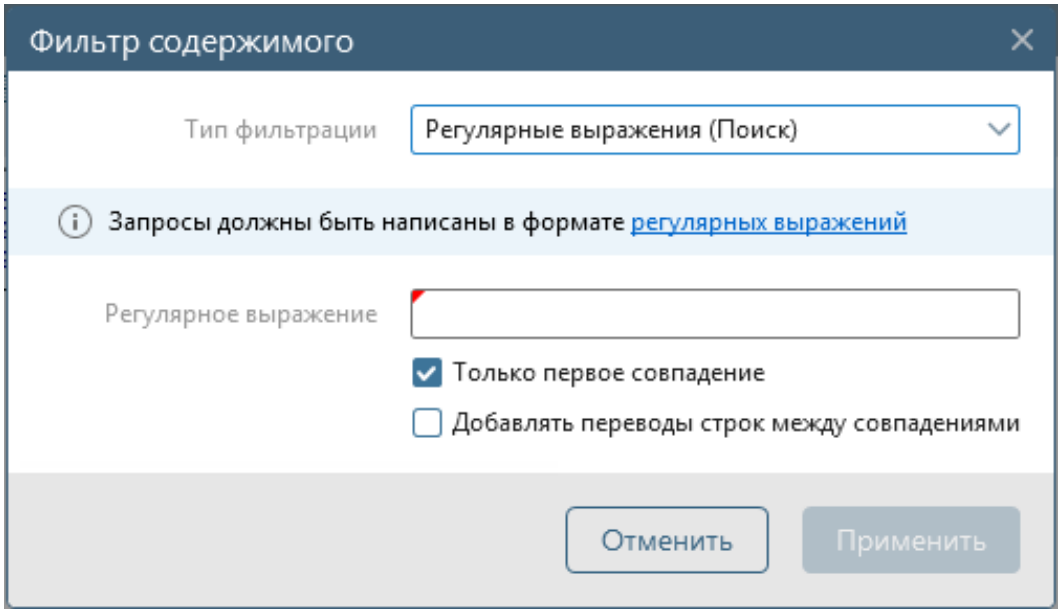
б) при выборе параметра ***Регулярные выражения (Поиск)*** (рис. 104, б) ввести в поле ***Регулярное выражение*** шаблон для поиска искомых данных в загружаемом отчете. Отметить требуемые параметры поиска:
   – ***только первое совпадение*** – для выполнения поиска данных до обнаружения первого совпадения;
   – ***добавлять переводы строк между совпадениями*** – для отображения каждого из найденных совпадений (при поиске всех совпадений) на новой строке отчета.

в) при выборе параметра ***Регулярные выражения (Замена)*** (рис. 104, в) ввести в поле ***Регулярное выражение*** шаблон для поиска искомых данных в загружаемом отчете, а в поле ***Выражение замены*** – данные, которыми будут заменены искомые выражения. При необходимости отметить требуемые параметры поиска:
   – ***только совпадения*** – в форме просмотра отфильтрованного отчета в одну строку будут отображены только найденные и замененные выражения;
   – ***заменять только первое совпадение*** – в форме просмотра отфильтрованного отчета будет изменено только первое из найденных выражений.

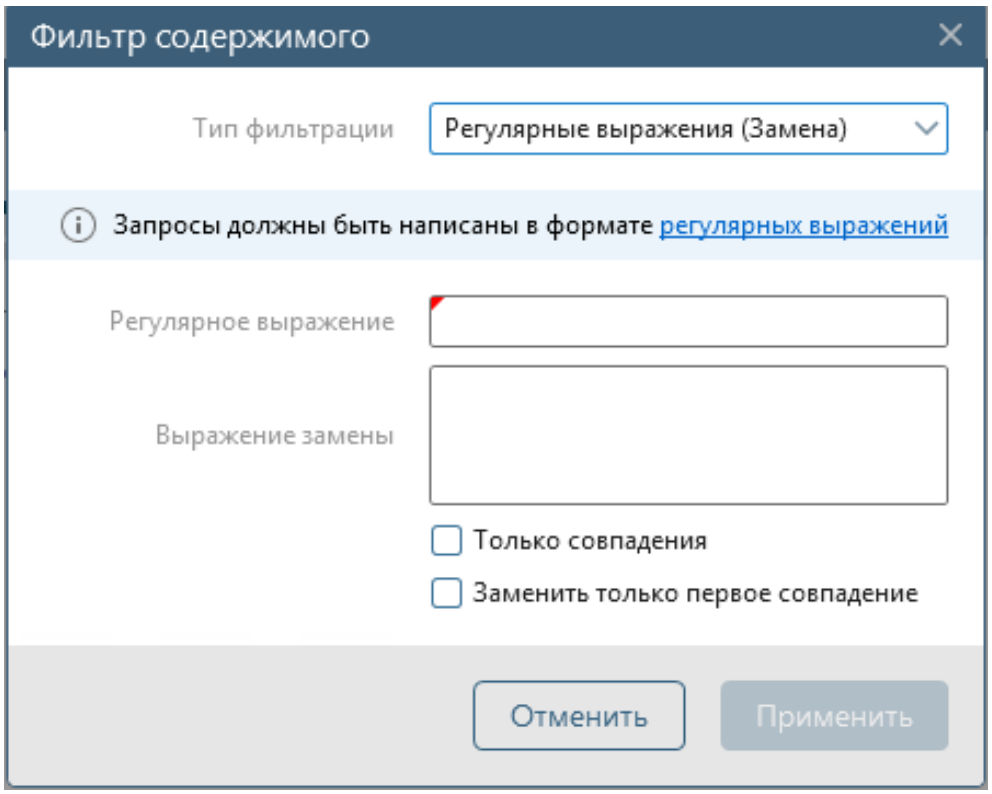
3) Нажать кнопку ***Применить***. В результате отчет в форме просмотра будет отображен в соответствии с введенными критериями отбора.



а)



б)



в)

Рисунок 104 – Фильтр содержимого текстового отчета

2.9.8. Просмотр правил игнорирования изменений параметров устройства

Правила игнорирования изменений конфигурации устройства настраиваются пользователями с правами *Управление* в категории *Настройки контроля*.

Добавленные для отчета правила учитываются при последующих загрузках этого типа отчета с любого из контролируемых на сервере ПК устройств: изменения параметров, указанных в правилах, игнорируются.

Для просмотра правил игнорирования изменений в версиях загруженных с устройств текстовых отчетов пользователю необходимо выполнить следующие действия:

1) В форме просмотра текстовых отчетов (рис. 105) нажать кнопку ***Исключения*** ( ).

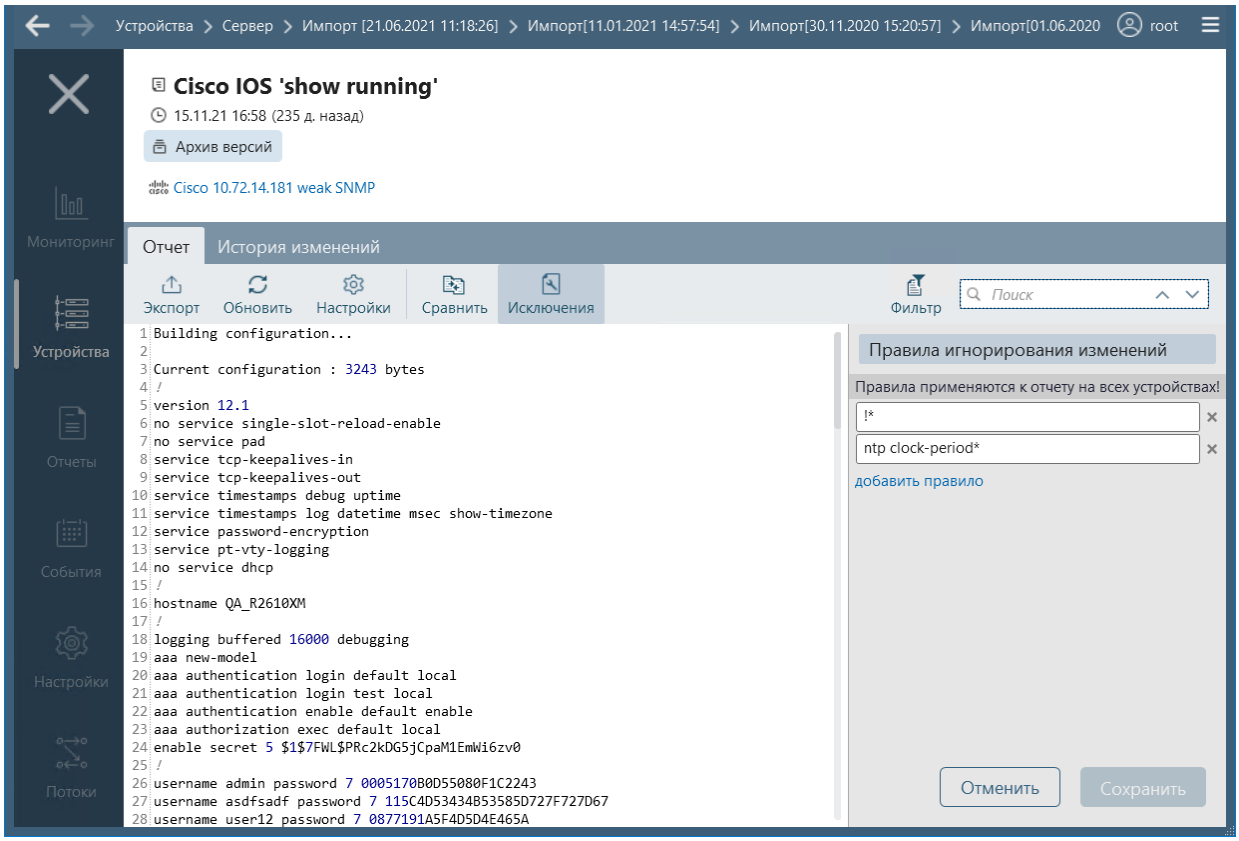


Рисунок 105 – Просмотр правил игнорирования изменений

2) В открывшейся с правой стороны формы области настройки правил игнорирования изменений ***Правила игнорирования изменений*** будут отображены имеющиеся правила.

3) Для выхода из режима просмотра – повторно нажать кнопку ***Исключения*** ( ).

При просмотре результатов сравнения версий отчетов с установленными правилами игнорирования изменений, указанные в правилах параметры отмечены затененным шрифтом, а изменения – выделены (рис. 106).

При сохранении результатов сравнения в файл формата HTML все изменения будут в нем отображены, а параметры, указанные в правилах игнорирования изменений, будут отмечены затененным шрифтом.

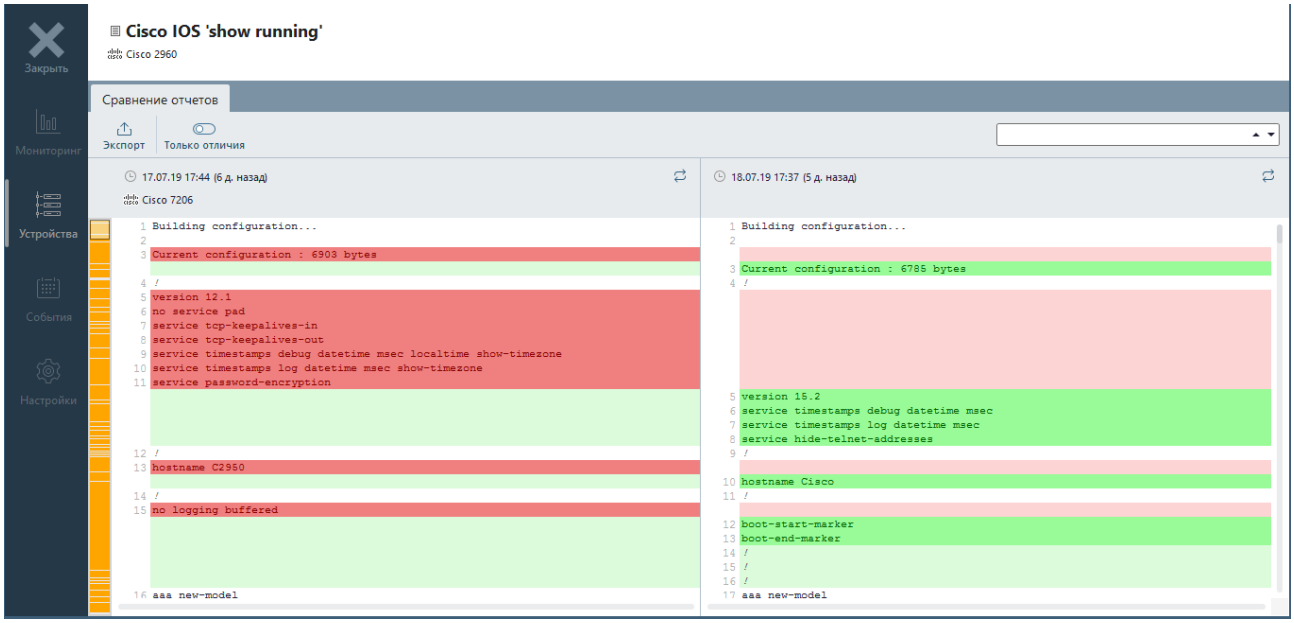


Рисунок 106 – Результат сравнения версий отчета с установленными правилами игнорирования изменений

2.10. Работа с архивными версиями отчетов

2.10.1. Просмотр архивной версии отчета

Для просмотра архивной версии отчета необходимо во вкладке ***Архив*** раздела **Устройства** дважды щелкнуть на строке с требуемой версией отчета. На рис. 107 приведен пример просмотра ***структурированного отчета.***

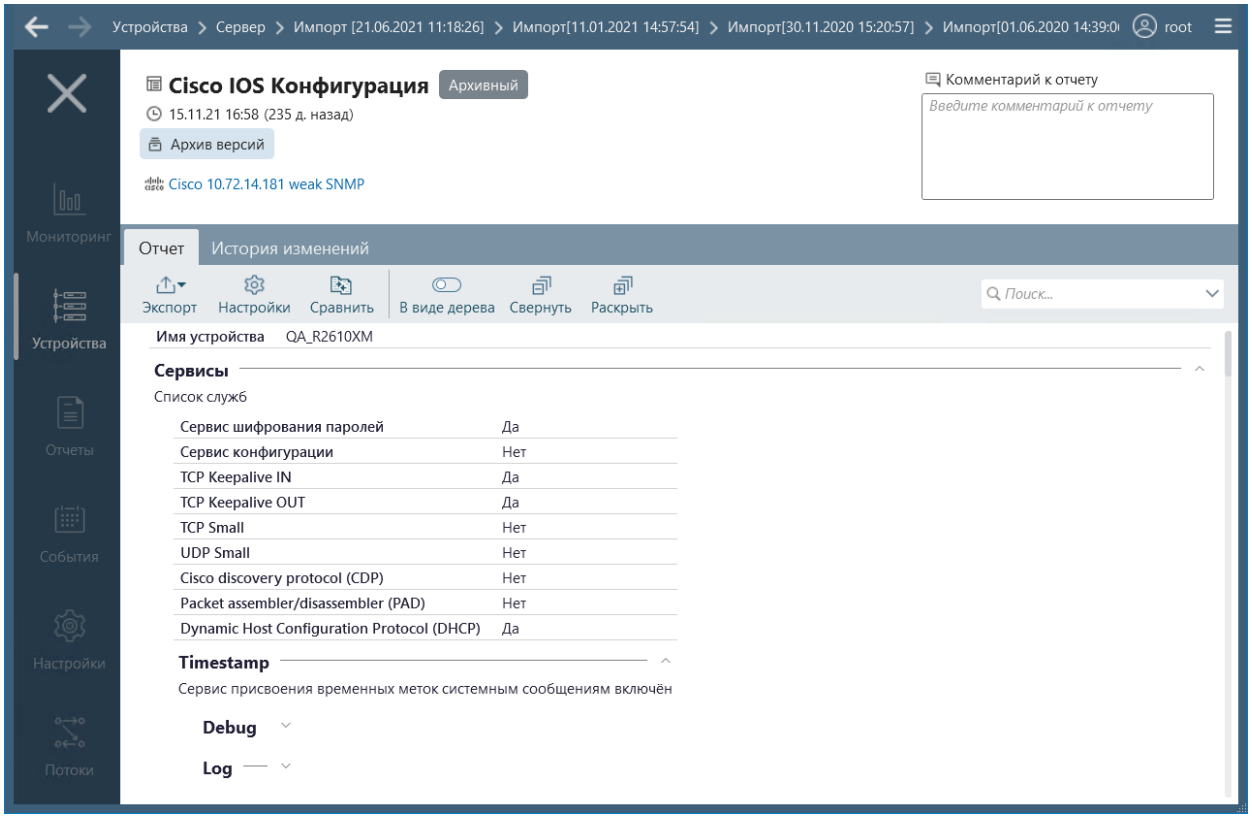


Рисунок 107 – Форма просмотра архивной версии структурированного отчета

В открывшейся форме просмотра отчета пользователь может выполнить следующие действия:

- просмотреть карточку устройства (рис. 108), нажав на ссылку-наименование устройства, в карточке пользователь имеет возможность выделить и скопировать данные устройства: имя устройства, адрес, описание (при его наличии в карточке), модель, версию;
- выполнить поиск в содержимом отчета, введя ключевой слово в соответствующее поле ввода;
- сохранить просматриваемую версию отчета в файл формата TXT (для текстовых отчетов), XML или HTML (для структурированных отчетов);
- настроить использование отчета для устройства (выбор из значений: *Контроль изменений, Архив версий, Только последний, Запрещено* или *Наследовать* (XXXX), где XXXX – настройки базового отчета);
- сравнить просматриваемую версию отчета с другой сохраненной в архиве версией этого отчета;
- настроить представление отчета: в табличном виде или в виде дерева (с раскрытыми или свернутыми уровнями дерева) (для структурированных отчетов);
- просмотреть историю изменений конфигурации устройства, зафиксированную в загруженных версиях отчетов;
- ввести комментарий к отчету.

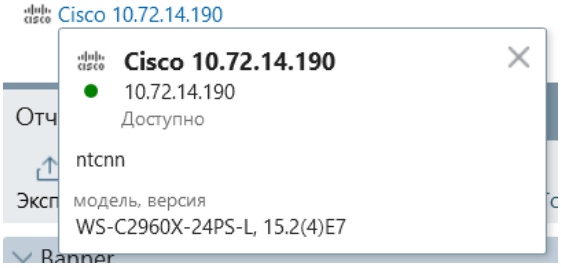


Рисунок 108 – Карточка устройства в форма просмотра архивной версии отчета

2.10.2. Просмотр истории изменений конфигурации устройства

Для просмотра истории изменений конфигурации контролируемого устройства пользователю необходимо выполнить следующие действия:

- во вкладке ***Архив*** раздела **Устройства** дважды щелкнуть на строке с требуемой версией отчета;
- в открывшейся форме просмотра отчета перейти на вкладку ***История изменений*** (рис. 109).

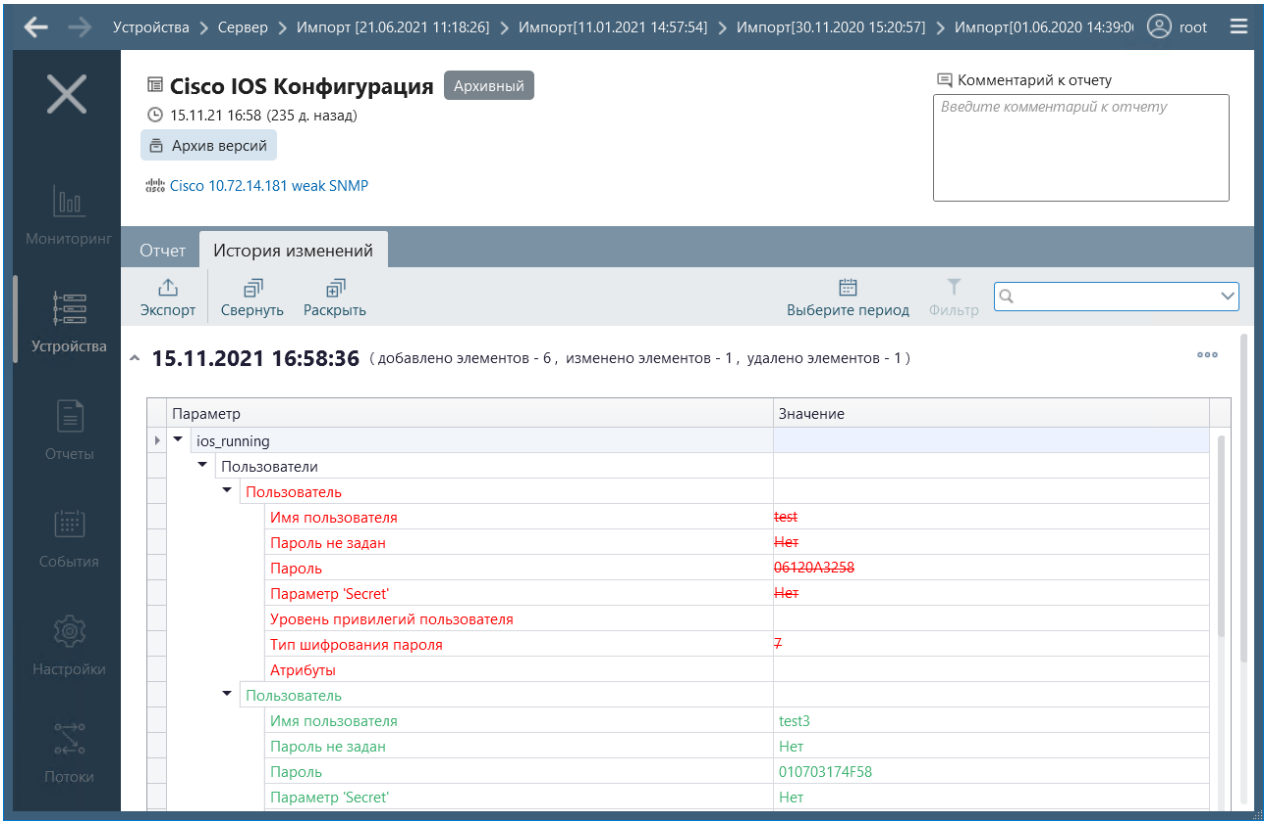


Рисунок 109 – Форма просмотра истории изменений структурированного отчета

2.10.2.1. Выборка архивных версий отчетов по типу и времени с использованием средств управления клиентской консоли

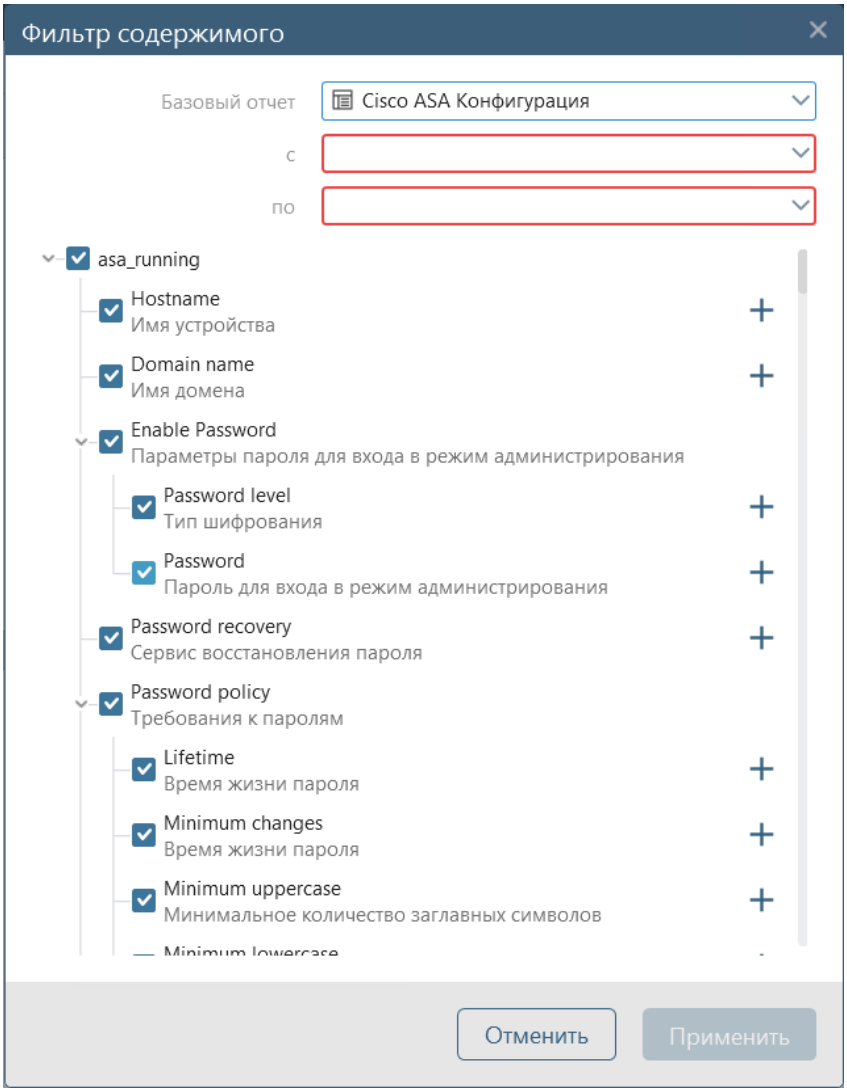
Для выборки архивных отчетов по типу и времени с использованием средств управления клиентской консоли пользователю необходимо выполнить следующие действия:

1) Для выбранного устройства во вкладке ***Архив*** раздела **Устройства** выделить требуемый отчет и нажать кнопку ***Выборка*** ( ).

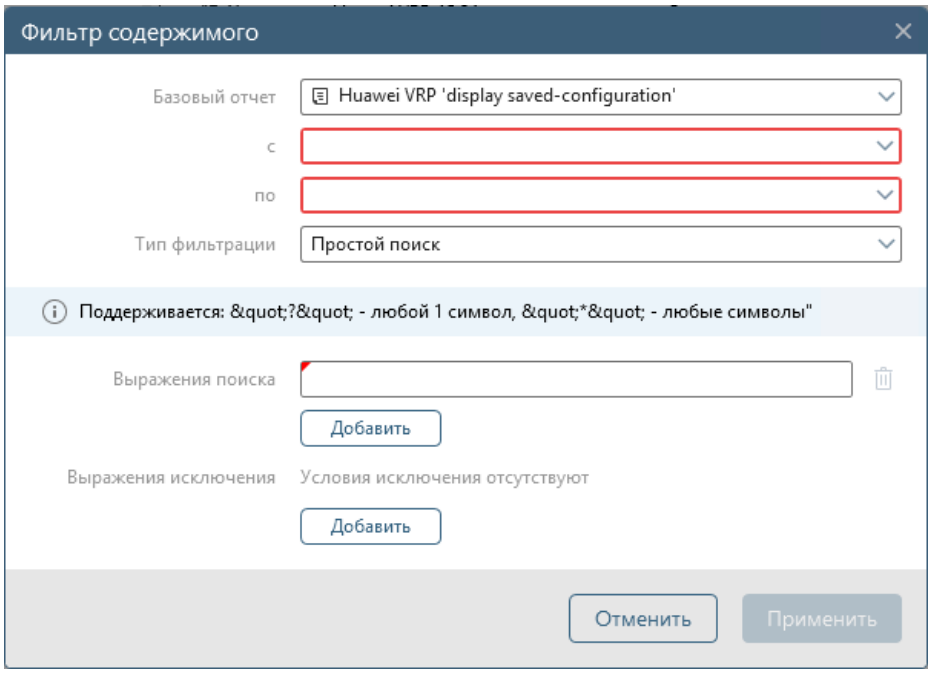
2) В открывшемся окне **Фильтр содержимого** (рис. 110, для структурированного отчета – а, для текстового отчета – б) указать параметры отбора: тип, интервал времени сохранения версий требуемого отчета (описание полей окна приведено в таблице 14).

Для выделенного во вкладке ***Архив*** отчета в окне **Фильтр содержимого** будет автоматически заполнено поле: ***Базовый отчет*** – имя выделенного отчета.

Если во вкладке ***Архив*** не выделен отчет, то в окне **Фильтр содержимого** будут отображаться только поля выбора типа отчета и интервала времени, поля будут не заполнены.



а)



б)

Рисунок 110 – Окно **Фильтр содержимого**

Таблица 14 – Описание полей окна **Фильтр содержимого**

Параметр	Описание/Назначение
Тип отчета	Выбор типа отчета. Для выбора доступны все типы отчетов, загружаемые и формируемые для выбранного устройства
С, по	Выбор дат и времени начала и окончания периода, за который должны быть отобраны архивные отчеты. Раскрывающиеся списки содержат все имеющиеся в таблице значения даты и времени сохранения в архиве версий выбранного типа отчета

3) В окне **Фильтр содержимого** задать условия отбора данных для структурированных отчетов в соответствии с пунктом 2.9.7.1 «Настройка условий фильтрации для структурированных отчетов», для текстовых отчетов – с пунктом 2.9.7.2 «Настройка условий фильтрации для текстовых отчетов» и нажать кнопку ***Применить***.

В результате откроется форма просмотра с данными загруженных версий выбранного типа отчета за указанный временной период с учетом установленных условий фильтра данных (рис. 111).

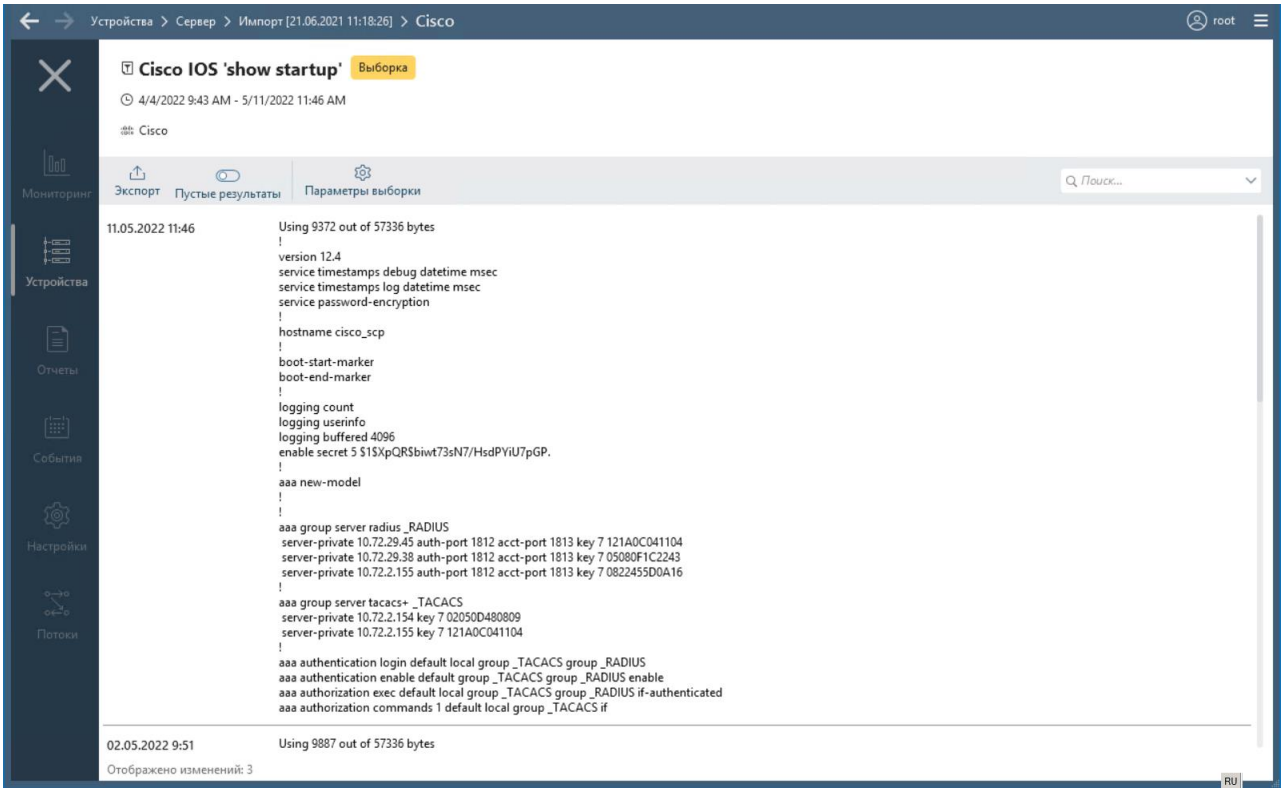


Рисунок 111 – Форма просмотра с данными загруженных версий выбранного типа отчета за указанный временной период с учетом установленных условий фильтра данных

В нижней части формы будет отображаться общее количество отображаемых в выборке версий отчетов. Количество отображаемых версий отчетов в выборке ограничено. Если версий более 100, то выводятся первые 100 записей в

соответствии с заданными настройками периода и фильтрации, в нижней части окна отображается сообщение *Показаны первые 100 записей*. Для просмотра требуемой версии отчета, не попавшей в число отображаемых, необходимо выбрать другой временной период и/или параметры фильтрации списка.

В форме просмотра пользователь может:

- по нажатию кнопки ***Экспорт*** () сохранить отчет в файл формата HTML;
- выбрав положение переключателя ***Пустые результаты*** () настроить представление отчета с пустыми результатами и без (по умолчанию пустые результаты не отображаются);
- по нажатию кнопки ***Параметры выборки*** () перейти в окно **Фильтр содержимого**, в котором – просмотреть заданные условия отбора данных, выбрать другой временной интервал (по нажатию кнопки ***Применить*** в форме просмотра отобразятся данные в соответствии с новым временным интервалом).

2.10.2.2. Сравнение просматриваемой версии отчета с другой версией архивного отчета

Для сравнения просматриваемой версии отчета с другой версией архивного отчета пользователю необходимо выполнить следующие действия:

- для выбранного устройства во вкладке ***Архив*** открыть необходимую версию отчета для просмотра, дважды щелкнув левой кнопкой «мыши» на строке с именем отчета, и в открывшейся форме просмотра отчета нажать кнопку ***Сравнить***;
- в открывшемся окне выбора версии отчета для сравнения, выделить устройство, с версией отчета которого требуется сравнить просматриваемую версию отчета, и в списке версий отчетов двойным щелчком левой кнопки «мыши» выбрать версию отчета для сравнения.

В результате откроется форма просмотра результата сравнения версий отчета. Возможные действия пользователя в формах просмотра результатов сравнения версий отчета для структурированного и текстового отчетов приведены в п. 2.9.6 «Сравнение отчета с эталонной версией».

2.10.2.3. Сравнение просматриваемой версии отчета с последней загруженной версией отчета

Для сравнения просматриваемой версии отчета с последней загруженной версией отчета пользователю необходимо:

- во вкладке ***Архив*** выбранного устройства открыть необходимую версию отчета для просмотра, дважды щелкнув левой кнопкой «мыши» на строке с именем отчета, и в открывшейся форме просмотра отчета нажать кнопку ***Сравнить*** ();
- в открывшемся окне выбора версии отчета для сравнения выделить устройство, с версией отчета которого требуется сравнить просматриваемую версию отчета, и в списке версий отчетов двойным

щелчком выбрать версию отчета, у которой в поле ***Дополнительно*** указано значение ***Текущий***.

В результате откроется форма просмотра результатов сравнения просматриваемой и последней загруженной версий отчета. Возможные действия пользователя в формах просмотра результатов сравнения версий отчета для структурированного и текстового отчетов приведены в п. 2.9.6 «Сравнение отчета с эталонной версией».

2.10.2.4. Сравнение просматриваемой версии отчета с эталонной версией

Для сравнения просматриваемой версии отчета с его эталонной версией пользователю необходимо:

- во вкладке ***Архив*** выбранного устройства открыть необходимую версию отчета для просмотра, дважды щелкнув левой кнопкой «мыши» на строке с именем отчета, и в открывшейся форме просмотра отчета нажать кнопку ***Сравнить*** ();
- в открывшемся окне выбора версии отчета для сравнения выделить устройство, с версией отчета которого требуется сравнить просматриваемую версию отчета и в списке версий отчетов двойным щелчком выбрать версию отчета, у которой в поле ***Дополнительно*** указано, что она является эталонной.

В результате откроется форма просмотра результатов сравнения просматриваемой и последней загруженной версий отчета. Возможные действия пользователя в формах просмотра результатов сравнения версий отчета для структурированного и текстового отчетов приведены в п. 2.9.6 «Сравнение отчета с эталонной версией».

2.10.2.5. Ввод комментария к архивной версии отчета

Ввести комментарий к архивной версии отчета пользователь может несколькими способами:

1) Из окна просмотра архивной версии отчета:

- для выбранного устройства во вкладке ***Архив*** открыть необходимую версию отчета для просмотра, дважды щелкнув левой кнопкой «мыши» на строке с именем отчета;
- в открывшемся окне просмотра версии ввести необходимый комментарий в поле ***Комментарий к отчету***.

2) При помощи контекстного меню:

- для выбранного устройства во вкладке ***Архив*** выделить необходимую версию отчета и вызвав его контекстное меню выбрать пункт ***Изменить комментарий***;
- в открывшемся окне **Комментарий к отчету** внести необходимые изменения в существующий комментарий или ввести новый комментарий к выбранной версии отчета;
- нажать кнопку ***Сохранить***.

2.11. Просмотр журнала событий устройств

Пользователь в окне клиентской консоли программного комплекса может просмотреть список всех событий, которые происходили с контролируемыми на сервере ПК устройствами, доступными пользователю. В разделе **События** содержится список 1000 последних зафиксированных событий для всех устройств**,** во вкладке ***События*** раздела **Устройства**. – список из 1000 последних событий, которые произошли на устройстве, выбранном в панели списка устройств.

2.11.1. Просмотр событий в разделе События

Раздел **События** (рис. 112) содержит панели:

- списка событий;
- ***Подробности*** – с данными выбранного в списке события;
- ***Фильтр*** – фильтрации списка событий по периоду, устройствам, типу события или по сообщению.

Панель списка событий содержит список последних 1000 событий, которые зафиксированы серверной частью комплекса на всех доступных пользователю устройствах, подключенных к серверу ПК. Для каждого события построчно отображаются:

- наименование устройства;
- дата и время произошедшего события;
- тип события;
- краткое описание произошедшего события.

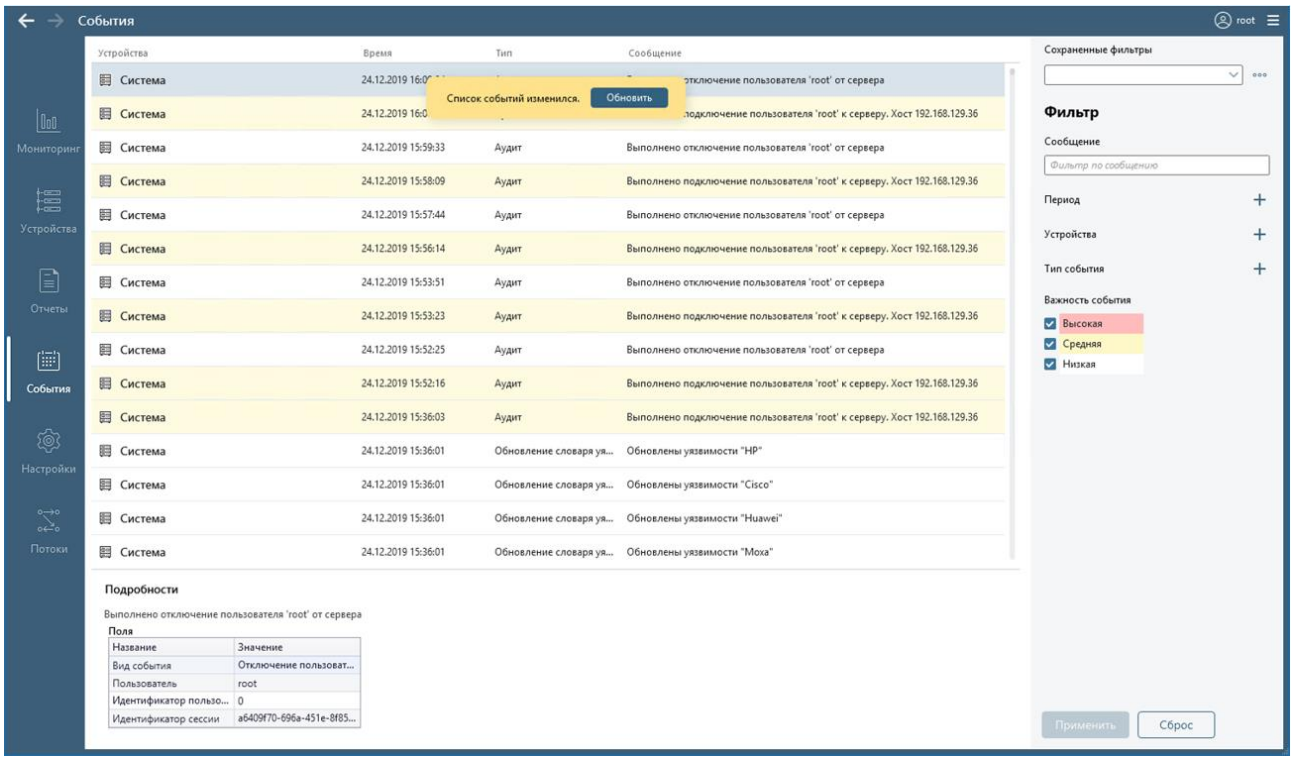


Рисунок 112 – Раздел **События**

В панели ***Подробности*** приводятся сведения о выбранном событии, которые не отображены в списке: тип отчета, название триггера, результат выполнения задания, время загрузки и т.д. Также в панели ***Подробности*** может содержаться ссылка:

- ***Подробнее*** – в случае, когда операция закончилась ошибкой (сообщение об ошибке). При выборе ссылки ***Подробнее*** открывается информационное окно, содержащее информацию из отчета.
- ***Показать изменения*** – в случае, когда зафиксировано отличие полученной с устройства версии отчета от сохраненной ранее (события типа *Изменение отчета*).

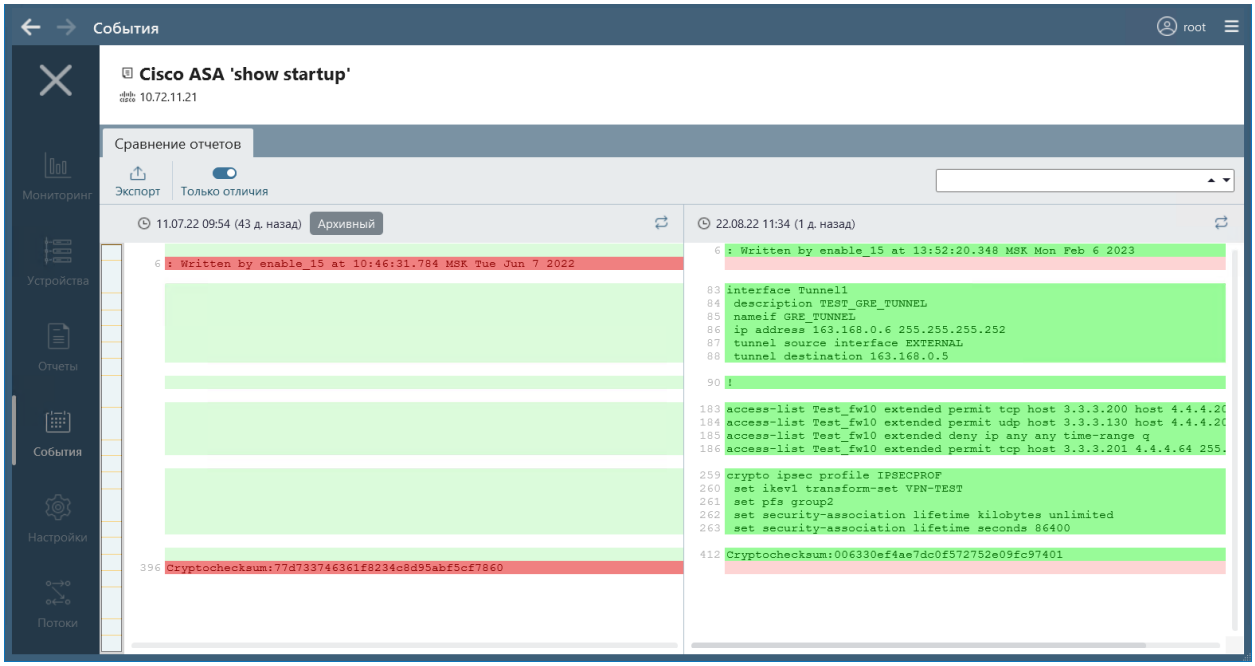
Пользователь имеет возможность копирования текста полей панели ***Подробности*** для последующей его обработки средствами другого ПО. Для копирования необходимо щелчком правой кнопки «мыши» раскрыть контекстное меню требуемой записи и выбрать пункт ***Копировать***.

В случае просмотра события типа *Изменение отчета* в панели ***Подробности*** появляется информация по внесенным в отчет изменениям и ссылка ***Показать изменения***. При выборе ссылки открывается форма сравнения версий отчетов, если загруженная версия отчета отличается от сохраненной в БД комплекса (рис. 113, а – для текстовых отчетов, б – для струтурированных отчетов и отчетов типа ***Проверка***).

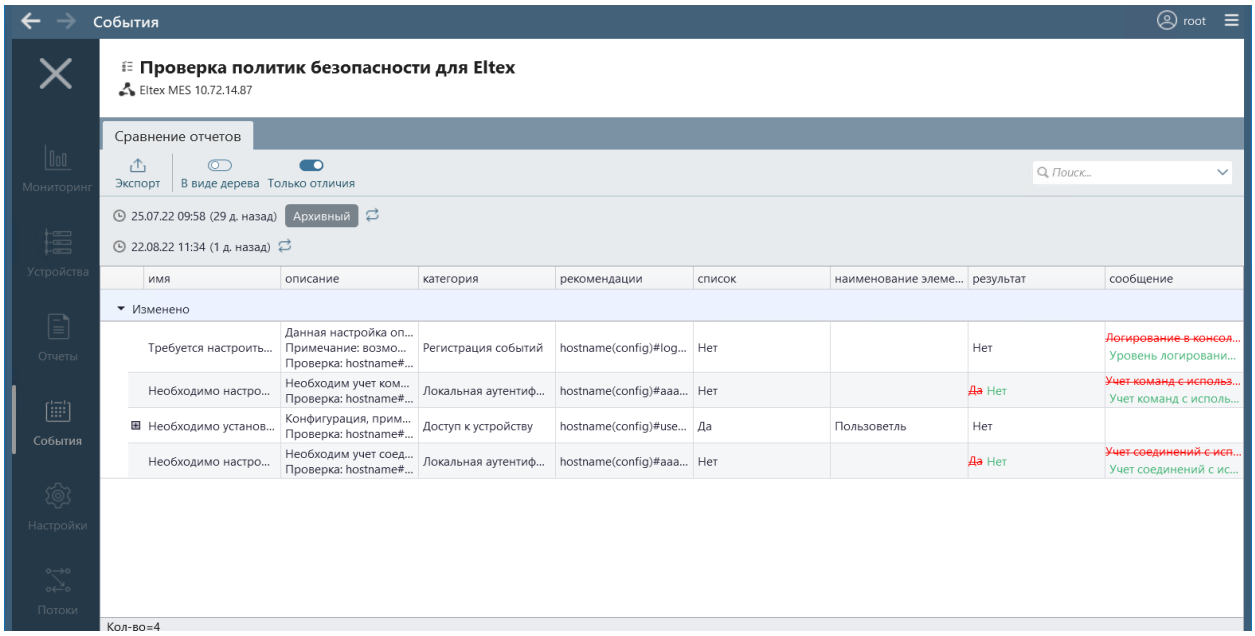
В форме сравнения версий отчетов пользователь имеет возможность:

1) Сохранить результат сравнения выбранной версии отчета с исходным в файл формата HTML, нажав кнопку ***Экспорт.***
2) Выбрать режим отображения данных:
   - в виде списка (выбран по умолчанию) или дерева (для структурированных отчетов), изменив положение переключателя ***В виде дерева***;
   - полностью или только данные с изменениями, изменив положение переключателя ***Только отличия***.
3) Выполнить поиск в содержимом отчетов, введя ключевое слово в соответствующее поле ввода. Для текстовых отчетов в поле дополнительно отображаются кнопки ***вверх*** (▲) и ***вниз*** (▼), предназначенные для перехода к предыдущим и следующим результатам поиска.
4) Выбрать другие отчеты для сравнения. Окно выбора отчета открывается по нажатию кнопки ***Выбрать отчет*** (🔁).

Группировка списка событий по умолчанию отсутствует. Список событий доступен пользователю для группировки, сортировки и фильтрации с использованием параметров, расположенных в панели обновления и фильтрации (см. п. 2.11.3 «Фильтрация событий с использованием панели фильтрации»).



а) для текстовых отчетов



б) для структурированных отчетов и отчетов типа ***Проверка***

Рисунок 113 – Форма **Сравнение отчетов**

Для обновления списка событий, с учетом заданных ранее пользователем правил фильтрации, необходимо нажать кнопку ***Обновить*** во всплывающем сообщении ***«Список событий изменился. Обновить»*** (см. рис. 112).

По нажатию кнопки ***Обновить*** выполняется загрузка списка событий с учетом заданных ранее пользователем правил фильтрации событий. При отсутствии установленных критериев фильтра, по нажатию кнопки ***Обновить*** происходит загрузка последних 1000 событий, произошедших на контролируемых устройствах и в комплексе.

2.11.2. Просмотр событий во вкладке События раздела Устройства

Вкладка ***События*** раздела **Устройства** (рис. 114) содержит панели:

- списка событий;
- ***Подробности*** – с данными выбранного в списке события;
- фильтрации списка событий.

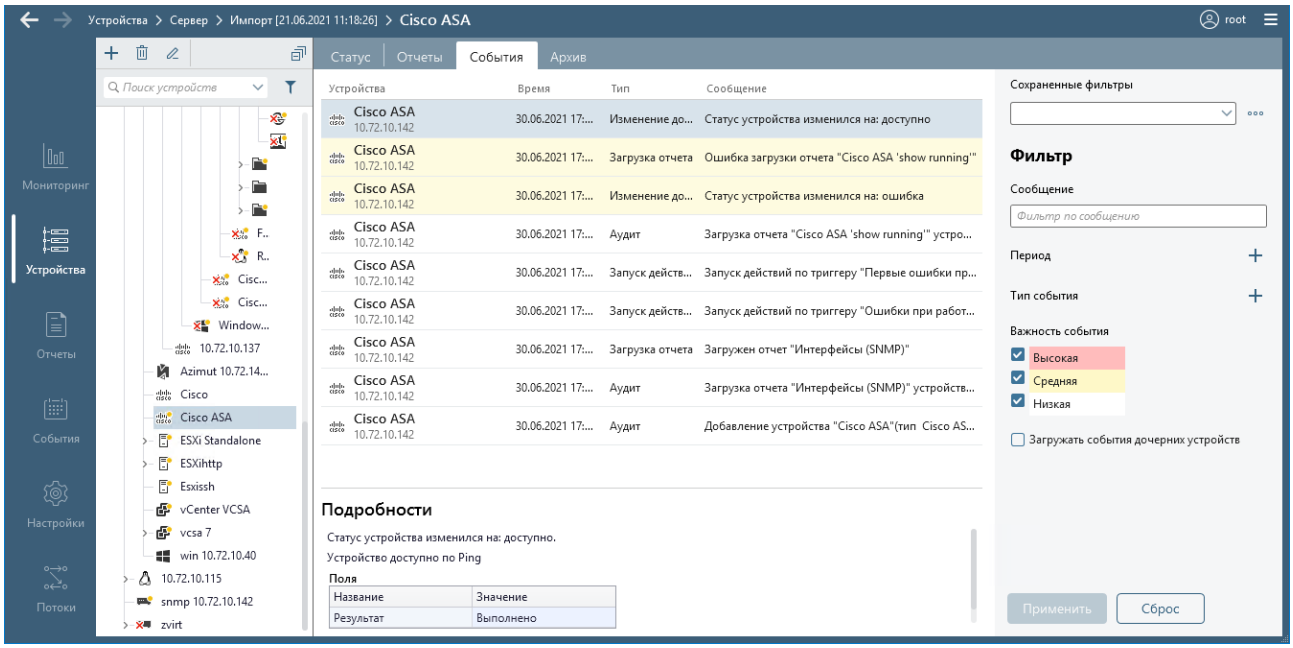


Рисунок 114 – Вкладка **События**

Панель списка событий содержит список всех зафиксированных для устройства/группы событий. Для каждого события построчно отображаются:

- дата и время произошедшего события;
- тип события;
- текст с кратким описанием события.

Пользователь имеет возможность копирования текста события для последующей его обработки средствами другого ПО.

Группировка списка событий во вкладке ***События*** по умолчанию отсутствует. В панели списка событий пользователю доступны операции группировки, сортировки и фильтрации с использованием параметров, расположенных в панели фильтрации (см. п. 2.11.3 «Фильтрация событий с использованием панели фильтрации»).

Для обновления списка событий, с учетом заданных ранее пользователем правил фильтрации, необходимо нажать кнопку ***Обновить*** в всплывающем сообщении ***«Список событий изменился. Обновить»***.

2.11.3. Фильтрация событий с использованием панели фильтрации

В списках событий раздела **События** и вкладки ***События*** раздела **Устройства** реализована возможность установки фильтра (см. рис. 112 и 114). По умолчанию события отфильтрованы по дате.

Заданные параметры фильтрации возможно сохранить, для применения к другим устройствам, зарегистрированным в комплексе. Для сохранения параметров фильтрации необходимо задать параметры фильтрации в полях панели **Фильтр** (рис. 115) (правила ввода параметров приведены ниже), нажать в поле ***Сохраненные фильтры*** кнопку ***Меню*** (), выбрать в раскрывшемся меню пункт ***Сохранить как***, ввести в открывшемся окне наименование создаваемого фильтра и нажать кнопку ***Сохранить***. Сохраненный фильтр появится в выпадающем списке поля ***Сохраненные фильтры***. Для удаления сохраненнного фильтра необходимо выбрать его наименование в списке поля ***Сохраненные фильтры*** нажать кнопку ***Меню*** () и выбрать в раскрывшемся меню пункт ***Удалить***.

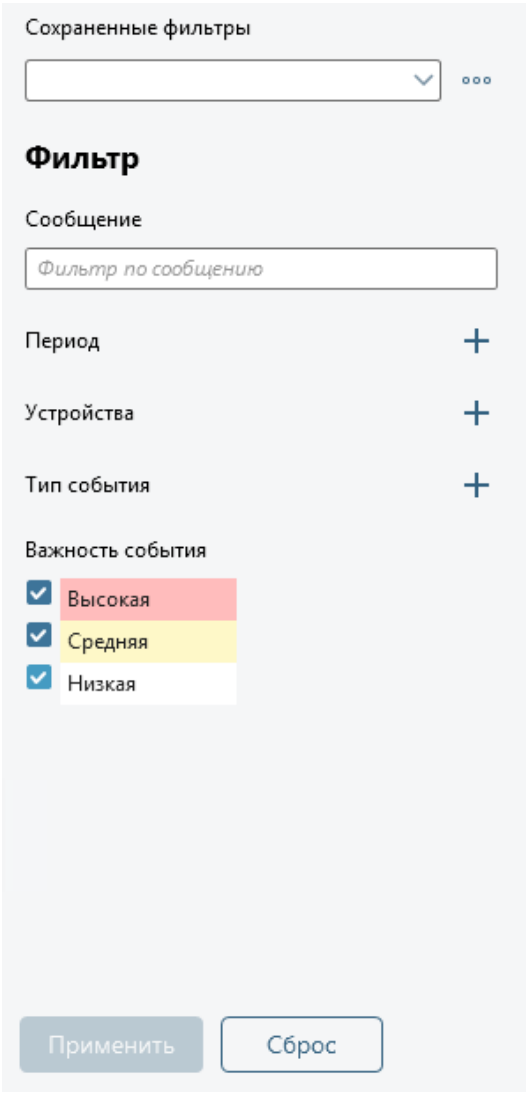


Рисунок 115 – Панель **Фильтр** списка событий

Для фильтрации событий по тексту сообщения, пользователю необходимо выполнить следующие действия:

1) В поле *Сообщение* (см. рис. 115) указать фрагмент сообщения, по которому должны быть отобраны события.
2) Нажать кнопку ***Применить***.

Примечание – Поиск по тексту сообщения выполняется с учетом регистра введенных символов.

Для фильтрации событий по времени, пользователю необходимо выполнить следующие действия:

1) В группе полей *Период* нажать кнопку ***Добавить*** (+), в отобразившихся дополнительных полях ***С*** и ***По*** указать даты начала и окончания временного периода, за который должны быть отобраны события.

2) Нажать кнопку ***Применить***. В панели списка событий устройства отобразится список событий, которые произошли на устройстве за указанный промежуток времени.

В разделе **События** настройка фильтрации отличается наличием в области настройки фильтра группы полей ***Устройства.*** Фильтр предназначен для выбора устройств, события которых должны отображаться в списке. При нажатии кнопки «+» открывается окно выбора устройств. Устройства выбираются установкой флагов, фильтр применятся после нажатия кнопки ***Применить*** в окне выбора.

Для фильтрации событий по типу события пользователю необходимо выполнить следующие действия:

1) В группе полей *Тип события* нажать кнопку ***Добавить*** (+).

2) Выбрать в списке отобразившегося поля тип события, для которого задается условие фильтрации.

3) Задать, при необходимости, дополнительные условия отбора событий для выбранного типа. Для добавления одного дополнительного условия необходимо выполнить следующие действия:

- нажать ссылку Добавить доп.условие;
- в открывшемся окне **Условие** из раскрывающегося списка поля ***Параметр*** выбрать событие, для которого задается условие фильтрации, в зависимости от выбранного параметра в окне **Условие** отобразятся дополнительные поля (пример окна с дополнительными полями приведен на рис. 116);
- установить необходимые переключатели (рис. 116, а) или заполнить поля выбора условия и указать значения этого условия фильтрации для выбранного события (рис. 116, б);
- нажать кнопку ***Сохранить***.

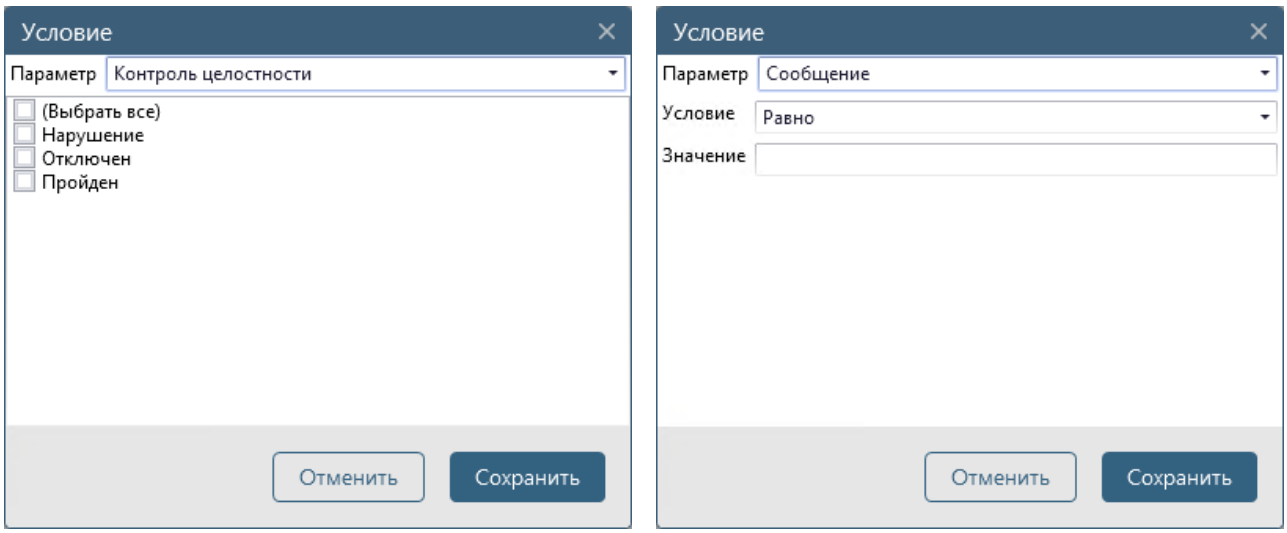
4) Внести, при необходимости, изменения в заданные дополнительные условия, для чего:

- нажать в строке дополнительного условия кнопку ***Изменить*** (✎);
- внести изменения в поля окна **Условие**;
- нажать кнопку ***Сохранить***.

5) При необходимости, добавить другие типы событий, повторив шаги 1 – 4.

6) Отменить ошибочно выбранные типы событий и заданные для них дополнительные условия, нажав соответствующие им кнопки ***Удалить*** (🗑).

7) Нажать кнопку ***Применить***. В панели списка событий выбранного устройства отобразится список событий, которые удовлетворяют заданным условиям фильтрации.



а) б)

Рисунок 116 – Окно **Условие** с дополнительными полями

Для отображения во вкладке ***События*** выбранного устройства сообщений только определенной степени важности необходимо установить флаги в полях группы *Важность события* и нажать кнопку ***Применить***. В комплексе существует возможность фильтрации событий по трем степеням важности: ***Высокая***, ***Средняя*** и ***Низкая***.

Для удаления введенных параметров фильтра необходимо нажать кнопку ***Сброс***. В панели списка событий выбранного устройства отобразится список всех событий, произошедших на устройстве.

Параметр ***Загружать события с дочерних устройств*** позволяет отобразить список событий для устройств, которые входят в группу на сервере ПК (если в панели устройств выделена группа) или в состав устройства, контролируемого на сервере ПК (например, список виртуальных машин на сервере управления VMware vCenter).

Для обновления списка событий – нажать кнопку ***Обновить*** в информационном сообщении *Список событий изменился* (см. рис. 112).

2.12. Просмотр отчетов в разделе Отчеты

ПК «Efros Config Inspector» v.4 предоставляет пользователям возможность просмотра сводной информации по нескольким выбранным устройствам.

В разделе **Отчеты** клиентской консоли программного комплекса пользователь может создать список шаблонов для формирования на их основе пользовательских отчетов следующих типов:

- ***Выборка*** – отчеты, содержащие последние загруженные с выбранных устройств версии отчета формата ***Конфигурации*** и ***Проверки*** (см. п. 2.4.3) выбранного типа в соответствии с заданными условиями фильтрации;
- ***Уязвимости устройств*** – отчеты, содержащие перечень уязвимостей для устройств заданных типов;

- ***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, неиспользуемых правил МЭ и правил с нулевым Hit Count для устройств заданных типов.

Раздел **Отчеты** (рис. 117) содержит:

- кнопку ***Сервер*** – при нажатии кнопки открывается окно выбора сервера для ведения списка шаблонов и просмотра отчетов по устройствам выбранного сервера. Окно выбора аналогично окну выбора сервера в разделе **Настройки** (см. пункт 2.3 «Настройка комплекса») и содержит список доступных пользователю в соответствии с иерархией серверов – текущий сервер и подчиненные ему сервера (если в ПК «Efros Config Inspector» v.4 настроена иерархия подключенных серверов);
- кнопку ***Отчет*** () – при нажатии кнопки открывается меню выбора типа отчета добавляемого шаблона;
- кнопку ***Фильтр*** (

) – по нажатию кнопки открывается окно фильтрации списка отчетов по их типу. Выбор осуществляется при установке флагов в полях требуемых типов отчетов. Отмена фильтрации выполняется по нажатию в окне ссылки ***Сбросить фильтр***;
- поле ***Поиск*** – для ввода символов из имени искомого шаблона, позволяет искать в списке шаблонов те из них, которые удовлетворяют введенному в поле значению;
- список шаблонов.

После установки комплекса в списке содержатся два шаблона:

- «Все изменения за сутки» – в отчете отображаются данные обо всех зафиксированных за предыдущие сутки изменениях во всех отчетах всех контролируемых устройств;
- «Все уязвимости» – в отчете отображаются данные обо всех уязвимостях любой критичности для всех контролируемых устройств.

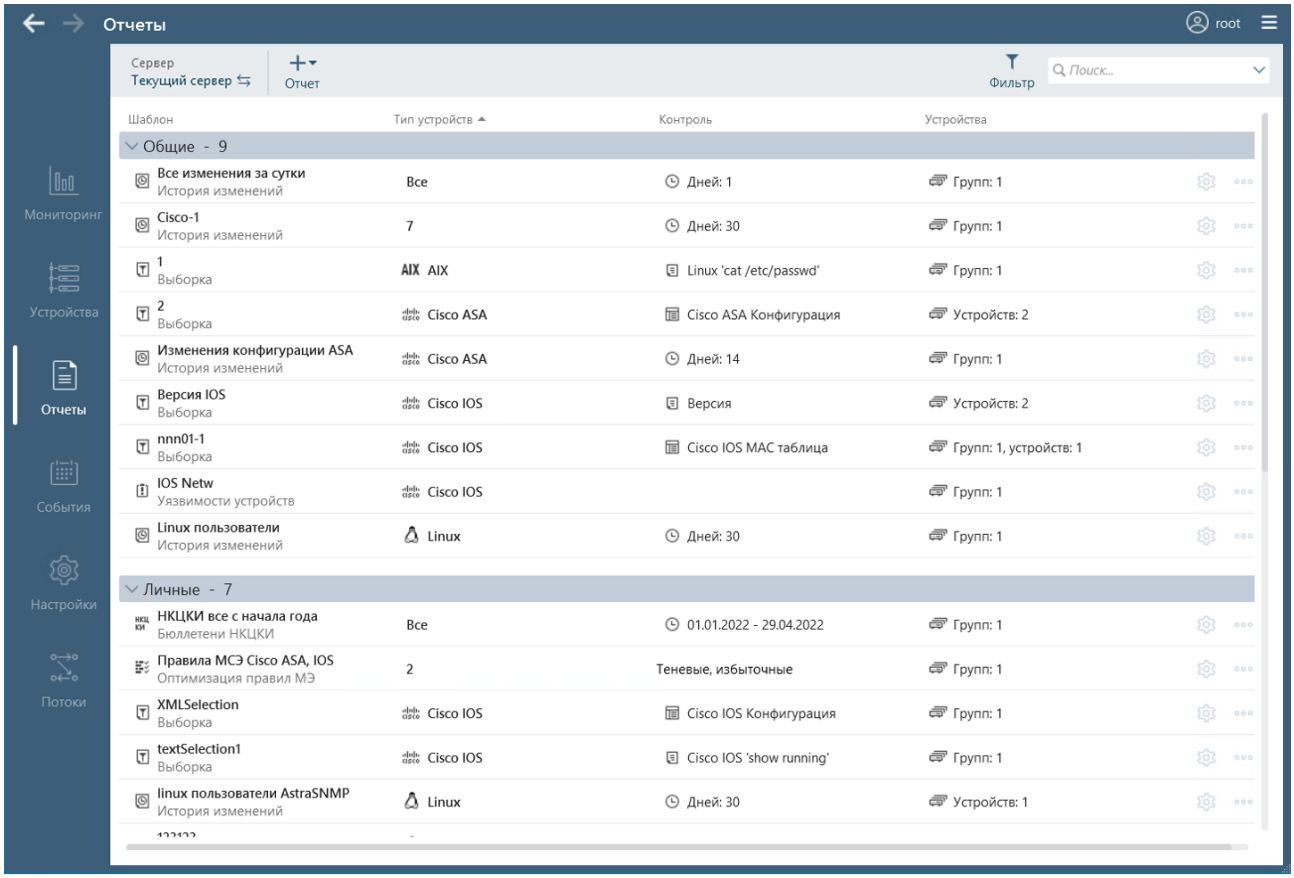


Рисунок 117 – Раздел **Отчеты**

Для каждого шаблона (по умолчанию и созданных пользователями (см. п. 2.12.1 «Добавление шаблона отчета и первичный просмотр отчета»)) в списке отображаются:

- пиктограмма типа отчета: «» – *Выборка*, «» – *История изменений*, «» – *Уязвимости устройств*, «» – *Бюллетени НКЦКИ*, «» – *Правила межсетевых экранов* и *Оптимизация правил МЭ* либо пиктограмма ошибки шаблона «»;
- наименование шаблона;
- тип устройства, количество выбранных типов устройств, если выбрано более одного типа устройств, или текст «*Все*», если выбраны все устройства в списке;
- для отчетов типа *Выборка* и *Проверки устройств* – тип отчета, для отчетов типа *История изменений* и *Бюллетени НКЦКИ* – период (интервал дат или количество предыдущих текущей дате дней, за который построен отчет), для отчетов типа *Оптимизация правил МЭ* – тип правил («теневые», избыточные или оба типа);
- количество групп устройств и устройств, для которых сформирован шаблон.

Кроме того, каждому шаблону в зависимости от прав пользователя (см. ниже) соответствуют кнопки:

- ***Изменить*** () – для перехода в форму настройки шаблона отчета (см. п. 2.12.3 «Изменение шаблона отчета»);

- ***Меню*** (…) – по нажатию кнопки раскрывается меню с пунктами:
  а) ***Выполнить на основе*** – для перехода в окно настройки параметров шаблона с возможностью запуска формирования отчета с обновленными параметрами;
  б) ***Удалить*** – для удаления шаблона (см. п. 2.12.4 «Удаление шаблона отчета»).

Шаблоны группируются в списке по их типу:
- ***Личные*** – шаблон доступен только создавшему его пользователю;
- ***Общие*** – шаблон доступен всем пользователям.

Доступ к списку ***Личные*** раздела **Отчеты** имеют все пользователи, имеющие доступ к ПК «Efros Config Inspector» v.4. Пользователи имеют возможность создания/редактирования/удаления личных шаблонов, формирования на их основе отчетов.

Права пользователей на просмотр/управление шаблонами типа ***Общие*** определяются правами доступа к функциям *Настройки контроля* (см. п. 1.2):

1) Если пользователю назначены права *Нет доступа* или *Просмотр*, то группа шаблонов ***Общие*** раздела **Отчеты** доступна ему для просмотра, пользователь имеет возможность сформировать на основе общего шаблона отчет, создать на основе общего шаблона новый шаблон типа ***Личные***. При этом пользователь не имеет возможности внести изменения в общий шаблон, удалить его.

2) Пользователи с правами *Управление* имеют полный доступ к шаблонам типа ***Общие*** – могут создавать, редактировать и удалять общие шаблоны.

По двойному щелчку левой клавишей «мыши» по наименованию шаблона запускается формирование отчета по заданным в шаблоне параметрам. При этом, если в шаблоне выбраны устройства/группы устройств, которые удалены из списка устройств сервера ПК или пропал доступ к ним, то эти устройства не будут учтены в отчете.

Если в шаблоне заданы параметры, по которым невозможно сформировать отчет (есть ошибки в шаблоне, из-за которых невозможно сформировать отчет), то слева от наименования шаблона отображается пиктограмма ошибки шаблона «», строка шаблона выделена розовым цветом фона. Такой шаблон доступен для изменения его параметров и повторного запуска формирования отчета.

2.12.1. Добавление шаблона отчета и первичный просмотр отчета

Для добавления на сервер ПК нового шаблона отчета необходимо выполнить следующие действия:

1) Перейти в раздел **Отчеты**.

2) В заголовке раздела нажать кнопку ***Отчет*** (+) и выбрать в открывшемся меню тип отчета шаблона (рис. 118).

3) Ввести в открывшемся окне параметры формирования отчета (подробнее для каждого типа шаблона см. пункты 2.12.1.1 – 2.12.1.5).

4) Нажать кнопку ***Применить***.

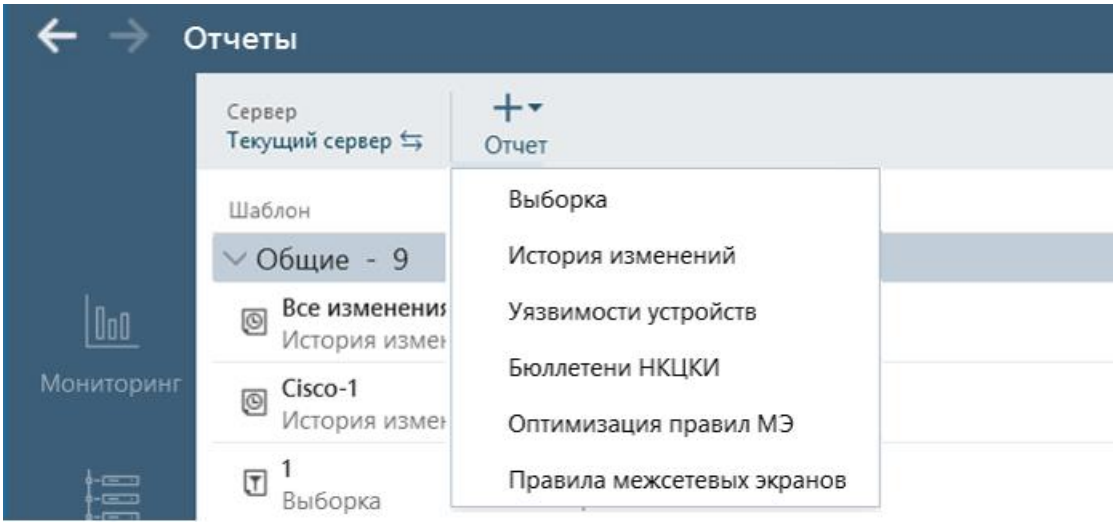


Рисунок 118 – Меню раздела **Отчеты**

5) Просмотреть отчет и при необходимости сохранить его в файл формата HTML, для чего нажать кнопку ***Экспорт*** и выбрать в открывшемся стандартном окне ОС путь для сохранения файла.

6) При необходимости, изменить параметры отчета, для чего нажать кнопку ***Параметры выборки***, в открывшемся окне настройки параметров отчета внести требуемые изменения и нажать кнопку ***Применить***. Отчет отобразится в соответствии с новыми параметрами.

7) Сохранить шаблон отчета, для чего нажать кнопку ***Шаблон***, в открывшемся окне **Сохранение шаблона** (рис. 119):

- выбрать тип шаблона ***Личные*** или ***Общие***;
- ввести в поле ***Название*** имя шаблона,
- оставить текущие параметры формирования отчета без изменений или внести требуемые изменения;
- нажать кнопку ***Сохранить***.

Примечание – Имя нового шаблона должно быть уникальным, запрещено использовать имена уже существующих на сервере ПК шаблонов в разделе **Отчеты**.

Созданный шаблон в зависимости от его типа и прав доступа пользователя (см. п. 2.12 «Просмотр отчетов в разделе Отчеты») доступен для редактирования его параметров, удаления и повторного запуска формирования отчета по шаблону всем пользователям или создавшему шаблон пользователю.

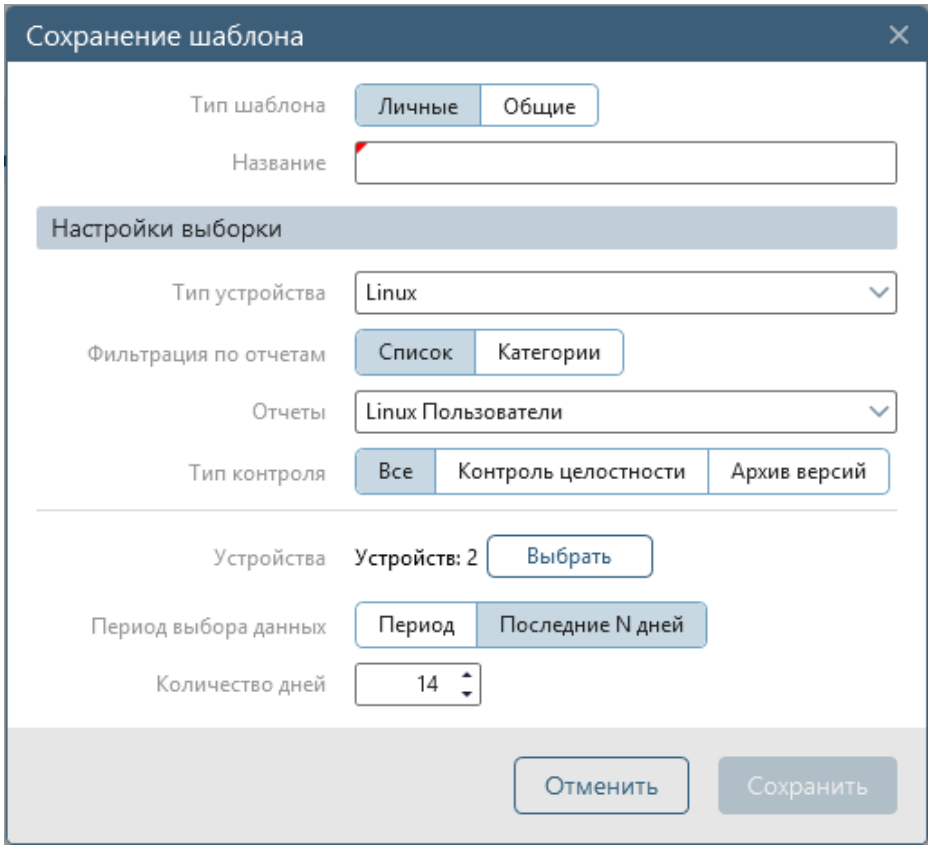


Рисунок 119 – Окно **Сохранение шаблона**

2.12.1.1. Ввод параметров отчета и просмотр отчета для типа шаблона *Выборка*

При выборе типа шаблона ***Выборка*** открывается окно **Выборка** (рис. 120). Далее необходимо в окне:

1) Выбрать в полях ***Тип устройства*** и ***Базовый отчет*** требуемый тип устройства и тип отчета для загрузки.

2) Выбрать устройства для создания выборки отчетов – нажать в поле ***Устройства*** кнопку ***Выбрать*****,** в открывшемся окне **Выбор устройств** отметить устройства, загруженные версии отчетов с которых будут выведены в отчете, и нажать кнопку ***Выбрать***.

Примечания:

- в списке поля ***Тип устройств*** окна **Выборка** отображаются все типы устройств, внешние модули, для работы с которыми подключены к серверу ПК, и для которых предусмотрена загрузка отчетов с устройства;
- в списке поля ***Базовый отчет*** отображаются все доступные типы отчетов для выбранного типа устройств, кроме служебных отчетов типа «Версия», «Модель», «Серийный номер»;
- список устройств окна **Выбор устройств** содержит наименования контролируемых на сервере ПК устройств выбранного типа, для которых доступен выбранный тип отчета. Правила поиска, фильтрации и выбора групп и устройств в окне приведены в п. 2.2.5.4 «Настройка виджетов».

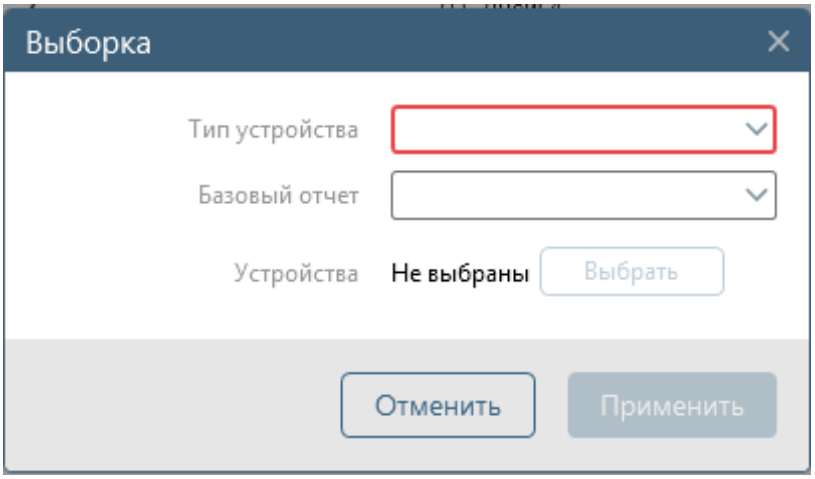
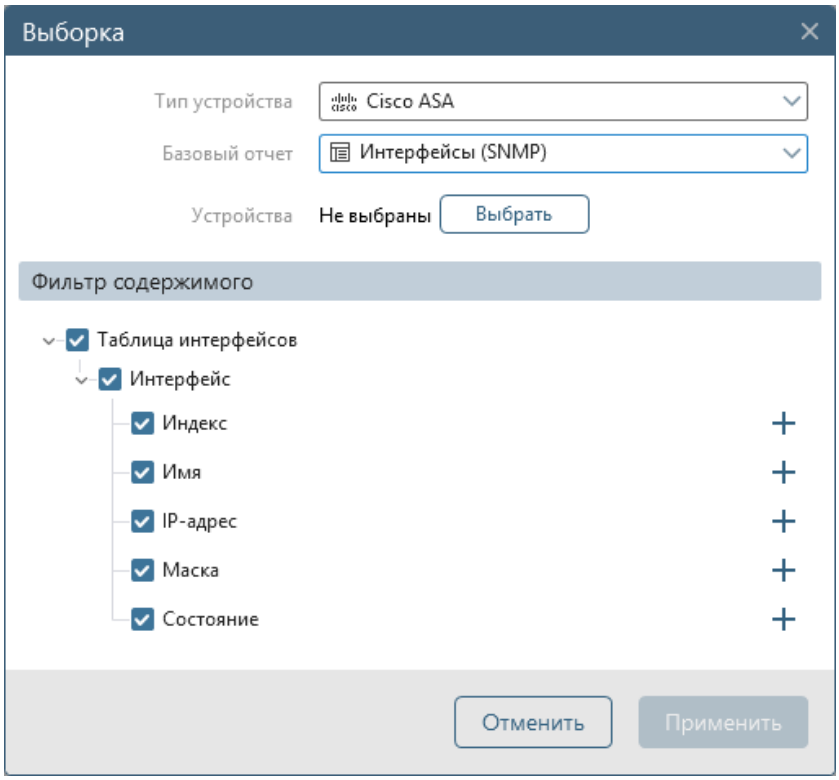


Рисунок 120 – Окно **Выборка**

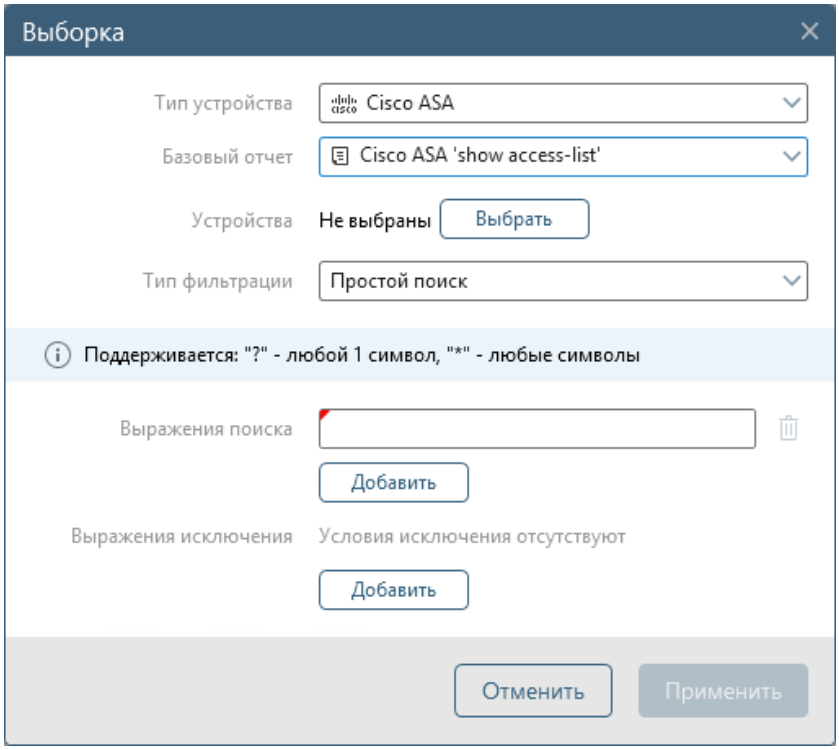
3) В отобразившихся дополнительных полях настроить условия отбора данных:

– если выбран базовый отчет формата ***Конфигурации*** – для структурированных отчетов (рис. 121, а) в соответствии с п. 2.9.7.1 «Настройка условий фильтрации для структурированных отчетов», для текстовых отчетов (рис. 121, б) – в соответствии с п. 2.9.7.2 «Настройка условий фильтрации для текстовых отчетов»;

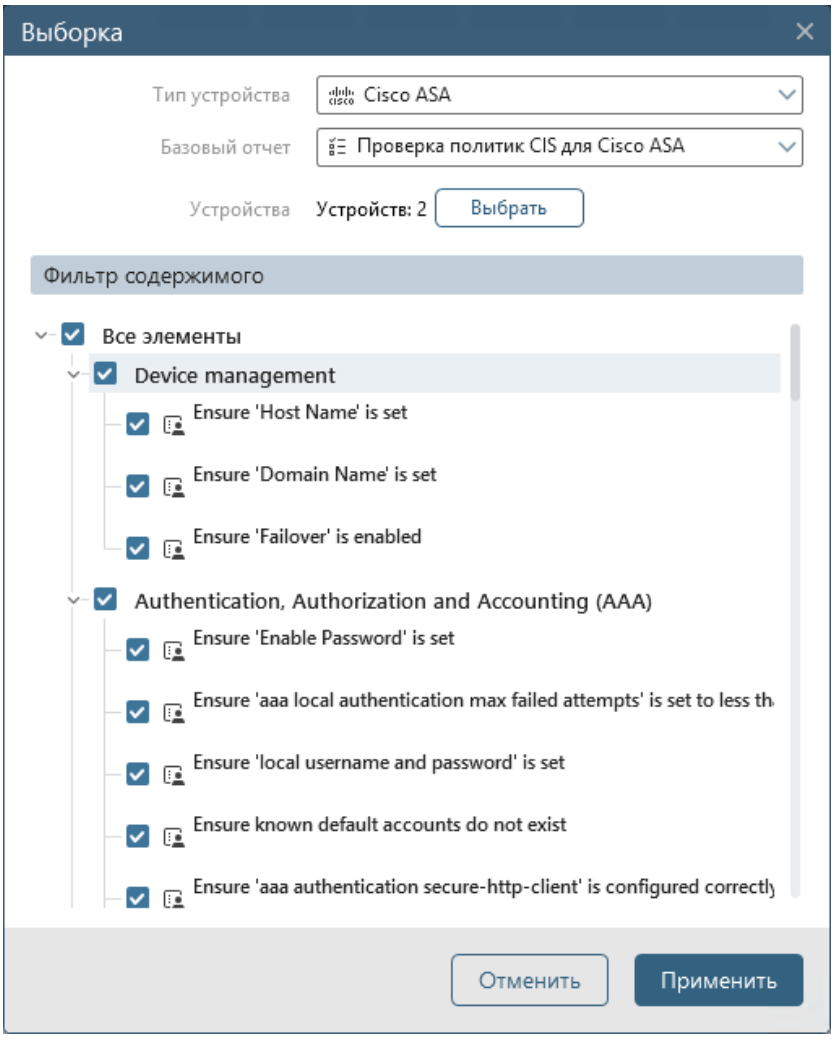
– если выбран базовый отчет формата ***Проверки*** – установить/отменить установку флагов (рис. 121, в) для отдельных проверок и групп проверок в целом.



а)



б)



в)

Рисунок 121 – Окно **Выборка** с фильтром содержимого отчета

4) Нажать кнопку ***Применить***. Откроется окно просмотра сформированного отчета. В заголовке отчета указано имя базового отчета, общее количество выбранных для отчета устройств. В отчете на основе отчета формата:

– ***Конфигурации*** (рис. 122) – левая панель отчета содержит список выбранных устройств, правая панель – последние загруженные с устройств версии отчета выбранного типа в соответствии с заданными условиями фильтрации. Если отчет для устройства с заданными параметрами отсутствует, то отображается сообщение *Нет данных*. Для скрытия таких строк в отчете необходимо выключить переключатель *Пустые результаты*;

– ***Проверки*** (рис. 123) – приведен перечень проверок с результатами их выполнения для всех выбранных устройств. Для каждой проверки приведено количество устройств, прошедших проверку успешно и не прошедших проверку, описание проверки и в блоке ***Устройства*** – список выбранных для отчета устройств с результатом выполнения проверки для каждого из них. Для отображения в отчете только данных о нарушении проверок необходимо включить переключатель *Только нарушения.*

При выборе имени устройства открывается карточка устройства (см. рис. 123), в которой приведены основные сведения о его конфигурации, уровне защищенности, обнаруженных уязвимостях (с учетом наличия скрытых уязвимостей) и количестве уведомлений по типам (отображается информация только об имеющихся уведомлениях).

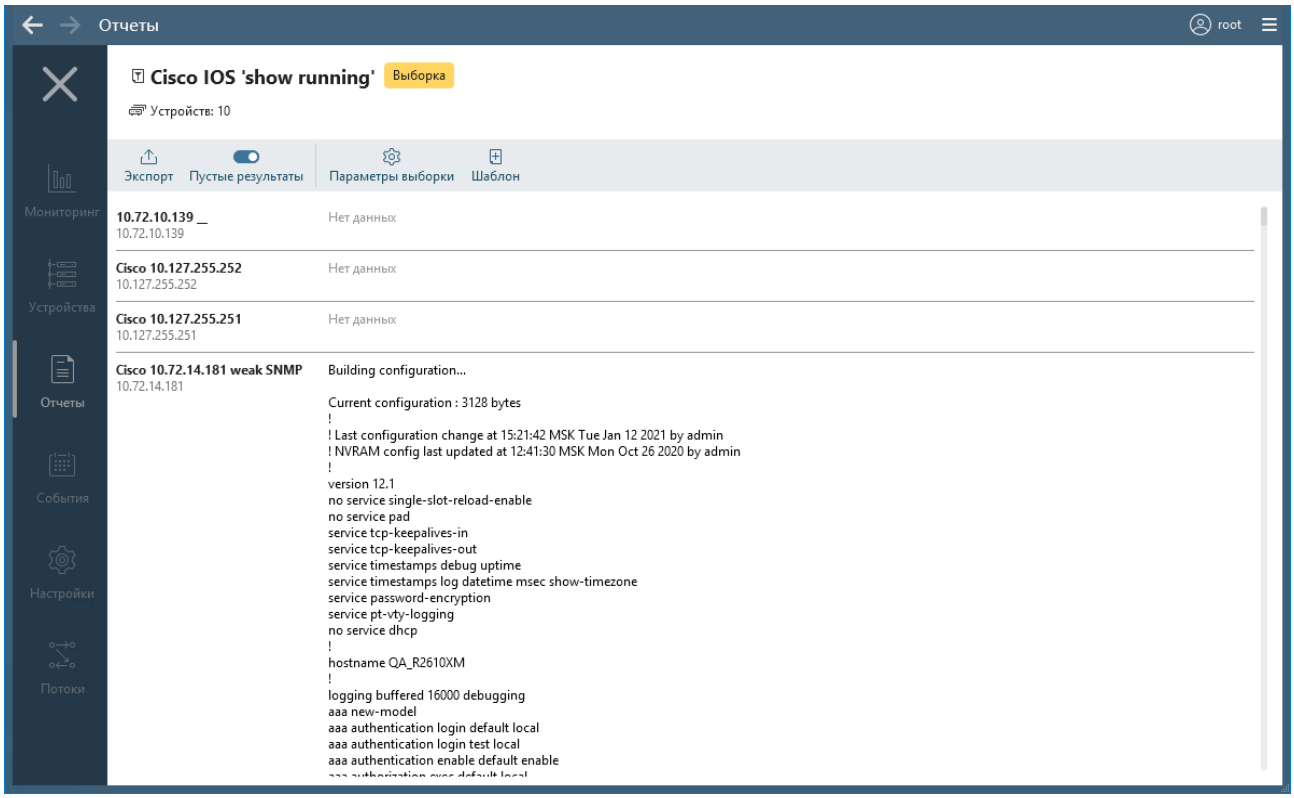


Рисунок 122 – Окно просмотра отчета типа ***Выборка***, сформированного для базового отчета формата ***Конфигурации***

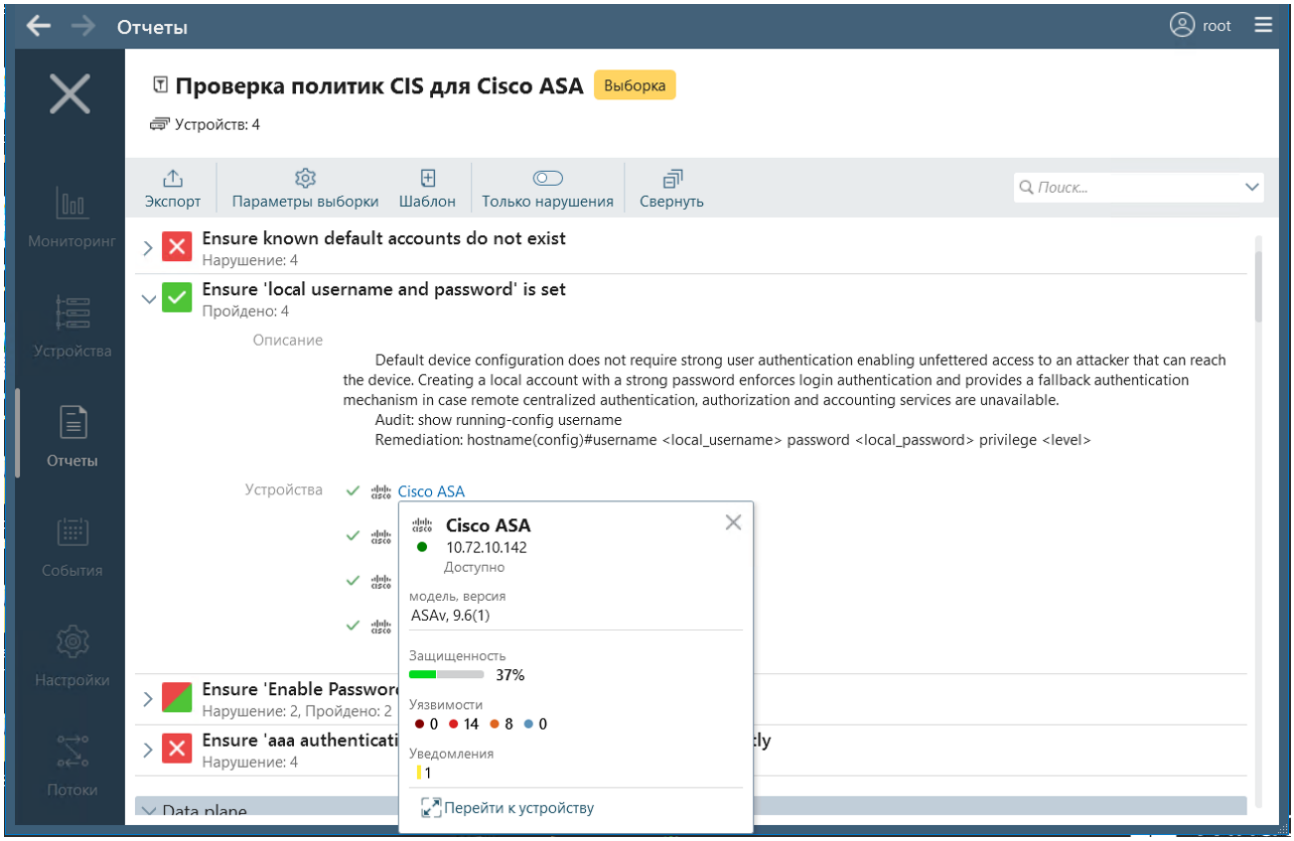


Рисунок 123 – Окно просмотра отчета типа ***Выборка***, сформированного для базового отчета формата ***Проверки***

Пользователь имеет возможность в карточке выделить и скопировать данные устройства: имя устройства, адрес, описание (при его наличии в карточке), модель, версию. Из карточки устройства можно перейти на вкладку ***Статус*** раздела **Устройства**, нажав кнопку ***Перейти к устройству***, расположенную в нижней части карточки.

В отчетах ***Выборка*** на основе структурированных базовых отчетов (формата .xml) и на основе отчетов по проверкам безопасности пользователь, используя кнопку ***Свернуть*** (), может настроить представление отчета с раскрытыми или свернутыми уровнями дерева.

2.12.1.2. Ввод параметров отчета и просмотр отчета для типа шаблона *Уязвимости устройств*

При выборе типа шаблона ***Уязвимости устройств*** открывается окно **Уязвимости устройств** (рис. 124).

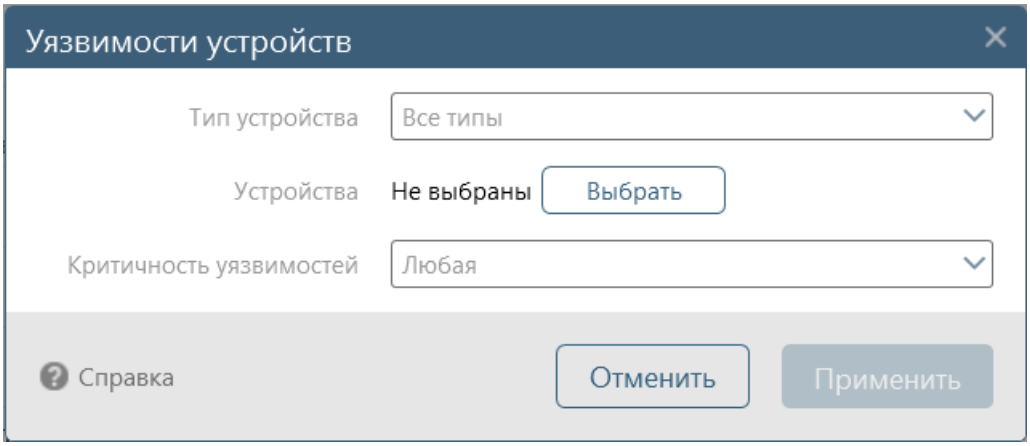


Рисунок 124 – Окно **Уязвимости устройств**

Далее необходимо в окне:

1) Выбрать в поле ***Тип устройства*** требуемый тип устройства.

2) Выбрать устройства для создания выборки отчетов, выполнив действия аналогично шагу 2 пункта 2.12.1.1 «Ввод параметров отчета и просмотр отчета для типа шаблона *Выборка*».

3) Выбрать в поле ***Критичность уязвимостей*** требуемые уровни критичности уязвимостей. При установке в поле курсора раскрывается список полей для выбора уровней критичности: *Критический*, *Высокий*, *Средний*, *Низкий*. Если ни в одном поле не установлен флаг, то для формирования отчета выбраны все уровни критичности.

4) Нажать кнопку ***Применить***. Откроется окно просмотра сформированного отчета (рис. 125).

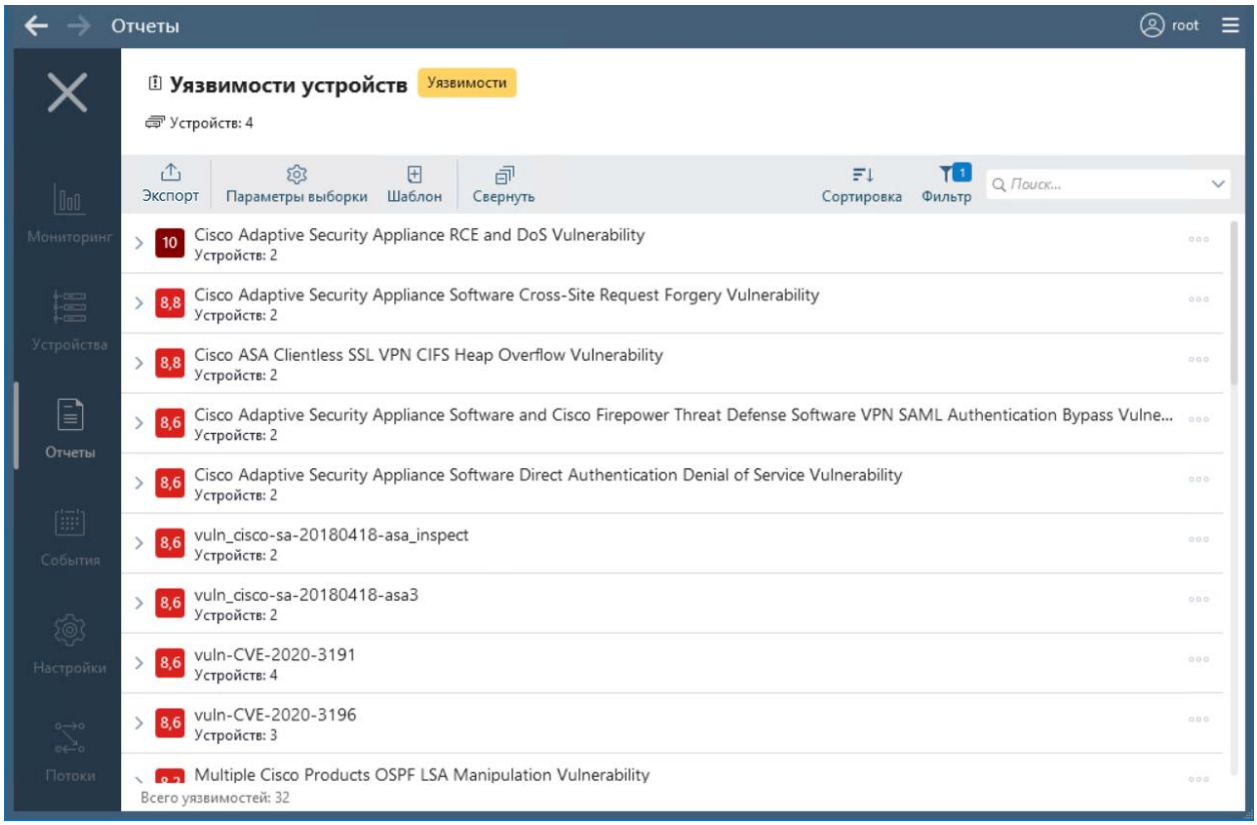


Рисунок 125 – Отчет типа ***Уязвимости устройств***

В заголовке отчета указан тип отчета и общее количество выбранных для отчета устройств. В отчете приведен перечень уязвимостей заданной критичности, выявленных хотя бы для одного из выбранных для отчета устройств. В нижней части отчета приведено общее количество отобранных уязвимостей. По умолчанию уязвимости отсортированы в порядке уменьшения оценки их критичности. Пользователь имеет возможность выбрать тип сортировки по количеству устройств, для которых уязвимости выявлены, для чего – нажать кнопку ***Сортировка*** () и установить переключатель в поле ***по количеству устройств***.

Кроме того, установкой флагов в окне фильтрации (открывается по кнопке ***Фильтр*** ()) список уязвимостей может быть отфильтрован по состоянию (*Активные*/*Скрытые*). По умолчанию в окне установлен флаг в поле ***Активные*** и в отчете отображаются уязвимости, находящиеся в состоянии *Активные* хотя бы для одного из устройств, для которых они выявлены. Если уязвимость скрыта для всех устройств, для которых она выявлена, то она будет отображаться в списке только при выборе в окне фильтрации состояния *Скрытые*.

Для каждой уязвимости (рис 126) в ее заголовке указаны уровень критичности, ее наименование, количество устройств, для которых она выявлена и активна, и, при наличии скрытых уязвимостей – количество устройств, для которых уязвимость скрыта. При клике по заголовку раскрывается панель с описанием уязвимости, в блоке *Устройства* которой приведен список устройств. При выборе имени устройства открывается карточка устройства аналогично отчету типа ***Проверки устройств*** (см. шаг 4 пункта 2.12.1.1 «Ввод параметров отчета и просмотр отчета для типа шаблона *Выборка*»).

Примечание – Используя кнопку ***Свернуть*** (), пользователь может настроить представление отчета с раскрытыми или свернутыми панелями описания уязвимостей.

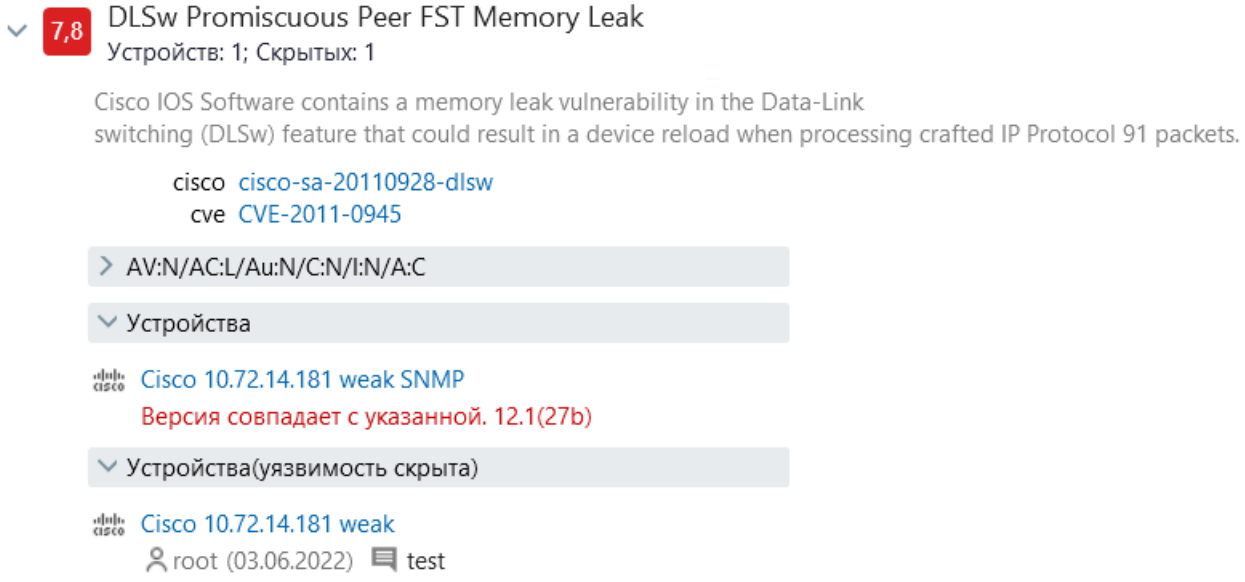


Рисунок 126 – Отображение данных уязвимости

В блоке ***Устройства*** под названием устройств, для которых уязвимость скрыта, дополнительно отображаются логин пользователя, скрывшего уязвимость, дата скрытия и введенный пользователем комментарий.

Например, на рис 126 уязвимость выявлена для двух устройств, для устройства *Cisco 10/72/14/181 weak* уязвимость скрыта и отображается в списке устройств, поскольку в окне фильтрации установлен флаг ***Скрытые***.

Пользователь имеет возможность скрыть уязвимости и активировать скрытые ранее.

Примечание – Пользователь для доступа к функции скрытия/активирования уязвимости должен иметь полные права доступа к устройствам.

Для скрытия уязвимости необходимо:

1) Нажать в строке скрываемой уязвимости кнопку ***Меню*** (⋯) и выбрать пункт ***Скрыть для устройств...***.
2) Ввести в открывшемся окне (рис. 127) комментарий.
3) Выбрать в поле ***Устройства*** установкой флагов устройства, для которых должна быть скрыта уязвимость. Список устройств содержит устройства, для которых уязвимость выявлена и не скрыта ранее. Установкой флага ***Все устройства*** для скрытия уязвимости выбираются все устройства, для которых уязвимость выявлена.
4) Нажать кнопку ***Скрыть***.

Примечание – Заполнение поля **Комментарий** обязательно.

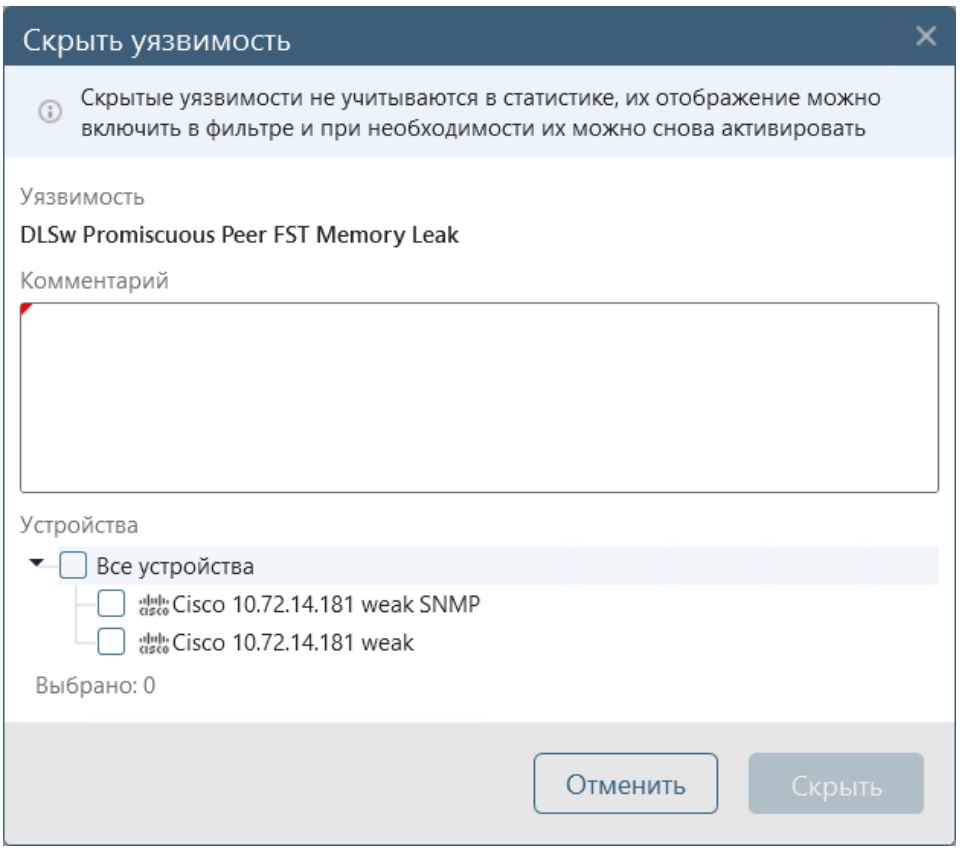


Рисунок 127 – Окно **Скрыть уязвимость** для нескольких устройств

Скрытые уязвимости доступны для активации. Для активации уязвимости необходимо:

1) Нажать в строке скрываемой уязвимости кнопку ***Меню*** (⋯) и выбрать пункт ***Активировать для устройств...***.

2) Выбрать в поле ***Устройства*** открывшегося окна (рис. 128) установкой флагов устройства, для которых должна быть активирована уязвимость. Список устройств содержит устройства, для которых уязвимость выявлена и скрыта ранее. Установкой флага ***Все устройства*** для активации уязвимости выбираются все устройства списка.

3) Нажать кнопку ***Активировать***.

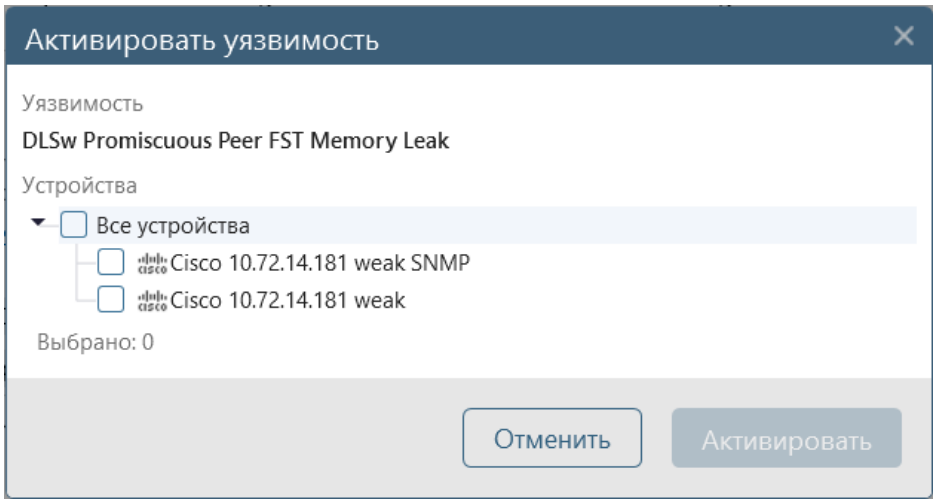


Рисунок 128 – Окно **Активировать уязвимость** для нескольких устройств

2.12.1.3. Ввод параметров отчета и просмотр отчета для типа шаблона *История изменений*

При выборе типа шаблона ***История изменений*** открывается окно **История изменений конфигураций** (рис. 129). Состав полей окна приведен в таблице 15.

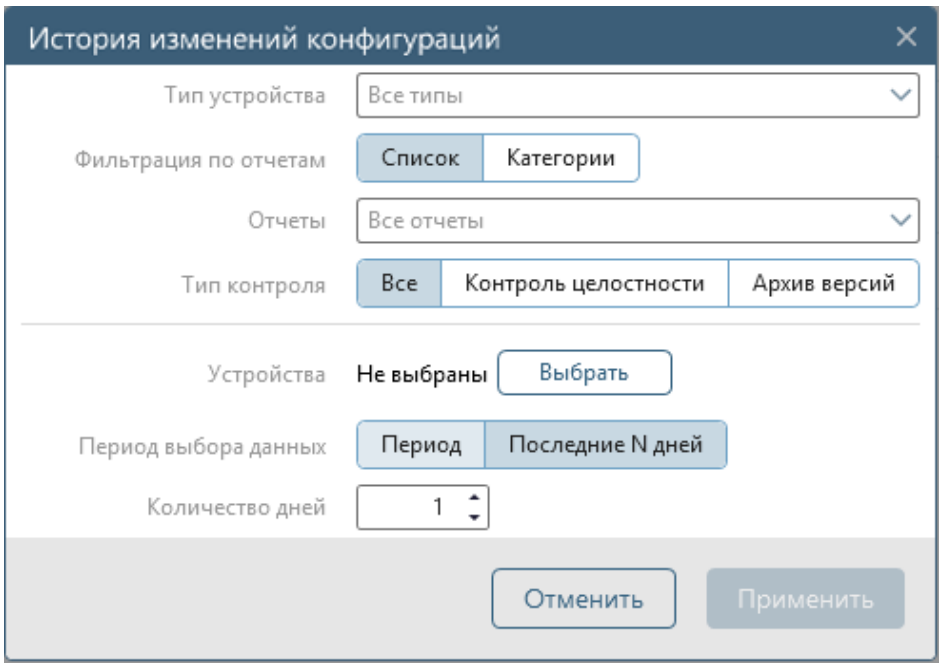


Рисунок 129 – Окно **История изменений конфигураций**

Таблица 15 – Состав и описание полей окна создания/редактирования расписания

Поле	Описание/Назначение
Типы устройств	Поле для выбора типов устройств, для которых должен быть сформирован отчет. Содержит список поддерживаемых сервером ПК типов устройств (зависит от состава подключенных к серверу ПК внешних модулей). Каждому типу устройств соответствует поле для флага. Требуемые типы устройств выбираются установкой флагов
Фильтрация по отчетам	Переключатель с двумя положениями: – *Список* – пользователь сможет выбрать в поле *Отчеты* (см. ниже) требуемые отчеты из полного списка отчетов выбранных ранее типов устройств; – *Категории* – пользователь сможет выбрать в поле *Категория отчетов* (см. ниже) требуемые категории отчетов из списка категорий отчетов
Отчеты	Поле для выбора типов отчетов, по данным которых должен быть сформирован отчет. Отображается только после нажатия в поле *Фильтрация по отчетам* кнопки ***Список***. Содержит список типов отчетов, поддерживаемых выбранными ранее типами устройств. Каждому типу отчета соответствует поле для флага. Требуемые типы отчетов выбираются установкой флагов
Категория отчетов	Поле для выбора категорий отчетов, по данным которых должен быть сформирован отчет. Отображается только после нажатия в поле *Фильтрация по отчетам* кнопки ***Категория***. Содержит список категорий отчетов, поддерживаемых выбранными ранее типами устройств. Каждой категории отчета соответствует поле для флага. Требуемые категории отчетов выбираются установкой флагов
Тип контроля	Переключатель выбора типа контроля, заданного для отчетов, по которым история изменений должна попасть в отчет
Устройства	Поле для выбора устройств и групп устройств, для которых должен быть сформирован отчет. Выбор выполняется установкой флагов в окне **Выбор устройств**, которое открывается по нажатию кнопки ***Выбрать***. После нажатия в окне выбора кнопки ***Выбрать*** в поле отображается количество выбранных устройств и групп устройств
Период выбора данных	Переключатель для выбора варианта выбора данных для формирования отчета, в зависимости от выбранного положения переключателя в окне отображаются дополнительные поля: – *Период* – дополнительные поля *Начало периода* и *Конец периода*, в которых указываются начальная и конечная даты период выборки данных в отчет; – *Последние N дней* – дополнительное поле *Количество дней*, в котором указывается количество дней, предшествующих текущему дню, для выборки данных в отчет

После задания параметров шаблона (выбора типа устройств и устройств, вида отчета, периода выборки данных, типа контроля отчета и категории отчета) и

нажатия кнопки ***Применить*** открывается окно просмотра сформированного по заданным параметрам отчета (рис. 130).

В заголовке отчета указано имя базового отчета (при его отсутствии – тип отчета, например, ***История изменений***), общее количество выбранных для отчета устройств и заданный период формирования отчета.

Левая панель отчета содержит список-дерево выбранных устройств, на нижнем уровне дерева – отчеты, по которым зафиксированы изменения, правая панель – содержит данные по выбранному в дереве элементу: список измененных отчетов для устройства/группы устройств, история изменений выбранного отчета за выбранный период либо, если изменений нет, то сообщение *Изменения отсутствуют*.

По умолчанию в отчете отобразятся данные только для тех устройств, для которых в заданный период зафиксированы изменения, для просмотра данных по всем выбранным устройствам (с изменениями и без) – перевести переключатель ***Устройства без изменений*** в положение *Включено* ().

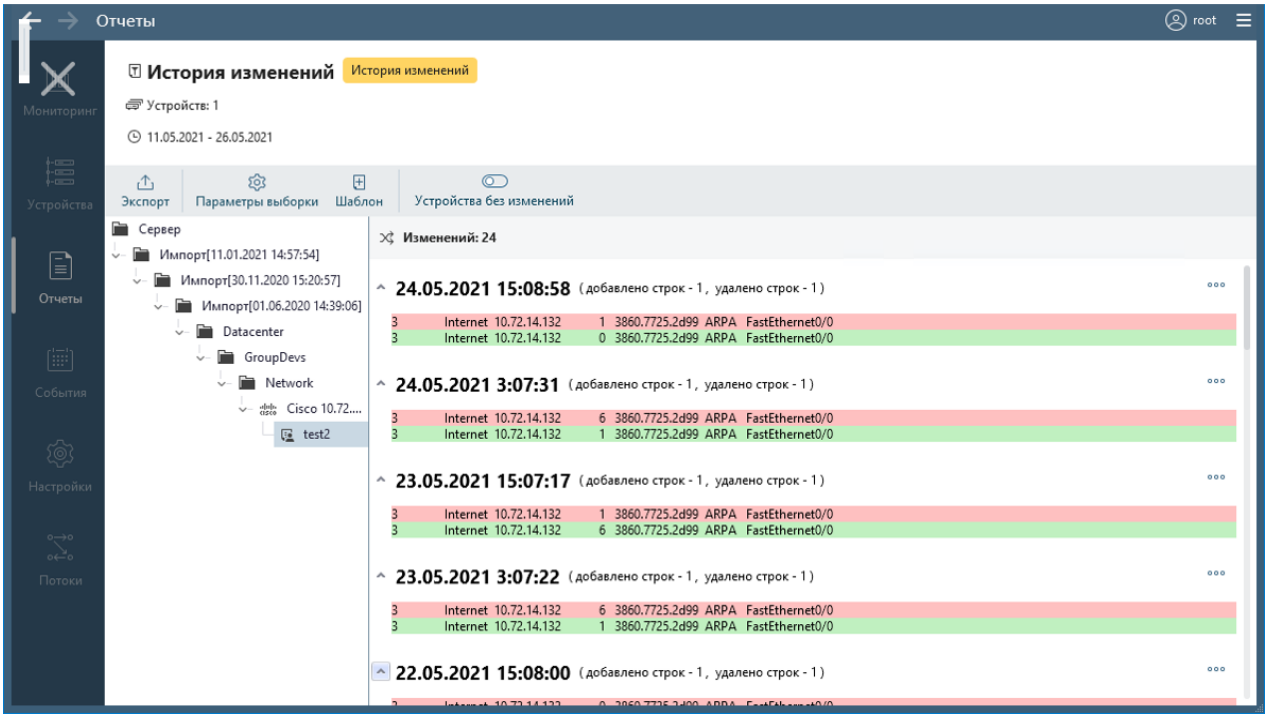


Рисунок 130 – Отчет **История изменений**

2.12.1.4. Ввод параметров отчета и просмотр отчета для типа шаблона *Бюллетени НКЦКИ*

При выборе типа шаблона ***Бюллетени НКЦКИ*** открывается окно **Бюллетени НКЦКИ** (рис. 131). Состав полей окна приведен в таблице 16.

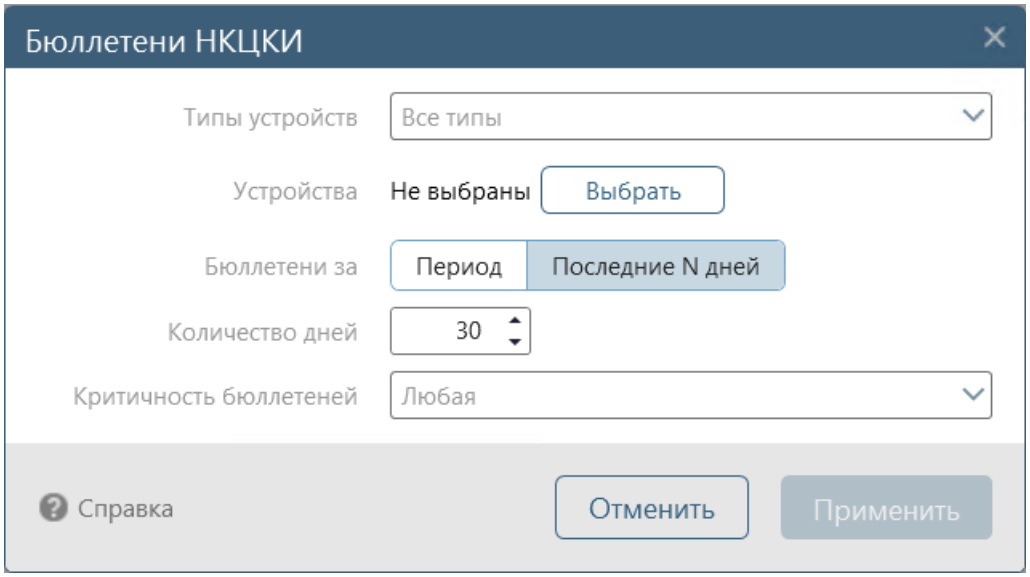


Рисунок 131 – Окно **Бюллетени НКЦКИ**

Таблица 16 – Состав и описание полей окна **Бюллетени НКЦКИ**

Поле	Описание/Назначение
Типы устройств	Поле для выбора типов устройств, для которых должен быть сформирован отчет. Содержит список поддерживаемых сервером ПК типов устройств (зависит от состава подключенных к серверу ПК внешних модулей). Каждому типу устройств соответствует поле для флага. Требуемые типы устройств выбираются установкой флагов
Устройства	Поле для выбора устройств и групп устройств, для которых должен быть сформирован отчет. Выбор выполняется установкой флагов в окне **Выбор устройств**, которое открывается по нажатию кнопки ***Выбрать***. После нажатия в окне выбора кнопки ***Выбрать*** в поле отображается количество выбранных устройств и групп устройств
Бюллетени за	Переключатель для выбора варианта выбора бюллетеней для формирования отчета, в зависимости от выбранного положения переключателя в окне отображаются дополнительные поля: – *Период* – дополнительные поля *Начало периода* и *Конец периода*, в которых указываются начальная и конечная даты периода выборки данных в отчет (по умолчанию – предыдущая и текущая даты); – *Последние N дней* – дополнительное поле *Количество дней*, в котором указывается количество дней, предшествующих текущему дню, для выборки данных в отчет (по умолчанию – 30 дней)
Критичность бюллетеней	Поле со списком полей для выбора уровней критичности: *Критичные*, *Высокой важности*, *Средней важности*, *Не определена*. Если ни в одном поле не установлен флаг, то для формирования отчета выбраны все уровни критичности уязвимостей

После задания параметров шаблона (выбора типа устройств и устройств, периода выбора данных) и нажатия кнопки ***Применить*** открывается окно просмотра сформированного по заданным параметрам отчета (рис. 132). В заголовке отчета указаны тип устройств, общее количество выбранных для отчета устройств.

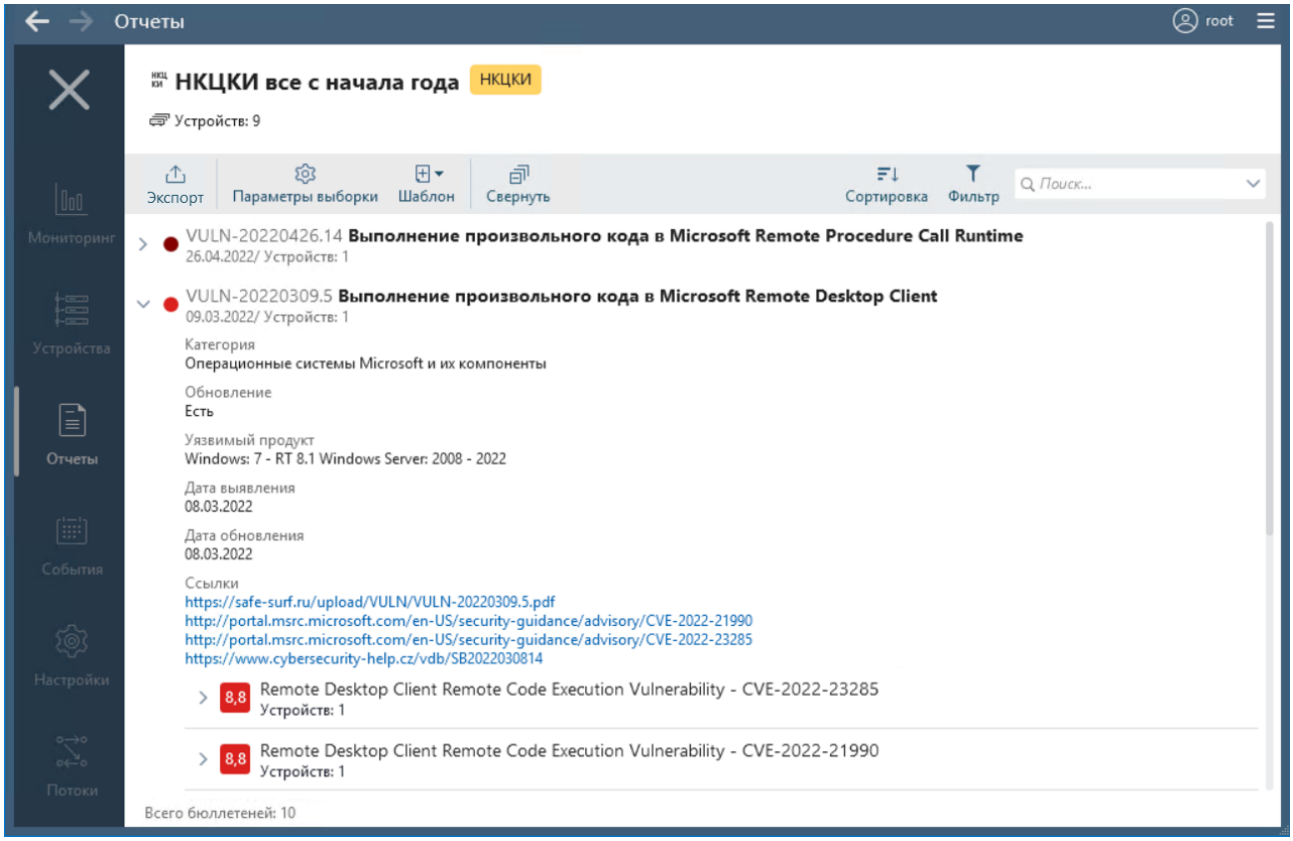


Рисунок 132 – Отчет **Бюллетени НКЦКИ**

Отчет содержит список бюллетеней, отобранных по указанным параметрам. В нижней части отчета приведено общее количество отобранных бюллетеней.

Для каждого бюллетеня отображаются: ID, название, дата выпуска и общее количество устройств в бюллетене. Для просмотра подробной информации бюллетеня необходимо выбрать установкой курсора название требуемого бюллетеня, раскроется панель просмотра с общими данными бюллетеня и списком уязвимостей.

Список уязвимостей отсортирован по критичности уязвимостей, начиная с высшего уровня критичности с наибольшей оценкой (10) до уровня критичности *Не определено*. Для каждой уязвимости отображаются ее полное описание, вектор и список устройств комплекса, для которых уязвимость актуальна.

При просмотре отчета пользователю доступны сортировка списка по критичности/дате/количеству устройств, поиск по имени и ID, настройка представления отчета с раскрытыми или свернутыми панелями просмотра данных бюллетеней.

2.12.1.5. Ввод параметров отчета и просмотр отчета для типа шаблона *Оптимизация правил МЭ*

При выборе типа шаблона ***Оптимизация правил МЭ*** открывается окно **Оптимизация правил МЭ** (рис. 133). Состав полей окна приведен в таблице 17.

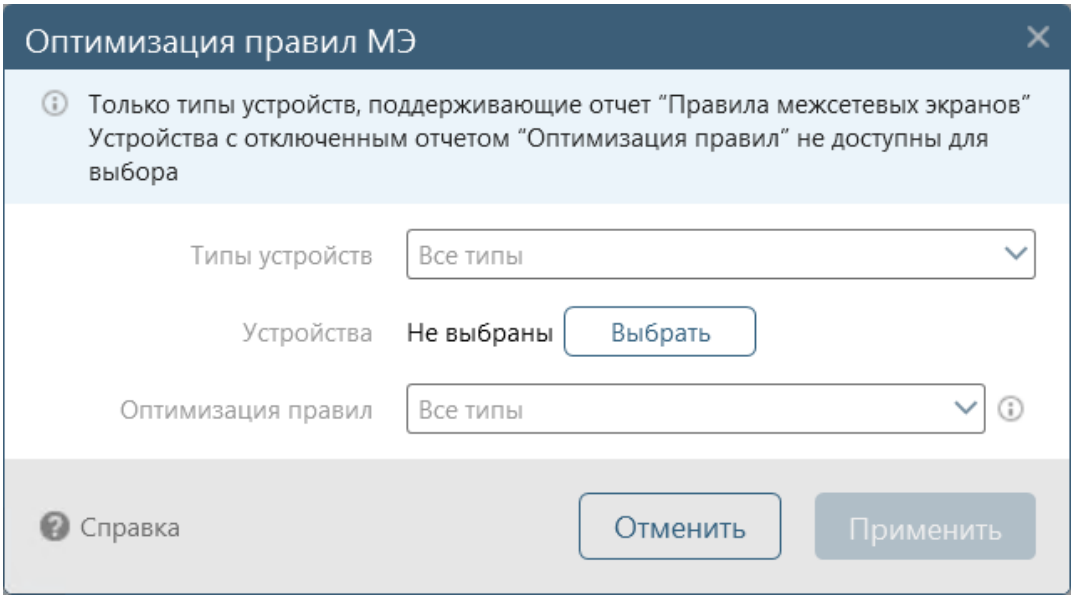


Рисунок 133 – Окно **Оптимизация правил МЭ**

Таблица 17 – Состав и описание полей окна **Оптимизация правил МЭ**

Поле	Описание/Назначение
Типы устройств	Поле для выбора типов устройств, для которых должен быть сформирован отчет. Содержит список поддерживаемых сервером ПК типов устройств, у которых доступны правила МЭ и разрешен для загрузки отчет ***Оптимизация правил***. Каждому типу устройств соответствует поле для флага. Требуемые типы устройств выбираются установкой флагов
Устройства	Поле для выбора устройств и групп устройств, для которых должен быть сформирован отчет. Выбор выполняется установкой флагов в окне **Выбор устройств**, которое открывается по нажатию кнопки ***Выбрать***. Примечание – Поле для флага, соответствующее устройству, для которого не включен отчет по оптимизации, неактивно. Соответственно, при выборе группы устройств в итоговую выборку такие устройства не попадают. После нажатия в окне выбора кнопки ***Выбрать*** в поле отображается количество выбранных устройств и групп устройств
Оптимизация правил	Поле для выбора типов правил МЭ для формирования отчета: *Теневые*, *Избыточные, Неиспользуемые и Нулевые Hit Count.* Каждому типу правил МЭ соответствует поле для флага. По умолчанию во всех полях флаги отсутствуют, выбраны все типы правил. Требуемые типы правил МЭ выбираются установкой флагов

После задания параметров шаблона (выбора типа устройств и устройств, типа правил) и нажатия кнопки ***Применить*** открывается окно просмотра сформированного по заданным параметрам отчета (рис. 134). В заголовке отчета указано общее количество выбранных для отчета устройств.

Отчет содержит список устройств, отобранных по указанным параметрам. По умолчанию список устройств отсортирован по типам устройств. Для каждого устройства указано его наименование, общее количество политик и количество политик выбранного при формировании отчета типа (*Избыточные*, *Теневые, Неиспользуемые и/или Нулевые Hit Count*). Если количество политик выбранного типа равно «0», то наименование такого типа не отображается в итоговой строке для устройства.

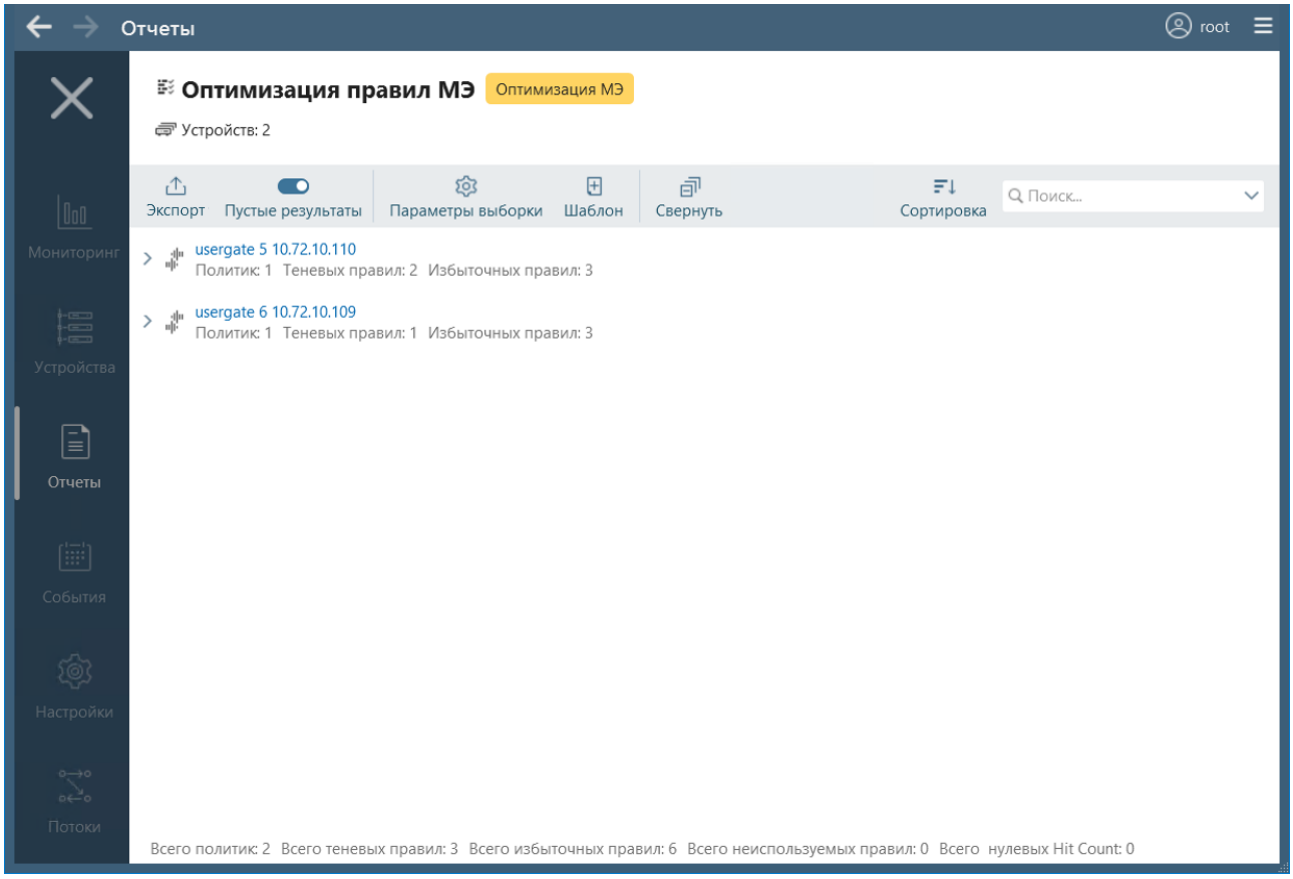


Рисунок 134 – Отчет **Оптимизация правил МЭ**

В нижней части отчета приведено общее количество отобранных политик и общее количество политик для каждого выбранного при формировании отчета типа с учетом нулевых значений.

Если количество отобранных для отчета правил превышает 1000, то устройство в списке устройств после достижения предела отображается, но при этом вместо данных о количестве правил для него отображается текст «*Данные не получены. Достигнуто ограничение в 1000 записей*».

При выборе имени устройства аналогично отчету типа ***Выборка*** (см. рис. 123) открывается карточка устройства, в которой приведены основные сведения о его конфигурации, уровне защищенности, обнаруженных уязвимостях (с учетом наличия скрытых уязвимостей) и количестве уведомлений по типам (отображается информация только об имеющихся уведомлениях). Пользователь имеет возможность в карточке выделить и скопировать данные устройства: имя устройства, адрес, описание (при его наличии в карточке), модель, версию. Из

карточки устройства можно перейти на вкладку ***Статус*** раздела **Устройства**, нажав кнопку ***Перейти к устройству***, расположенную в нижней части карточки.

Для просмотра списка внесенных в отчет правил устройства необходимо нажать в строке требуемого устройства кнопку «›». В соответствии с рисунком 135 в окне отобразятся включенные для устройства проверки с перечнями найденных в них правил выбранного при формировании отчета типа.

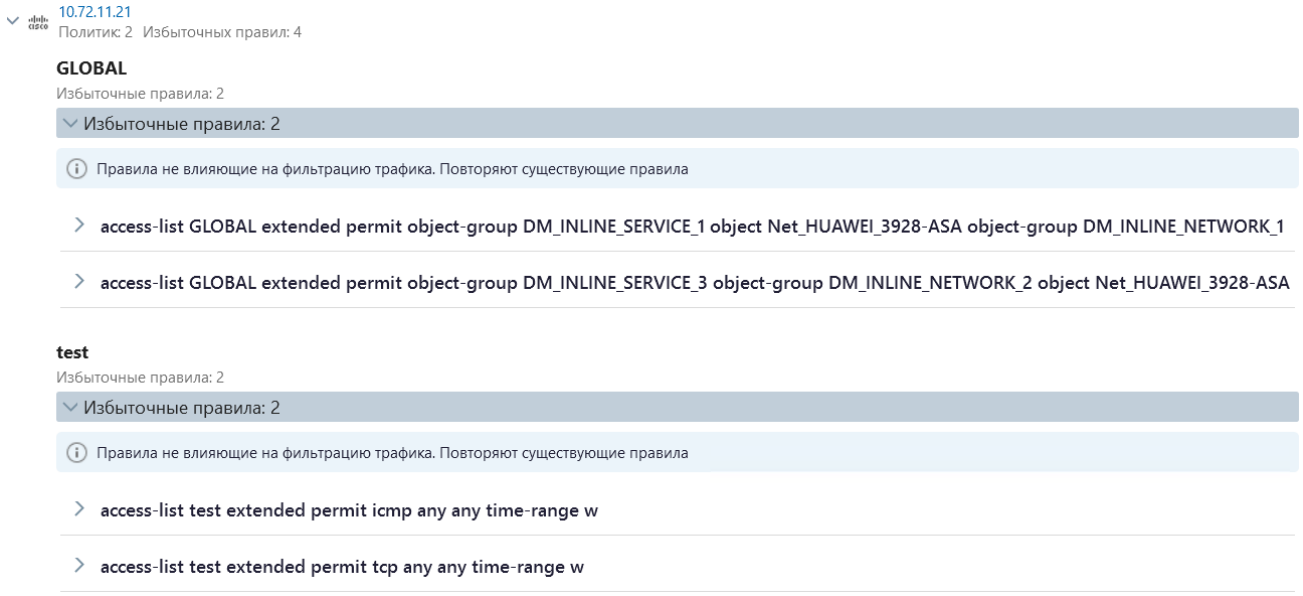


Рисунок 135 – Список правил, внесенных в отчет для устройства

При просмотре отчета пользователю доступны сортировка списка по имени или типу устройств, поиск по имени устройства, настройка отображения устройств с пустыми списками выбранного типа правил, настройка представления отчета с раскрытыми или свернутыми панелями просмотра данных списков проверок с правилами.

2.12.1.1. Ввод параметров отчета и просмотр отчета для типа шаблона *Правила межсетевых экранов*

При выборе типа шаблона ***Правила межсетевых экранов*** открывается окно **Правила межсетевых экранов** (рис. 136). Состав полей окна приведен в таблице 18.

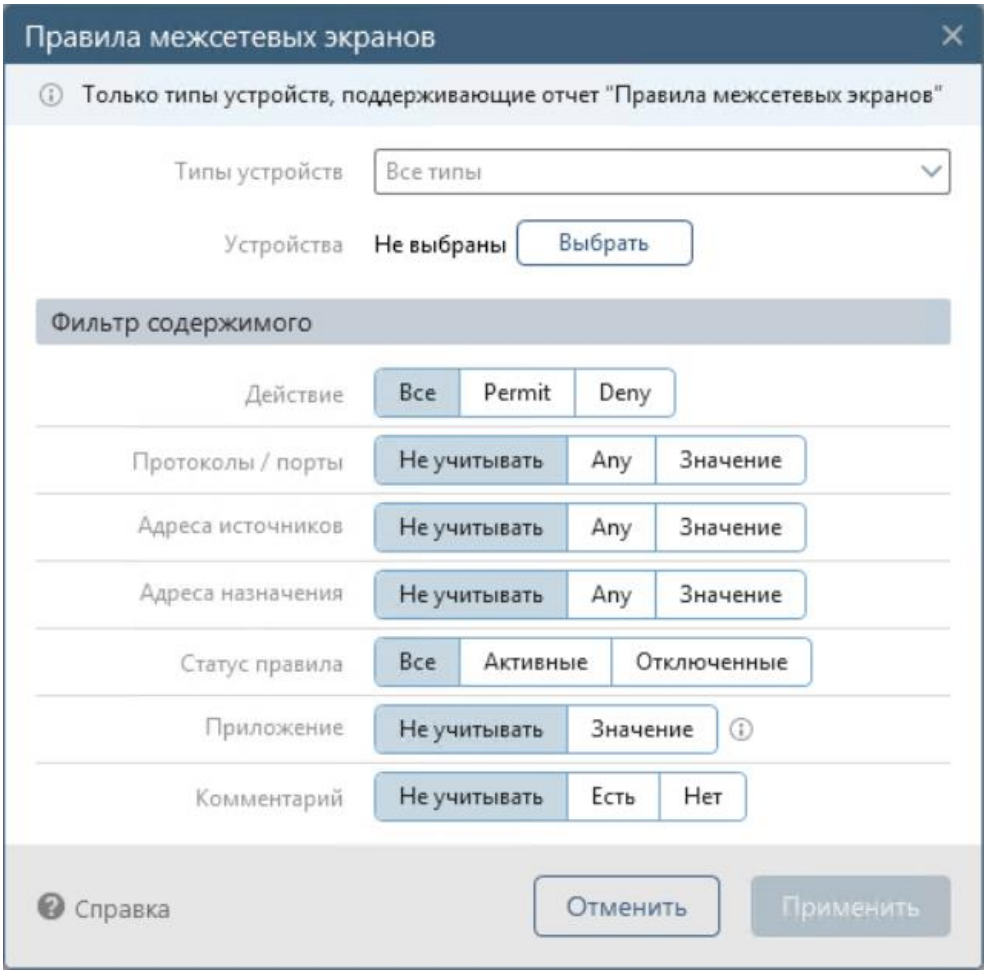


Рисунок 136 – Окно **Правила межсетевых экранов**

Таблица 18 – Состав и описание полей окна **Правила межсетевых экранов**

Поле	Описание/Назначение
Типы устройств	Поле для выбора типов устройств, для которых должен быть сформирован отчет. Содержит список контролируемых сервером ПК типов устройств, поддерживающих отчет ***Правила межсетевых экранов***. Каждому типу устройств соответствует поле для флага. Требуемые типы устройств выбираются установкой флагов
Устройства	Поле для выбора устройств и групп устройств, для которых должен быть сформирован отчет. Выбор выполняется установкой флагов в окне **Выбор устройств**, которое открывается по нажатию кнопки ***Выбрать***. После нажатия в окне выбора кнопки ***Выбрать*** в поле отображается количество выбранных устройств и групп устройств
Блок *Фильтр содержимого*	
Действие	Переключатель для выбора типа указанного во включаемом в отчет правиле действия. При выборе значения: – *Все* – в отчет попадают правила независимо от значения действия правила; – *Permit* – в отчет попадают правила, в которых в качестве действия указано *Permit*;

Поле	Описание/Назначение
	– *Deny* – в отчет попадают правила, в которых в качестве действия указано *Deny*
Протоколы/порты	Переключатель для выбора включаемых в отчет правил по указанным протоколам/портам. При выборе значения: – *Не учитывать* – в отчет попадают правила независимо от значения протоколов/портов правила; – *Any* – в отчет попадают правила, если протокол правила имеет значение *Any*; – *Значение* – в отчет попадают правила, содержащие указанные в проверке значения для протокола и портов. После выбора значения *Значение* в окне дополнительно отображаются поля (рис. 137): – выбора протокола (*TCP*, *UDP*, *TCP/UDP*, *ICMP* или *Другой*); – ввода портов проверки и исключений портов (для протоколов *TCP*, *UDP, TCP/UDP)* или ввода номера IP-протокола (для *Другой протокол*); – исключения из отчета правил со значением *Any* или аналогиных ему (исключение включается установкой флага). Примечание – Справа от полей расположена кнопка ***Информация*** (ⓘ), по нажатию которой открывается окно с правилами заполнения соответствующего поля. При выборе значения *Другой* подсказка содержит ссылку на таблицу интернет-протоколов транспортного уровня с соответствующими им номерами
Адреса источников	Переключатель для выбора включаемых в отчет правил по указанным адресам источников. При выборе значения: – *Не учитывать* – в отчет попадают правила независимо от значения адреса источника; – *Any* – в отчет попадают правила, если адрес источника правила имеет значение Any; – *Значение* – в отчет попадают правила, содержащие все указанные в проверке значения для адресов источников. После выбора значения *Значение* в окне дополнительно отображаются поля (см. рис. 136): – для ввода адресов источников, указанных во включаемом в отчет правиле. В качестве адреса источника могут быть указаны адреса подсетей/диапазоны адресов/адреса хостов; – исключения из отчета правил, если адрес источника правила имеет значение Any или аналогиных ему (исключение включается установкой флага). Примечание – Справа от полей расположена кнопка ***Информация*** (ⓘ), по нажатию которой открывается окно с правилами заполнения соответствующего поля.
Адреса назначения	Переключатель для выбора включаемых в отчет правил по указанным адресам назначения. При выборе значения: – *Не учитывать* – в отчет попадают правила независимо от значения адреса назначения;

Поле	Описание/Назначение
	– *Any* – в отчет попадают правила, если адрес назначения правила имеет значение Any; – *Значение* – в отчет попадают правила, содержащие все указанные в проверке значения для адресов назначения. После выбора значения *Значение* в окне дополнительно отображаются поля (см. рис. 136); – для ввода адресов назначения, указанных во включаемом в отчет правиле. В качестве адреса назначения могут быть указаны адреса подсетей/диапазоны адресов/адреса хостов; – исключения из отчета правил, если адрес назначения правила имеет значение Any или аналогиных ему (исключение включается установкой флага). Примечание – Справа от полей расположена кнопка ***Информация*** (ⓘ), по нажатию которой открывается окно с правилами заполнения соответствующего поля.
Статус правила	Переключатель для статуса правил, включаемых в отчет. При выборе значения: – *Все* – в отчет попадают правила в любом статусе; – *Активные* – в отчет попадают активные правила; – *Отключенные* – в отчет попадают отключенные правила
Приложение	Переключатель для выбора включаемых в отчет правил по указанным приложениям. При выборе значения: – *Не учитывать* – в отчет попадают правила независимо от наличия приложений; – *Значение* – в отчет попадают правила, содержащие хотя бы одно из указанных в проверке приложений. После выбора значения *Значение* в окне дополнительно отображаются (см. рис. 136); – поле для ввода имени приложения (поддерживается ввод имени приложения с учетом регистра и заменой символом «*» любых символов); – кнопка **Добавить** (+) – для добавления поля для ввода имени следующего проверяемого приложения; – кнопка **Удалить** (🗑) – для удаления соответствующего поля с наименованием приложения. Примечание – Справа от поля *Приложение* расположена кнопка ***Информация*** (ⓘ), по нажатию которой открывается окно с правилами заполнения полей
Комментарий	Переключатель для выбора включаемых в отчет правил по наличию комментария. При выборе значения: – *Не учитывать* – в отчет попадают правила независимо от наличия комментария к правилу ACL (при этом не важно поддерживаются на устройстве комментарии к правилам или нет); – *Есть* – в отчет попадают правила при наличии комментариями; – *Нет* – в отчет попадают правила при отсутствии комментария

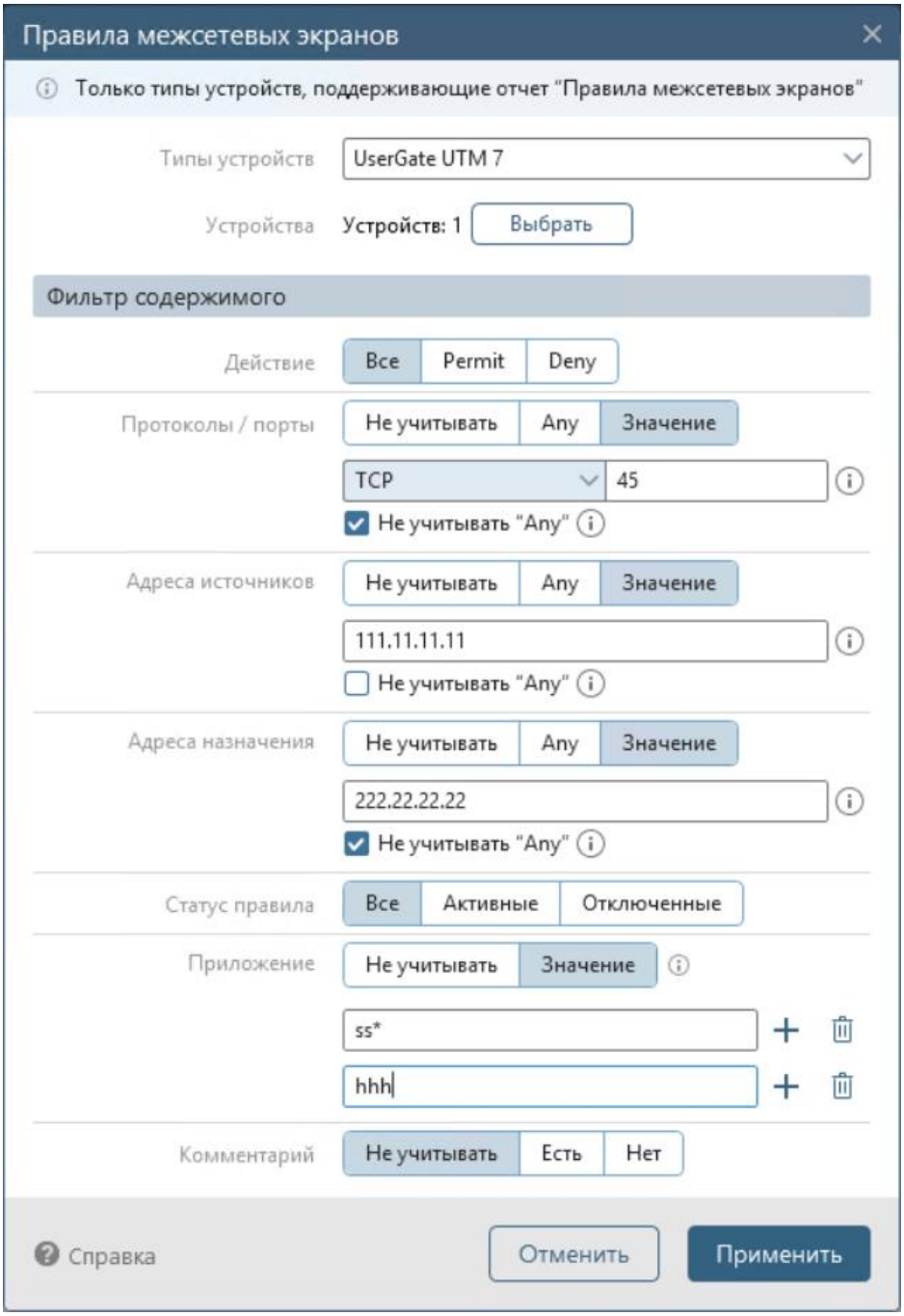


Рисунок 137 – Окно **Правила межсетевых экранов** с дополнительными полями

После задания параметров шаблона (выбора типа устройств и устройств, ввода параметров включаемых в отчет правил) и нажатия кнопки ***Применить*** открывается окно просмотра сформированного по заданным параметрам отчета (рис. 138).

В заголовке отчета указано общее количество выбранных для отчета устройств.

Отчет содержит список устройств, отобранных по указанным параметрам. По умолчанию список устройств отсортирован по типам. Для каждого устройства указано его наименование, количество политик и правил, удовлетворяющих заданным условиям формирования отчета (включая устройства с не найденными по соответствующим параметрам политиками и правилами).

В нижней части отчета приведено общее количество отобранных политик и правил.

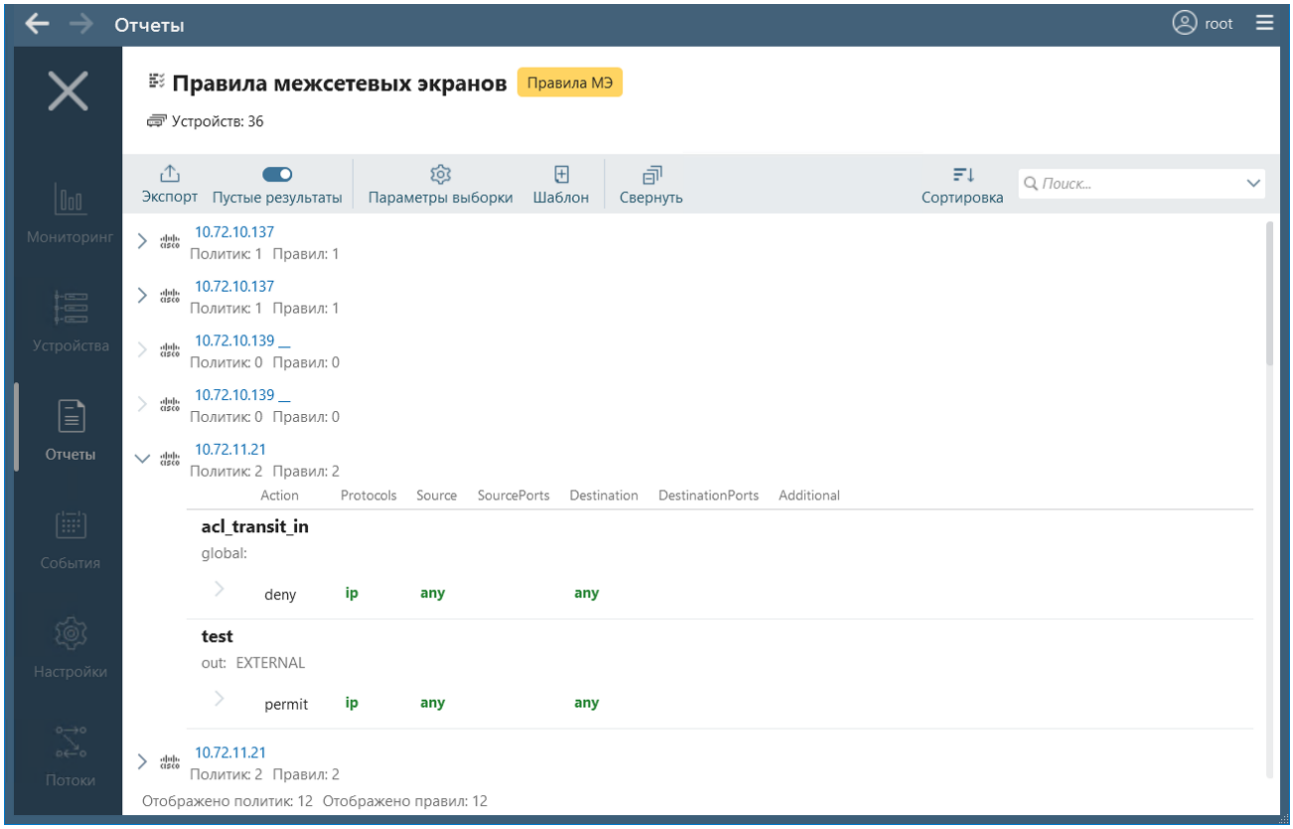


Рисунок 138 – Отчет ***Правила межсетевых экранов***

Если количество отобранных для устройства правил превышает 1000, то для него в отчете отображается только первая 1000 правил, справа от количества правил в скобках отображается сообщение *Достигнут лимит вывода данных, отображены только первые 1000 правил.*

При выборе имени устройства аналогично отчету типа ***Выборка*** (см. рис. 123) открывается карточка устройства, в которой приведены основные сведения о его конфигурации, уровне защищенности, обнаруженных уязвимостях (с учетом наличия скрытых уязвимостей) и количестве уведомлений по типам (отображается информация только об имеющихся уведомлениях). Пользователь имеет возможность в карточке выделить и скопировать данные устройства: имя устройства, адрес, описание (при его наличии в карточке), модель, версию. Из карточки устройства можно перейти на вкладку ***Статус*** раздела **Устройства**, нажав кнопку ***Перейти к устройству***, расположенную в нижней части карточки.

Для просмотра списка внесенных в отчет политик и правил устройства необходимо нажать в строке требуемого устройства кнопку «›». В соответствии с рисунком 136 в окне отобразятся включенные для устройства проверки с перечнями найденных в них правил, удовлетворяющих заданным условиям формирования отчета.

При просмотре отчета пользователю доступны сортировка списка по имени или типу устройств, поиск по имени устройства, настройка отображения устройств с пустыми списками отобранных в отчет политик и правил, настройка представления отчета с раскрытыми или свернутыми панелями просмотра данных списков политик с правилами.

2.12.2. Добавление нового шаблона отчета на основе имеющегося в списке шаблона

Для добавления на сервер ПК нового шаблона отчета на основе имеющегося в списке шаблона (далее – исходный шаблон) необходимо выполнить следующие действия:

1) Перейти в раздел **Отчеты**.
2) Сформировать отчет на основе исходного шаблона (см. п. 2.12.3 «Формирование и просмотр отчетов»).
3) Нажать кнопку ***Шаблон*** ().
4) В раскрывшемся меню выбрать пункт *Сохранить как*.
5) В открывшемся окне **Сохранение шаблона** (пример см. на рис.119):
   - выбрать тип нового шаблона ***Личные*** или ***Общие*** (при наличии прав пользователя на создание общих шаблонов);
   - ввести имя нового шаблона;
   - оставить текущие параметры формирования отчета или внести требуемые изменения в соответствии с правилами, приведенными в п. 2.12.1 «Добавление шаблона отчета»;
   - нажать кнопку ***Сохранить***.

Примечание – Имя нового шаблона должно быть уникальным, запрещено использовать имена уже существующих на сервере ПК шаблонов в разделе **Отчеты**.

Созданный шаблон в зависимости от его типа и прав доступа пользователя (см. п. 2.12 «Просмотр отчетов в разделе Отчеты») доступен для редактирования его параметров, удаления и повторного запуска формирования отчета по шаблону всем пользователям или создавшему шаблон пользователю.

2.12.3. Формирование и просмотр отчетов

Правила первичного формирования и просмотра отчета приведены в п. 2.12.1 «Добавление шаблона отчета и первичный просмотр отчета».

Для формирования и просмотра отчета на основе созданного ранее шаблона пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Отчеты** клиентской консоли.
2) Найти требуемый шаблон.
3) Дважды кликнуть по наименованию шаблона либо в строке шаблона нажать кнопку ***Меню*** (), в раскрывшемся меню выбрать пункт ***Выполнить на основе*** и в открывшемся окне настройки параметров шаблона нажать кнопку ***Применить***. Откроется окно просмотра сформированного по заданным параметрам отчета, аналогичное окну просмотра отчета при его первичном формировании, с актуальными на текущий момент времени данными. В заголовке отчета отображается имя выбранного шаблона.

При просмотре отчета пользователь имеет возможность:

1) Изменить параметры просматриваемого отчета без внесения изменений в шаблон, для чего:
   - нажать кнопку **Параметры выборки** ();

- в открывшемся окне настройки параметров отчета внести требуемые изменения;
- нажать кнопку ***Применить***.

2) Сохранить внесенные в параметры отчета изменения в шаблон, для чего:

- нажать кнопку ***Шаблон*** ();
- в раскрывшемся меню выбрать пункт ***Сохранить***.

3) Создать новый шаблон отчета (см. п. 2.12.3 «Добавление нового шаблона отчета на основе имеющегося в списке шаблона»).

2.12.4. Изменение шаблона отчета

Для внесения изменений в параметры шаблона пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Отчеты** клиентской консоли.
2) Найти требуемый шаблон.
3) Нажать в строке шаблона кнопку ***Изменить*** ().
4) В открывшемся окне настройки параметров шаблона ***Сохранение шаблона*** (см. рис. 119) изменить имя шаблона, внести требуемые изменения в параметры формирования отчета в соответствии с правилами, приведенными в п. 2.12.1 «Добавление шаблона отчета».

Примечание – Поле ***Тип шаблона*** неактивно, изменение типа шаблона – не доступно.

5) Нажать кнопку ***Сохранить***.

Примечание – При внесении изменений в имя шаблона необходимо учитывать, что новое имя не должно повторять имена уже существующих на сервере ПК шаблонов в разделе **Отчеты**.

2.12.5. Удаление шаблона отчета

Удалять шаблоны отчетов типа ***Личные*** могут все пользователи, шаблоны типа ***Общие*** – только пользователи с правами *Управление* (см. п. 1.2).

Для удаления шаблона отчета пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Отчеты** клиентской консоли.
2) Найти требуемый шаблон.
3) В строке шаблона нажать кнопку ***Меню*** (), в раскрывшемся меню выбрать пункт ***Удалить*** и в открывшемся окне подтверждения удаления нажать кнопку ***Удалить***. Шаблон будет удален из списка шаблонов раздела **Отчеты**.

3. Действия после сбоев и ошибок при эксплуатации

При эксплуатации ПК «Efros Config Inspector» v.4 возможно возникновение следующих сбоев и ошибок:

- сбой функционирования сетевых служб;
- сбой после вмешательства посторонних лиц в ПК «Efros Config Inspector» v.4;
- сбой в работе сервера ПК «Efros Config Inspector» v.4;
- сбои и ошибки СУБД;
- сбой клиентской консоли ПК «Efros Config Inspector» v.4.

3.1. Сбой функционирования сетевых служб

Возможны следующие сбои функционирования сетевых служб:

1) В случае сбоя сетевого соединения между клиентской консолью и сервером ПК отобразится сообщение в соответствии с рис. 139. Пользователю следует сообщить о данном факте администратору ПК «Efros Config Inspector» v.4 и администратору сети. Администратор ПК «Efros Config Inspector» v.4 совместно с администратором сети осуществляет восстановление сбоя сетевых служб.

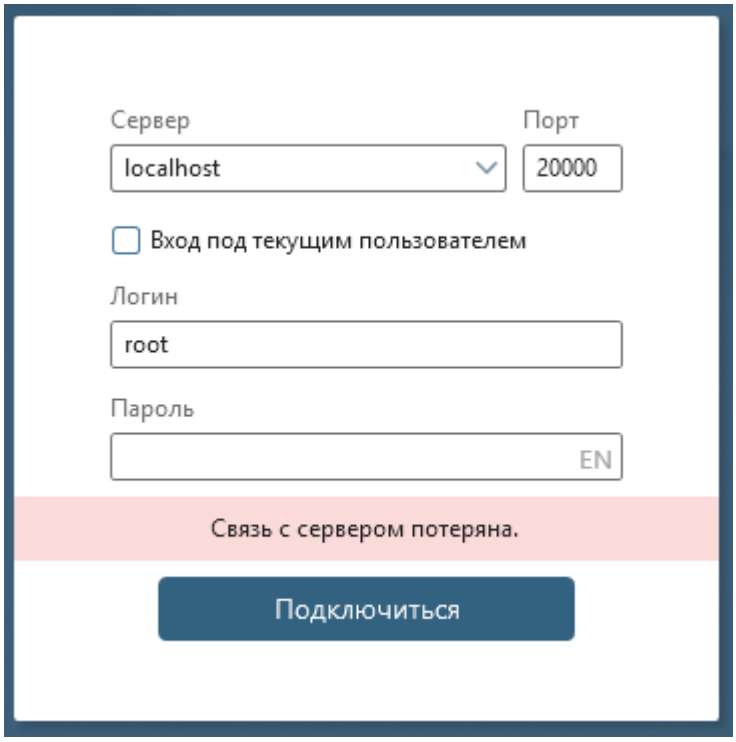


Рисунок 139 – Ошибка сетевого соединения между клиентской консолью и сервером ПК

2) В случае сбоя сетевого соединения между ПК «Efros Config Inspector» v.4 и контролируемыми устройствами в консоли изменится статус устройства на *Нет связи*. Пользователю следует сообщить о данном факте администратору ПК «Efros

Config Inspector» v.4 и администратору сети. Администратор ПК «Efros Config Inspector» v.4 совместно с администратором сети осуществляет восстановление сбоя сетевых служб.

В случае отсутствия доступа по портам, следует сообщить о данном факте администратору средств сетевой безопасности.

3.2. Сбой после вмешательства посторонних лиц в ПК «Efros Config Inspector» v.4

Возможны следующие сбои после вмешательства посторонних лиц в ПК «Efros Config Inspector» v.4:

1) В случае обнаружения при очередной проверке, выполняемой комплексом в автоматическом режиме, нарушения целостности компонентов комплекса: сервера ПК, windows-агентов, коллекторов, клиентской консоли, в клиентской консоли отобразится уведомление (пример см. на рис. 140). Запись об обнаружении нарушения будет также занесена в журнал событий раздела **События**.

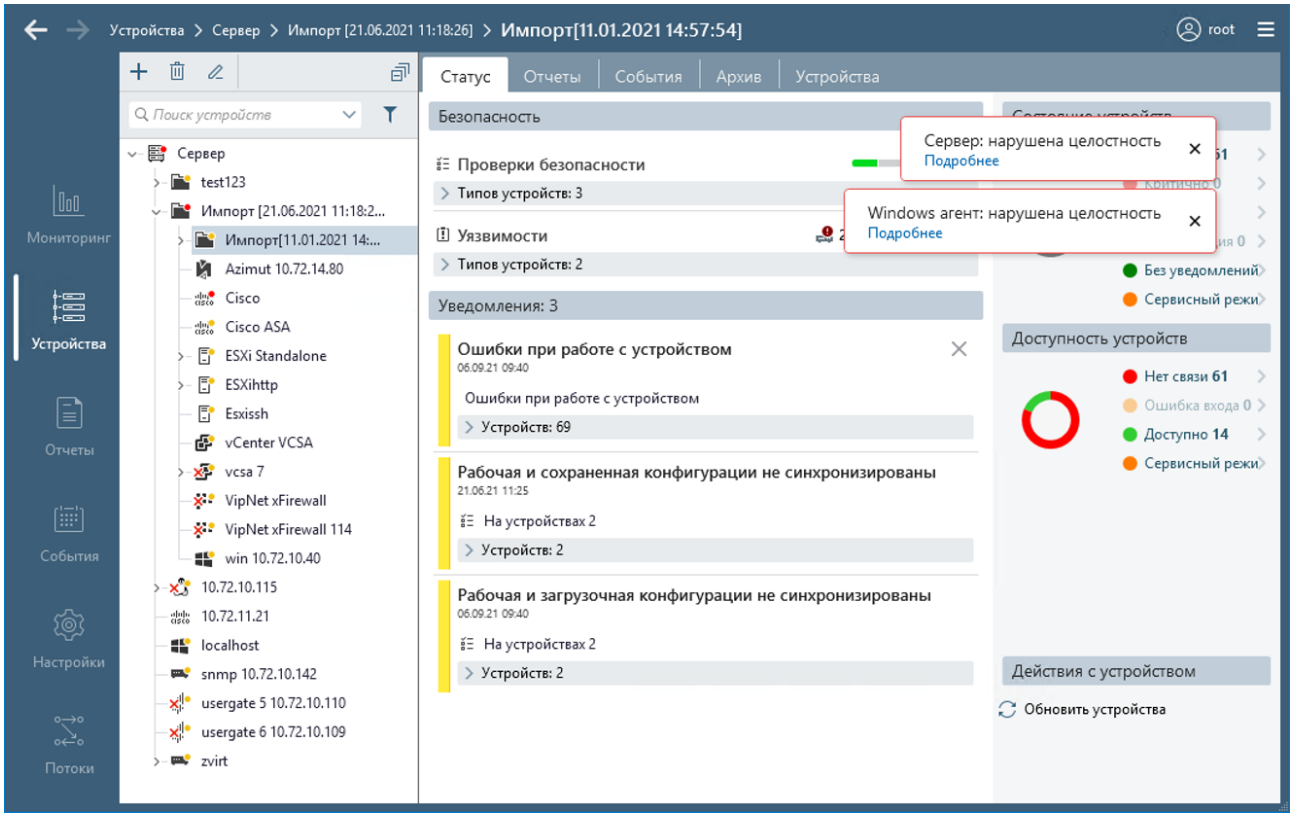


Рисунок 140 – Уведомления об обнаружении нарушения КЦ компонентов комплекса

Пользователь имеет возможность просмотреть перечень обнаруженных нарушений, нажав ссылку ***Подробнее*** (рис. 141). Возможные варианты нарушений: «нарушена целостность файла: <наименование файла>», «файл не найден: <наименование файла>», «неизвестный файл: <наименование файла>».

Если обнаруженные нарушения не связаны с плановыми изменениями компонентов комплекса, то пользователю следует сообщить о данном факте администратору ПК «Efros Config Inspector» v.4 и администратору сетевой безопасности. Администратор

ПК «Efros Config Inspector» v.4 совместно с администратором сетевой безопасности принимают меры в соответствии с корпоративной политикой безопасности.

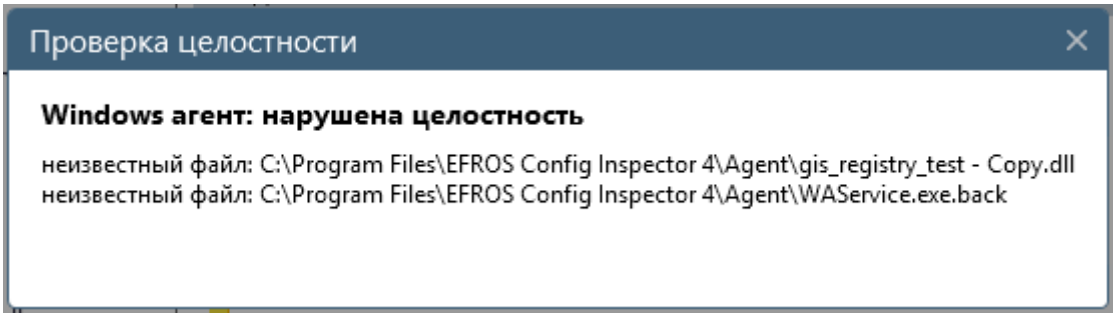


Рисунок 141 – Окно просмотра перечня обнаруженных нарушений при контроле КЦ компонента комплекса

2) В случае обнаружения несоответствия существующих настроек ПК «Efros Config Inspector» v.4 проектным настройкам пользователю необходимо проинформировать администратора ПК «Efros Config Inspector» v.4 с правами настройки контроля устройств (с правами *Управление* в категории *Настройки контроля*) о факте нарушения.

После этого администратор приводит настройки ПК «Efros Config Inspector» v.4 в соответствие с настройками, указанными в эксплуатационной документации.

3.3. Сбой в работе сервера ПК «Efros Config Inspector» v.4 или СУБД

В случае сбоя работоспособности сервера ПК «Efros Config Inspector» v.4 или СУБД, пользователь не сможет выполнить запуск клиентской консоли, пользователю необходимо обратиться к администратору ПК «Efros Config Inspector» v.4.

Администратору ПК «Efros Config Inspector» v.4 необходимо перезапустить службу «Efros Config Inspector» в соответствии с документом «643.72410666.00082-01 95 01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство администратора»

3.4. Сбой консоли управления ПК «Efros Config Inspector» v.4.

3.4.1. Ошибки идентификации

Сообщения об ошибках идентификации будут направлены пользователю в случае отсутствия соответствующих привилегий для их выполнения:

– отказ на получение доступа к серверу ПК.

Доступ к приложению ПК «Efros Config Inspector» v.4 будет невозможен в случаях:

– неверно указаны данные серверной части ПК «Efros Config Inspector» v.4 для подключения (IP-адрес/DNS-имя или порт);
– неверно указан идентификатор пользователя (логин);
– неверно указаны аутентификационные данные пользователя (пароль);
– превышено количество попыток неверного ввода пароля пользователя;

– учетная запись пользователя заблокирована в ПК «Efros Config Inspector» v.4.

При получении сообщения о неверно введенных аутентификационных данных (рис. 142) при подключении к серверу ПК необходимо проверить правильность введения логина пользователя и пароля. В случае ошибочного введения повторно ввести аутентификационные данные пользователя и нажать кнопку ***Подключиться***.

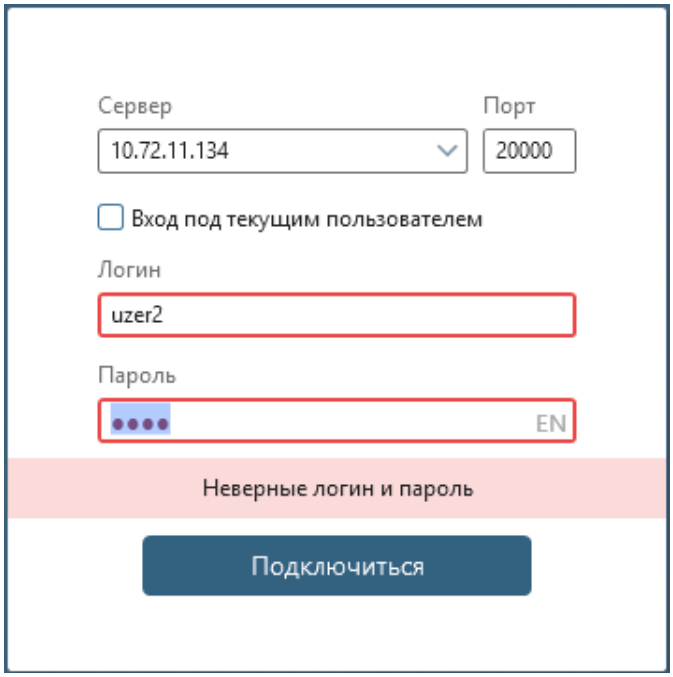


Рисунок 142 – Окно подключения к серверу ПК после ввода неверных данных пользователя

При получении сообщения о временной блокировке IP-адреса после нескольких подряд попытках (от 3 до 8) неверного ввода аутентификационных данных пользователя (рис. 143) при подключении к серверу ПК необходимо либо дождаться завершения периода блокирования (от 10 до 60 минут) и повторить попытку подключения к серверу ПК, либо обратиться к администратору ПК «Efros Config Inspector» v.4 для проверки аутентификационных данных или смены пароля.

Примечание – Параметры *Количество попыток неверного ввода пароля пользователя* и *Время блокирования IP-адреса* настраиваются администратором ПК «Efros Config Inspector» v.4.

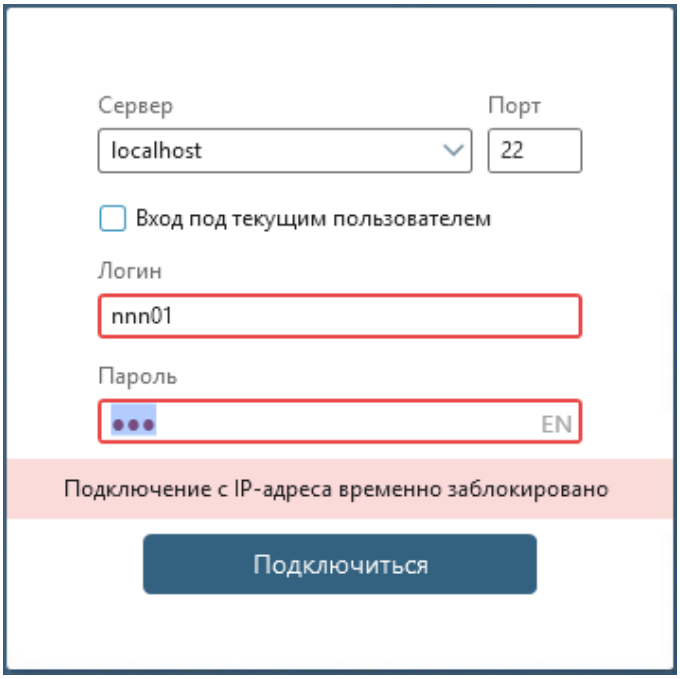


Рисунок 143 – Окно подключения к серверу ПК после превышения количества попыток неверного ввода аутентификационных данных пользователя

При получении сообщения о блокировке учетной записи пользователя (рис. 144) при подключении к серверу ПК необходимо обратиться к администратору ПК «Efros Config Inspector» v.4 для разблокирования учетной записи.

Примечание – Учетная запись пользователя может быть заблокирована как администратором ПК «Efros Config Inspector» v.4, так и в автоматическом режиме при превышении периода времени неиспользования учетной записи для работы с ПК «Efros Config Inspector» v.4 (от 1 до 90 дней). Параметр *Период времени неиспользования* настраивается администратором ПК «Efros Config Inspector» v.4.

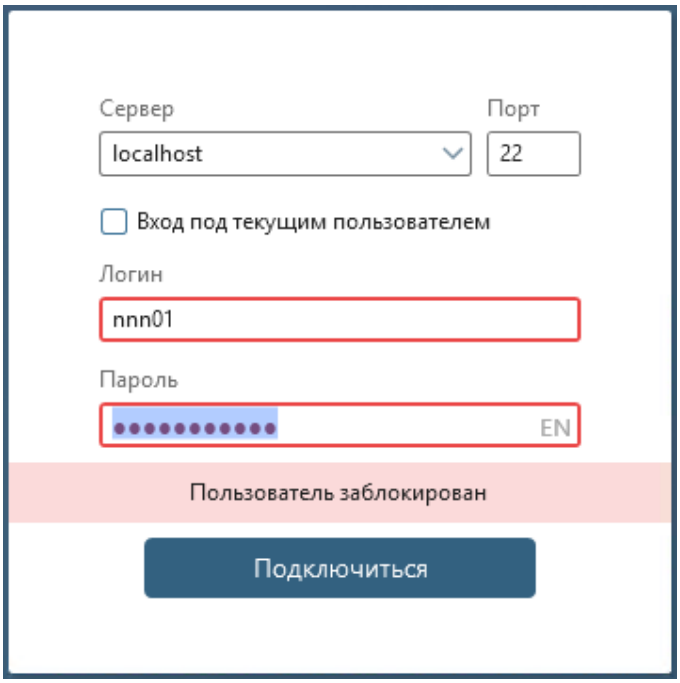


Рисунок 144 – Окно подключения к серверу ПК после ввода аутентификационных данных заблокированного пользователя

3.4.2. Ошибки смены пароля пользователя

При попытке смены пароля пользователем, если:

1) Введен неверный текущий пароль, то поле **Текущий пароль** окна смены пароля будет выделено рамкой красного цвета и при наведении на поле курсора будет отображаться сообщение *Пароль не верный.*

2) Введенный новый пароль не соответствует заданным при настройке ПК «Efros Config Inspector» v.4 требованиям к его сложности, то поле **Новый пароль** будет выделено рамкой красного цвета. Возможные нарушения:

- длина пароля меньше требуемой;
- в пароле отсутствуют буквы верхнего или нижнего регистра;
- в пароле отсутствуют цифры или спецсимволы;
- пароль начинается с имени пользователя;
- пароль ранее был использован пользователем;
- пароль отличается от предыдущего менее чем на три символа;
- пароль находится в списке популярных паролей.

3) Ведены разные пароли в поля **Новый пароль** и **Повторите пароль,** то поле **Повторите пароль** окна смены пароля будет выделено рамкой красного цвета и при наведении на поле курсора будет отображаться сообщение *Пароли не соответствуют.*

Пользователю необходимо корректно заполнить поля окна смены пароля и нажать кнопку ***Сохранить***. Если пользователь забыл текущий пароль, то ему необходимо обратиться к администратору ПК «Efros Config Inspector» v.4.

3.4.3. Ошибки управления доступом

Сообщения об ошибках будут направлены пользователю в случае отсутствия соответствующих привилегий для их выполнения:

- отказ на получение доступа к серверу ПК;
- выполнен вход с иными правами.

Пользователю при попытке выполнения действия, не доступного в соответствии с назначенными пользователю правами, будет выведено сообщение «Доступ запрещен».

При выполнении доступных действий по формированию списка устройств, настройке контроля устройств, формированию шаблонов пользовательских отчетов также могут быть выведены информационные сообщения, связанные с некорректным указанием данных при выполнении действий. Возможные информационные сообщения:

- «Обязательное поле»;
- «Обязательные поля»;
- «Поле должно содержать не менее X символов»;
- «Пароль может содержать только: латинские буквы обоих регистров, цифры, спец. символы (! @ # & ( ) - _ [{ }] : ; ', ? / * ~ $ ^ + = < >)»;
- «Поле должно быть корректным: '0-255.0-255.0-255.0-255' или '0-255.0-255.0-255.0-255/32'»;

– иные, в зависимости от контекста выполняемых действий.

3.4.4. Ошибки в работе консоли

В случае возникновения сбоев в работе клиентской консоли или возникновения ошибки, препятствующей дальнейшей работе программы (интерфейс клиентской консоли не реагирует на действия пользователя), необходимо завершить работу приложения принудительно с помощью диспетчера задач ОС и запустить снова в соответствии с п. 2.1 настоящего Руководства.

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, позволяющий производить удаленное управление и туннелирование TCP-соединений
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
НКЦКИ	–	Национальный координационный центр по компьютерным инцидентам
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 комплексом по результатам проверки загруженных или выбранных данных на соответствие заданным правилам

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

Базовый профиль – Профиль, предустановленный в комплексе

Родительский профиль – Профиль, настройки которого копируются при создании/редактировании другого профиля. Наследованные настройки родительского профиля могут быть изменены только после отмены режима наследования в формах изменения настройки отчетов, проверок и т.д.

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

Приложение 1

(справочное)

Регулярные выражения стандарта PCRE, допустимые к применению в ПК «Efros Config Inspector» v.4

Регулярные выражения – формальный язык поиска и осуществления манипуляций с подстроками в тексте, основанный на использовании метасимволов. Для поиска используется строка-образец, состоящая из символов и метасимволов и задающая правило поиска (см. таблицу П.1).

Таблица П.1 – Пример поиска символов

Символ	Описание	Пример	Соответствие
Обычный	Все символы, кроме специальных. Соответствуют сами себе	а	М**а**ма мыл**а** р**а**му
		от	**от** к**от**а
		12	(8**12**) 3**12**-24-67

Большинство символов в регулярном выражении представляют сами себя за исключением специальных символов **[ ] { } ( ) \ | . ? * $ ^ +** (см. таблицу П.2).
Для того, чтобы использовать эти символы в качестве текста, их необходимо экранировать символом **** (обратная косая черта).

Таблица П.2 – Примеры использования специальных символов

Символ	Описание	Пример	Соответствие
^	Начало строки	^a	**а**аа ааа
$	Конец строки	a$	ааа аа**а**
\b	Граница слова	\ba	**а**аа **а**аа
		a\b	аа**а** аа**а**
\B	Не граница слова	\Ba\B	а**а**а а**а**а
\G	Предыдущий успешный поиск	\Ga	**ааа** ааа (поиск остановился на четвертой позиции – там, где не нашлось а)
		\Gаха-	**аха-аха-**аха последнее «аха» не будет захвачено, т.к. успешный поиск состоит из «аха-»
.	Любой символ, кроме символа новой строки \n	к.т	**кот**, **кит**, **кат**ок

Также, вместо символа «**.**» можно использовать **[\s\S]** – это все пробельные и непробельные символы, включая символ новой строки «**\n**».

Символьные классы

Набор символов в квадратных скобках **[ ]**, позволяет указывать, что на данном месте в строке может стоять один из перечисленных символов (см. таблицу П.3). Например, **[абв]** задаёт возможность появления в тексте одного из трёх указанных символов, а **[1234567890]** задает соответствие одной из цифр. Так же возможно указание диапазона символов, **[А-Яа-я]** соответствует всем буквам русского алфавита, за исключением **ё** и **Ё**. Если требуется указать символы, которые не входят в набор, то используется символ «**^**» внутри квадратных скобок. Например, **[^0-9]** означает любой символ кроме цифр.
Некоторые символьные классы можно заменить специальными метасимволами:

Таблица П.3 – Регулярные выражения с использованием квадратных скобок

Символ	Эквивалент	Соответствие
\d	[0-9]	Цифровой символ
\D	[^0-9]	Не цифровой символ
\s	[\f\n\r\t\v]	Пробельный символ
\S	[^ \f\n\r\t\v]	Непробельный символ
\w	[[:word:]]	Буквенный или цифровой символ или знак подчеркивания
\W	[^[:word:]]	Любой символ, кроме буквенного или цифрового символа или знака подчеркивания

Обозначения пробельных символов:
\f – разрыв страницы
\n – перевод строки
\r – возврат каретки
\t – горизонтальная табуляция
\v – вертикальная табуляция

Квантификация (поиск последовательностей)

Квантификатор после символа, символьного класса или группы определяет, сколько раз предшествующее выражение может встречаться (см. таблицу П.4). Следует учитывать, что квантификатор может относиться более чем к одному символу в регулярном выражении, только если это символьный класс или группа.

Таблица П.4 – Примеры использования квантификаторов

Символ	Описание	Пример	Соответствие
*	Ноль или более. Эквивалент {0,}	сто*	**сто**, **стоо**, **стооо**, **ст**
+	Один или более раз. Эквивалентно {1,}	сто+	**сто**, **стоо**, **стооо**, ст
?	Ноль или одно. Эквивалент {0,1}	сто?	**сто**, **сто**о, **сто**оо, **ст**
{n}	Ровно n раз	сто{3}	сто, стоо, **стооо**
{m,n}	От m до n включительно	сто{2,3}	сто, **стоо**, **стооо**, стоооо
{m,}	Не менее m	сто{2,}	сто, **стоо**, **стооо**, **стоооо**

Символ	Описание	Пример	Соответствие
{,n}	Не более n	сто{,3}	**сто**, **стоо**, **стооо**, стоооо

Если символы **{ }** не образуют квантификатора, их специальное значение игнорируется.
Часто используется последовательность «**.***» (точка, звездочка) или «**.*?**» (точка, звездочка, вопросительный знак) для обозначения любого количества любых символов между двумя частями регулярного выражения (подробнее см. ниже в подразделе «Жадная и ленивая квантификация»).

Жадная и ленивая квантификация

В некоторых реализациях квантификаторам в регулярных выражениях соответствует максимально длинная строка из возможных. Это может оказаться значительной проблемой. Например, часто ожидают, что выражение (**<.*>**) найдёт в тексте теги HTML. Однако, если в тексте есть более одного HTML-тега, то этому выражению соответствует целиком строка, содержащая множество тегов.
Текст для примера, «жадной» и «ленивой» квантификации.
Эту проблему можно решить двумя способами.
Учитывать символы, не соответствующие желаемому образцу (**<[^>]*>** для вышеописанного случая).
Определить квантификатор как «ленивый» – большинство реализаций позволяют это сделать, добавив после него знак вопроса.
Использование «ленивых» квантификаторов может повлечь за собой обратную проблему, когда выражению соответствует слишком короткая, в частности, пустая строка. Если необходимо, чтобы выражение нашло как минимум один символ, то вместо ***** нужно использовать **+**.
Чтобы выделить отдельные теги, можно применить «ленивую» версию этого выражения: (**<.*?>**)
Ей соответствует не вся показанная выше строка, а отдельные теги
Текст для примера, жадной и ленивой квантификации.
В таблице П.5 приведены символы «жадной» и «ленивой» квантификации.

Таблица П.5 – Символы «жадной» и «ленивой» квантификации

Жадный	Ленивый
*	*?
+	+?
{n,}	{n,}?

Перечисление

Вертикальная черта разделяет допустимые варианты. Например, **a | b** соответствует **a** или **b**. Следует помнить, что перебор вариантов выполняется слева направо, как они указаны.
Если требуется указать перечень вариантов внутри более сложного регулярного выражения, то его нужно заключить в группу. Например, **gray | grey** или **gr (a|e) y** описывают строку **gray** или **grey**. В случае с односимвольными альтернативами

предпочтителен вариант **gr [ae] y**, так как сравнение с символьным классом выполняется проще, чем обработка группы с проверкой на все её возможные модификаторы и генерацией обратной связи.

Обратная связь

Одно из применений группировки – повторное использование ранее найденных групп символов (подстрок, блоков, отмеченных подвыражений, захватов). При обработке выражения подстро́ки, найденные по шаблону внутри группы, сохраняются в отдельной области памяти и получают номер, начиная с единицы. Каждой подстроке соответствует пара скобок в регулярном выражении. Квантификация группы не влияет на сохранённый результат, то есть, сохраняется лишь первое вхождение. Обычно поддерживается до 9 нумерованных подстрок с номерами от 1 до 9, но некоторые интерпретаторы позволяют работать с бо́льшим количеством. Впоследствии в пределах данного регулярного выражения можно использовать обозначения от **\1** до **\9** для проверки на совпадение с ранее найденной подстрокой.

Например, регулярное выражение **(та|ту)-\1** найдёт строку **та-та** или **ту-ту**, но пропустит строку **та-ту**.

Также ранее найденные подстроки можно использовать при замене по регулярному выражению. В таком случае в замещающий текст вставляются те же обозначения, что и в пределах самого выражения.

Группировка

Примеры использования группировки приведены в таблице П.6.

Таблица П.6 – Примеры использования группировки

Символ	Описание	Пример	Соответствие
( )	Для группировки. Шаблон внутри как единое целое. может быть квантифицирован	(ab){3}	abc**ababab**cdab
(?:шаблон)	Группировка без обратной связи. Не будет создавать групп	a(?:bc|b|x)cc	**abcc**axcc, abcc**axcc**
		здра(?:сти|вствуйте)	если требуется найти или «здравствуйте», или «здрасти», но не важно, какое именно приветствие найдено
(?>шаблон)	Атомарная группировка, запрещает возвращаться назад по строке, если часть шаблона уже найдена	a(?>bc|b|x)cc	abcc**axcc** но не **abcc**axcc: вариант x найден, остальные проигнорированы

Просмотр вперёд и назад

В большинстве реализаций регулярных выражений есть способ производить поиск фрагмента текста, «просматривая» (но не включая в найденное) окружающий текст,

который расположен до или после искомого фрагмента текста. Просмотр с отрицанием используется реже и «следит» за тем, чтобы указанные соответствия, напротив, не встречались до или после искомого текстового фрагмента (см. таблицу П.7).

Таблица П.7 – Перечень файлов для постановки на контроль

Представление	Вид просмотра	Пример	Соответствие
(?=шаблон)	Позитивный просмотр вперёд	Людовик(?=XVI)	ЛюдовикXV, **Людовик**XVI, **Людовик**XVIII, ЛюдовикLXVII, ЛюдовикXXL
(?!шаблон)	Негативный просмотр вперёд (с отрицанием)	Людовик(?!XVI)	**Людовик**XV, ЛюдовикXVI, ЛюдовикXVIII, **Людовик**LXVII, **Людовик**XXL
(?<=шаблон)	Позитивный просмотр назад	(?<=Сергей)Иванов	Сергей **Иванов**, Игорь Иванов
(?<!шаблон)	Негативный просмотр назад (с отрицанием)	(?<!Сергей)Иванов	Сергей Иванов, Игорь **Иванов**

Приложение 2

(рекомендуемое)

Список файлов, рекомендуемых производителями устройств для постановки на контроль целостности в ПК «Efros Config Inspector» v.4

Многие производители оборудования (операционных систем) рекомендуют ставить на контроль целостности файлы, несанкционированное изменение которых может нарушить корректную работу их оборудования. Список таких файлов в зависимости от типа оборудования (операционной системы) приведен в таблице П.8.

Таблица П.8 – Перечень файлов для постановки на контроль

Наименование шаблона отчета	Контролируемые файлы
VMware ESXi файлы	– */etc/vmware/hostd/config.xml;* – */etc/hosts;* – */etc/motd;* – */etc/openwsman/openwsman.conf;* – */etc/pam.d/passwd;* – */etc/vmware/hostd/proxy.xml;* – */etc/sfcb/sfcb.cfg;* – */etc/vmware/snmp.xml;* – */etc/ssh/sshd_config;* – */etc/ssh/ssh_host_dsa_key;* – */etc/ssh/ssh_host_dsa_key.pub;* – */etc/ssh/ssh_host_rsa_key;* – */etc/ssh/ssh_host_rsa_key.pub;* – */etc/ssh/keys-root/authorized_keys;* – */etc/vmware/ssl/rui.crt;* – */etc/vmware/ssl/rui.key;* – */etc/vmware/config;* – */etc/vmware/configrules;* – */etc/syslog.conf*
Linux файлы	– */bin/*;* – */etc/*.conf;* – */etc/*.config;* – */etc/*_conf;* – */etc/*_config;* – */etc/cron.d/logchecker;* – */etc/fs/*;* – */etc/sudoers;* – */lib/*.a;* – */lib/*.cfg;* – */lib/*.com;* – */lib/*.d;* – */lib/*.kdb;* – */lib/*.ksh;* – */lib/*.sh;* – */lib/*.so32;* – */lib/*.so64;*

Наименование шаблона отчета	Контролируемые файлы
	– */lib/*.tcl;* – */lib/*.vc;* – */lib/boot/*;* – */lib/drivers/*;* – */lib/objrepos/*;* – */lib/security/*;* – */lib/svc/nfs/lockd;* – */lib/svc/nfs/statd;* – */opt/sbin/in.named;* – */opt/sbin/lwresd;* – */opt/sbin/name;* – */sbin/*;* – */usr/bin/*;* – */usr/lib/*.a;* – */usr/lib/*.cfg;* – */usr/lib/*.com;* – */usr/lib/*.d;* – */usr/lib/*.ksh;* – */usr/lib/*.sh;* – */usr/lib/*.so32;* – */usr/lib/*.so64;* – */usr/lib/*.tcl;* – */usr/lib/*.vc;* – */usr/local/sbin/in.named;* – */usr/local/sbin/in.tnamed;* – */usr/local/sbin/lwresd;* – */usr/local/sbin/named;* – */usr/local/sbin/sshd;* – */usr/sbin/** **Исключения:** – */*.bmp;* – */*.gif;* – */*.gl;* – */*.gz;* – */*.help;* – */*.info;* – */*.jar;* – */*.log;* – */*.msg;* – */*.out;* – */*.pm;* – */*.ppm;* – */*.tar;* – */*.tpl;* – */*.txt;* – */*.xml;* – */*.xsd;* – */etc/*.log;* – */etc/tpvmlp.conf;* – */lib/font/*;*

Наименование шаблона отчета	Контролируемые файлы
	– /lib/lpd/pio/trans2/*; – /lib/nls/loc/*; – /lib/nls/msg/*; – /lib/tcl8.4/encoding/*; – /lib/tk8.4/demos/*; – /usr/lib/cron/log; – /usr/lib/font/*; – /usr/lib/nls/loc/*; – /usr/lib/nls/msg/*; – /usr/lib/objrepos/*; – /usr/lib/tcl8.4/encoding/*; – /usr/sbin/perf/*; – /usr/sbin/vsftpd
SunOS файлы	– /bin/*; – /etc/*.conf; – /etc/*.config; – /etc/*_conf; – /etc/*_config; – /etc/cron.d/logchecker; – /etc/fs/*; – /etc/sudoers; – /lib/*.a; – /lib/*.cfg; – /lib/*.com; – /lib/*.d; – /lib/*.kdb; – /lib/*.ksh; – /lib/*.sh; – /lib/*.so32; – /lib/*.so64; – /lib/*.tcl; – /lib/*.vc; – /lib/boot/*; – /lib/drivers/*; – /lib/objrepos/*; – /lib/security/*; – /lib/svc/nfs/lockd; – /lib/svc/nfs/statd; – /opt/sbin/in.named; – /opt/sbin/lwresd; – /opt/sbin/name; – /sbin/*; – /usr/bin/*; – /usr/lib/*.a; – /usr/lib/*.cfg; – /usr/lib/*.com; – /usr/lib/*.d; – /usr/lib/*.ksh; – /usr/lib/*.sh;

Наименование шаблона отчета	Контролируемые файлы
	– */usr/lib/*.so32;* – */usr/lib/*.so64;* – */usr/lib/*.tcl;* – */usr/lib/*.vc;* – */usr/local/sbin/in.named;* – */usr/local/sbin/in.tnamed;* – */usr/local/sbin/lwresd;* – */usr/local/sbin/named;* – */usr/local/sbin/sshd;* – */usr/sbin/** **Исключения:** – */*.bmp;* – */*.gif;* – */*.gl;* – */*.gz;* – */*.help;* – */*.info;* – */*.jar;* – */*.log;* – */*.msg;* – */*.out;* – */*.pm;* – */*.ppm;* – */*.tar;* – */*.tpl;* – */*.txt;* – */*.xml;* – */*.xsd;* – */etc/*.log;* – */etc/tpvmlp.conf;* – */lib/font/*;* – */lib/lpd/pio/trans2/*;* – */lib/nls/loc/*;* – */lib/nls/msg/*;* – */lib/tcl8.4/encoding/*;* – */lib/tk8.4/demos/*;* – */usr/lib/cron/log;* – */usr/lib/font/*;* – */usr/lib/nls/loc/*;* – */usr/lib/nls/msg/*;* – */usr/lib/objrepos/*;* – */usr/lib/tcl8.4/encoding/*;* – */usr/sbin/perf/*;* – */usr/sbin/vsftpd* Отметить параметр ***Выполнение команд от root***
Windows файлы	– *%ProgramFiles%*.dll;* – *%ProgramFiles%*.exe;* – *%SystemRoot%*.dll;* – *%SystemRoot%*.exe;* – *%SystemRoot%\System32*.acm;*

Наименование шаблона отчета	Контролируемые файлы
	– *%SystemRoot%\System32*.ax;* – *%SystemRoot%\System32*.com;* – *%SystemRoot%\System32*.cpl;* – *%SystemRoot%\System32*.drv;* – *%SystemRoot%\System32*.ocx;* – *%SystemRoot%\System32*.scr;* – *%SystemRoot%\System32*.sys;* – *%SystemRoot%\System32\drivers*.sys;* – *%SystemRoot%\System32\dsound.vxd;* – *%SystemRoot%\system*.drv;* – *%SystemRoot%\System32\AUTOEXEC.NT;* – *%SystemRoot%\System32\CONFIG.NT;* – *%SystemRoot%\System32\desktop.ini;* – *%SystemRoot%\desktop.ini;* – *%SystemRoot%\system.ini;* – *%SystemRoot%\win.ini.* **Исключения:** – *%SystemRoot%\temp*;* – *%SystemRoot%\softwaredistribution*;* – *%SystemRoot%\WinSxS*;* – *%SystemRoot%\System32\DriverStore\FileRepository*;* – *%SystemRoot%\LastGood.Tmp*;* – *%SystemRoot%\System32\Microsoft\Protect\S-1-5-18\User*;* – *%SystemRoot%\System32\spool*;* – *C:\Program Files\System Center Operations Manager\Agent\Health Service State*;* – *%SystemRoot%\assembly*;* – *%SystemRoot%\ccmcache*;* – *%SystemRoot%\Installer\$PatchCache$\Managed**
AIX Файлы	– */bin/*;* – */etc/*.conf;* – */etc/*.config;* – */etc/*_conf;* – */etc/*_config;* – */etc/cron.d/logchecker;* – */etc/fs/*;* – */etc/sudoers;* – */lib/*.a;* – */lib/*.cfg;* – */lib/*.com;* – */lib/*.d;* – */lib/*.kdb;* – */lib/*.ksh;* – */lib/*.sh;* – */lib/*.so32;* – */lib/*.so64;* – */lib/*.tcl;* – */lib/*.vc;* – */lib/boot/*;* – */lib/drivers/*;*

Наименование шаблона отчета	Контролируемые файлы
	– */lib/objrepos/*;* – */lib/security/*;* – */lib/svc/nfs/lockd;* – */lib/svc/nfs/statd;* – */opt/sbin/in.named;* – */opt/sbin/lwresd;* – */opt/sbin/name;* – */sbin/*;* – */usr/bin/*;* – */usr/lib/*.a;* – */usr/lib/*.cfg;* – */usr/lib/*.com;* – */usr/lib/*.d;* – */usr/lib/*.ksh;* – */usr/lib/*.sh;* – */usr/lib/*.so32;* – */usr/lib/*.so64;* – */usr/lib/*.tcl;* – */usr/lib/*.vc;* – */usr/local/sbin/in.named;* – */usr/local/sbin/in.tnamed;* – */usr/local/sbin/lwresd;* – */usr/local/sbin/named;* – */usr/local/sbin/sshd;* – */usr/sbin/** **Исключения:** – */*.bmp;* – */*.gif;* – */*.gl;* – */*.gz;* – */*.help;* – */*.info;* – */*.jar;* – */*.log;* – */*.msg;* – */*.out;* – */*.pm;* – */*.ppm;* – */*.tar;* – */*.tpl;* – */*.txt;* – */*.xml;* – */*.xsd;* – */etc/*.log;* – */etc/tpvmlp.conf;* – */lib/font/*;* – */lib/lpd/pio/trans2/*;* – */lib/nls/loc/*;* – */lib/nls/msg/*;* – */lib/tcl8.4/encoding/*;*

Наименование шаблона отчета	Контролируемые файлы
	– */lib/tk8.4/demos/*;* – */usr/lib/cron/log;* – */usr/lib/font/*;* – */usr/lib/nls/loc/*;* – */usr/lib/nls/msg/*;* – */usr/lib/objrepos/*;* – */usr/lib/tcl8.4/encoding/*;* – */usr/sbin/perf/*;* – */usr/sbin/rsct/msgmaps/*;* – */usr/sbin/rsct/optlevel.rsct.msg*;* – */usr/sbin/rsct/README/*;* – */usr/sbin/rsct/samples/*;* – */usr/sbin/vsftpd*
EfrosACS файлы	– */opt/efros-acs/etc/radius – словари радиуса, сертификаты и файлы конфигурации* – */opt/efros-acs/.postgresql* – */opt/efros-acs/etc/samba* – */opt/efros-acs/etc/tac_plus.cfg* – */opt/efros-acs/etc/krb5.conf* – */opt/efros-acs/share/radius/* – */opt/efros-acs/var/www/NLog.config* – */opt/efros-acs/var/www/appsettings.json* – */opt/efros-acs/var/www/appsettings.production.json*
Acronis файлы	– */var/lib/Acronis/AMS/*.db3* – */var/lib/Acronis/AMS/*.sql* – */var/lib/Acronis/AMS/*.db3-shm* – */var/lib/Acronis/AMS/*.db3-wal* – */var/lib/Acronis/AMS/postgresql/*.sql* – */var/lib/Acronis/AMS/postgresql/*.config* – */var/lib/Acronis/AccountServer/account_server.db* – */var/lib/Acronis/AccountServer/account_server.db-shm* – */var/lib/Acronis/AccountServer/account_server.db-wal* – */var/lib/Acronis/ActiveProtectionManager/acronis_active_protection.db* – */var/lib/Acronis/ActiveProtectionManager/acronis_active_protection.db-shm* – */var/lib/Acronis/ActiveProtectionManager/acronis_active_protection.db-wal* – */var/lib/Acronis/ApiGateway/routing_table.json* – */var/lib/Acronis/BackupAndRecovery/archives_cache.db3* – */var/lib/Acronis/BackupAndRecovery/archives_cache.db3-shm* – */var/lib/Acronis/BackupAndRecovery/archives_cache.db3-wal* – */var/lib/Acronis/BackupAndRecovery/ARSM/Database/arsm.sqlite* – */var/lib/Acronis/BackupAndRecovery/ARSM/Database/arsm.sqlite-shm* – */var/lib/Acronis/BackupAndRecovery/ARSM/Database/arsm.sqlite-wal* – */var/lib/Acronis/BackupManager/acronis_backup_manager.db* – */var/lib/Acronis/BackupManager/acronis_backup_manager.db-shm* – */var/lib/Acronis/BackupManager/acronis_backup_manager.db-wal* – */var/lib/Acronis/CatalogManager/catalog_manager_db.db3* – */var/lib/Acronis/Databases/*.config* – */var/lib/Acronis/GroupManager/groups.db3*

Наименование шаблона отчета	Контролируемые файлы
	– /var/lib/Acronis/GroupManager/groups.db3-shm – /var/lib/Acronis/GroupManager/groups.db3-wal – /var/lib/Acronis/MediaBuilder/scripts/entire_pc_local/*.sh – /var/lib/Acronis/MonitoringServer/am-database/am_collections_storage.db – /var/lib/Acronis/MonitoringServer/am-database/am_rta_storage.db – /var/lib/Acronis/MonitoringServer/am-database/auth.db – /var/lib/Acronis/MonitoringServer/am-database/collector.db – /var/lib/Acronis/MonitoringServer/am-database/metric_meta.db – /var/lib/Acronis/MonitoringServer/am-database/metric_registry.db /var/lib/Acronis/MonitoringServer/am-database/monitoring_objects.db – /var/lib/Acronis/MonitoringServer/am-database/rta_rules.db – /var/lib/Acronis/MonitoringServer/am-database/schema_version – /var/lib/Acronis/MonitoringServer/am-database/search.db – /var/lib/Acronis/MonitoringServer/am-database/metrics/directory.db – /var/lib/Acronis/MonitoringServer/am-database/metrics/directory.db-shm – /var/lib/Acronis/MonitoringServer/am-database/metrics/directory.db-wal – /var/lib/Acronis/PolicyManager/pmDatabase – /var/lib/Acronis/Scheduler/scheduler_db.sqlite3 – /var/lib/Acronis/Scheduler/scheduler_db.sqlite3-shm – /var/lib/Acronis/Scheduler/scheduler_db.sqlite3-wal – /var/lib/Acronis/TaskManager/task_manager_db.sqlite3 – /var/lib/Acronis/TaskManager/task_manager_db.sqlite3-shm – /var/lib/Acronis/TaskManager/task_manager_db.sqlite3-wal – /var/lib/Acronis/UpdateService/update_service.sqlite3
DATAPK ITM-K[1)] файлы	– /opt/datapkitm/docker-compose.sync.yaml – /opt/datapkitm/docker-compose.yaml – /opt/datapkitm/env/.env_agent – /opt/datapkitm/env/.env_db_pgsql – /opt/datapkitm/env/.env_srv – /opt/datapkitm/env/.env_sync_app ; – /opt/datapkitm/env/.env_web – /opt/datapkitm/zbx_env/etc/nginx/conf.d/nginx.conf – /opt/datapkitm/zbx_env/etc/ssl/nginx/nginx.crt – /opt/datapkitm/zbx_env/etc/ssl/nginx/nginx.key – /var/lib/jatoba/1/data/pg_hba.conf – /var/lib/jatoba/1/data/postgresql.conf
DATAPK ITM-H[1)] файлы	– /opt/datapkitm/docker-compose.sync.yam – /opt/datapkitm/docker-compose.yaml – /opt/datapkitm/env/.env_agent – /opt/datapkitm/env/.env_db_pgsql – /opt/datapkitm/env/.env_prx

[1)] Решение DATAPK ITM состоит из нескольких компонентов:

1. ITM-M – сервер управления решением (администрация);
2. ITM-V – сервер визуализации (администрация);
3. ITM-K – сервер консолидации (филиал);
4. ITM-H – сервер агентов (технологический объект).

Наименование шаблона отчета	Контролируемые файлы
	– /var/lib/jatoba/1/data/pg_hba.conf – /var/lib/jatoba/1/data/postgresql.conf
ViPNet StateWatcher файлы	– c:\Program Files\PostgreSQL\9.6\bin\postgres.exe – c:\Program Files\Apache Software Foundation\Tomcat 9.0\bin\Tomcat9.exe – c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\classes\net\statewatcher\web\context\ServletContextConfiguration.class – c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\lib\statewatcher.jar – c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\lib\swcascade.jar – c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\lib\swcollection.jar – c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\lib\swcommon.jar – c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\lib\swdao.jar – c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\lib\swdomain.jar – c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\lib\swgis.jar – c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\geoserver\WEB-INF\lib\gs-wfs-2.14.0.jar – c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\geoserver\WEB-INF\lib\gs-wms-2.14.0.jar
ViPNet Policy Manager файлы	C:\Program Files (x86)\InfoTeCS\ViPNet Policy Manager\ – addressbook-vc120-mt-32.dll – asntools-vc120-32.dll – boost_date_time-vc120-mt-32-1_62.dll – boost_filesystem-vc120-mt-32-1_62.dll – boost_regex-vc120-mt-32-1_62.dll – boost_serialization-vc120-mt-32-1_62.dll – boost_system-vc120-mt-32-1_62.dll – boost_thread-vc120-mt-32-1_62.dll – boost_wserialization-vc120-mt-32-1_62.dll – cert.dll – crptapi-vc120-32.dll – cryptapi-vc120-32.dll – Envelope.dll – fwcommon-vc120-mt-32.dll – idents-vc120-32.dll – itcs_custom_itcipc.dll – itcs_custom_itcscapi.dll – itcs_custom_pwdgen.dll – itcs_custom_storedev.dll – itcs_custom_structfiles.dll – itcselog.dll – ItcsPack.dll – itcupd.dll

Наименование шаблона отчета	Контролируемые файлы
	– *knownfiles-vc120-32.dll* – *logdisp-vc120-32.dll* – *nonmfc-vc120-mt-32.dll* – *pm.exe* – *pmclient-core.dll* – *pmclient-ui.dll* – *pmcommon.dll* – *pmserver-core.dll* – *product_info-vc120-32.dll* – *Qt5Core.dll* – *Qt5Gui.dll* – *Qt5Network.dll* – *Qt5PrintSupport.dll* – *Qt5Widgets.dll* – *Qt5XmlPatterns.dll* – *qtcontrols.dll* – *QtSolutions_MFCMigrationFramework-vc120-mt-32-2_8.dll* – *qttranslator_builder.dll* – *rvupdate-vc120-mt-32.dll* – *tools2-vc120-32.dll* – *xerces-vc120-mt-32-3_2_1.dll*
ViPNet Administrator файлы	– *C:\Program Files (x86)\InfoTeCS\ViPNet Administrator* – *\KCA\KeyCenter2.Exe* – *\NCC\Server\Infotecs.WinNcc.Communication.Hosting.exe* – *\NCC\Client\Infotecs.WinNcc.WinNcc.exe*
KES[1] файлы	– *%Program Files (x86)%\Kaspersky Lab\Kaspersky Endpoint Security for Windows\avp.exe*
MaxPatrol	*Перечень файлов приведен в документе «Система контроля защищенности и соответствия стандартам MaxPatrol. Контрольные суммы исполняемых файлов после инсталляции», из комплекта поставки MaxPatrol.*
Windows файлы “MSSQL”	– *C:\Program Files\Microsoft SQL Server*.exe.config* **Исключения:** – *C:\Program Files\Microsoft SQL Server\100\Setup Bootstrap** – *C:\Program Files\Microsoft SQL Server\110\Setup Bootstrap** – *C:\Program Files\Microsoft SQL Server\120\Setup Bootstrap**
Ankey SIEM	*Перечень контролируемых файлов:* *//opt/ankey/containers/** **Исключения:** – */opt/ankey/containers/*.log* – */opt/ankey/containers/*.pid* – */opt/ankey/containers/*.lock* – */opt/ankey/containers/*.0* – */opt/ankey/containers/*.1* – */opt/ankey/containers/*.dflt*

[1] KES – Kaspersky Endpoint Security

Наименование шаблона отчета	Контролируемые файлы
	– */opt/ankey/containers/*.sid.csv* – */opt/ankey/containers/*.idmap* – */opt/ankey/containers/*.syslogd.** – */opt/ankey/containers/hosts.t** – */opt/ankey/containers/syslog.prop** – */opt/ankey/containers/bcfips_** – */opt/ankey/containers/remote_management.** – */opt/ankey/containers/cacert** – */opt/ankey/containers/*.log.** – */opt/ankey/containers/ThreadDump.** – */opt/ankey/containers/*.aup**
Ankey SIEM MC	*Перечень контролируемых файлов:* – */opt/ankey/amc/current/arcsight/service/** – */opt/ankey/amc/current/local/apache/bin/** – */opt/ankey/amc/current/local/apache/conf/** – */opt/ankey/amc/current/local/apache/lib/** – */opt/ankey/amc/current/local/apache/modules/** – */opt/ankey/amc/current/local/jre/** – */opt/ankey/amc/current/local/lib/** – */opt/ankey/amc/current/local/monit/bin/** – */opt/ankey/amc/current/local/nss/** – */opt/ankey/amc/current/local/openssl/bin/** – */opt/ankey/amc/current/local/openssl/lib/** – */opt/ankey/amc/current/local/pcre/bin/** – */opt/ankey/amc/current/local/pcre/lib/** – */opt/ankey/amc/current/local/pgsql/bin/** – */opt/ankey/amc/current/local/pgsql/lib/** – */opt/ankey/amc/current/local/sysstat/** – */opt/ankey/amc/current/local/tomcat/bin/** – */opt/ankey/amc/current/local/tomcat/lib/** – */opt/ankey/amc/data/pgsql/*.conf* – */opt/ankey/amc/mc_ver.ank* – */opt/ankey/Ankey-SIEM-MC-SC-uninstall* – */opt/ankey/backup/bin/** – */opt/ankey/backup/bin/config/** – */opt/ankey/bin/ankey_container* – */opt/ankey/bin/ankey_container_conf* – */opt/ankey/bin/ankey_mc* – */opt/ankey/bin/ankey_mc_conf* – */opt/ankey/ci/** – */opt/ankey/nodejs/** **Исключения:** – */opt/ankey/ci/db/** – */opt/ankey/ci/logs/**
Ankey SIEM Logger	*Перечень контролируемых файлов:* – */etc/.SourceOSconfig/** – */etc/rc.d/init.d/ankey_logger* – */opt/ankey/ankey.ver* – */opt/ankey/Ankey-SIEM-Logger-uninstall*

Наименование шаблона отчета	Контролируемые файлы
	– /opt/ankey/backup/bin/* – /opt/ankey/backup/config/* – /opt/ankey/bin/ankey_logger – /opt/ankey/bin/ankey_logger_conf – /opt/ankey/ci/* – /opt/ankey/logger/current/ankey/bin/* – /opt/ankey/logger/current/ankey/logger/bin/* – /opt/ankey/logger/current/ankey/logger/config/* – /opt/ankey/logger/current/ankey/logger/i18n/* – /opt/ankey/logger/current/ankey/logger/jarball/jars/* – /opt/ankey/logger/current/ankey/logger/lib/* – /opt/ankey/logger/current/ankey/logger/version.txt – /opt/ankey/logger/current/ankey/service/* – /opt/ankey/logger/current/arcsight/aps/bin/* – /opt/ankey/logger/current/arcsight/aps/cli/lib/* – /opt/ankey/logger/current/arcsight/aps/conf/* – /opt/ankey/logger/current/arcsight/aps/jarball/jars/* – /opt/ankey/logger/current/arcsight/aps/snmp/lib/* – /opt/ankey/logger/current/arcsight/aps/webapps/core-service/WEB-INF/lib/* – /opt/ankey/logger/current/arcsight/aps/webapps/platform-service/WEB-INF/lib/* – /opt/ankey/logger/current/arcsight/aps/webapps/storage-service/WEB-INF/lib/* – /opt/ankey/logger/current/arcsight/autopass/* – /opt/ankey/logger/current/arcsight/bin/* – /opt/ankey/logger/current/arcsight/connector/current/agents-7.11.0.8129.0-common.xml – /opt/ankey/logger/current/arcsight/connector/current/agents-7.11.0.8129.0-linux64.xml – /opt/ankey/logger/current/arcsight/connector/current/agents-7.11.0.8129.0-unix.xml – /opt/ankey/logger/current/arcsight/connector/current/agents-7.13.0.8195.1-common.xml – /opt/ankey/logger/current/arcsight/connector/current/agents-7.13.0.8195.1-linux64.xml – /opt/ankey/logger/current/arcsight/connector/current/agents-7.13.0.8195.1-unix.xml – /opt/ankey/logger/current/arcsight/connector/current/bin/* – /opt/ankey/logger/current/arcsight/connector/current/config/* – /opt/ankey/logger/current/arcsight/connector/current/i18n/* – /opt/ankey/logger/current/arcsight/connector/current/jre/* – /opt/ankey/logger/current/arcsight/connector/current/lib/* – /opt/ankey/logger/current/arcsight/connector/current/system/agent/* – /opt/ankey/logger/current/arcsight/connector/current/utilities/keytoolgui/* – /opt/ankey/logger/current/arcsight/connector/current/version.txt – /opt/ankey/logger/current/arcsight/logger/bin/* – /opt/ankey/logger/current/arcsight/logger/config/* – /opt/ankey/logger/current/arcsight/logger/i18n/* – /opt/ankey/logger/current/arcsight/logger/jarball/jars/*

Наименование шаблона отчета	Контролируемые файлы
	– */opt/ankey/logger/current/arcsight/logger/lib/** – */opt/ankey/logger/current/arcsight/logger/version.txt* – */opt/ankey/logger/current/arcsight/service/** – */opt/ankey/logger/current/local/apache/bin/** – */opt/ankey/logger/current/local/apache/conf/** – */opt/ankey/logger/current/local/apache/lib/** – */opt/ankey/logger/current/local/apache/modules/** – */opt/ankey/logger/current/local/jre/** – */opt/ankey/logger/current/local/lib/** – */opt/ankey/logger/current/local/monit/bin/** – */opt/ankey/logger/current/local/mysql/bin/** – */opt/ankey/logger/current/local/mysql/lib/mysql/** – */opt/ankey/logger/current/local/nss/** – */opt/ankey/logger/current/local/openssl/bin/** – */opt/ankey/logger/current/local/openssl/lib/** – */opt/ankey/logger/current/local/pcre/bin/** – */opt/ankey/logger/current/local/pcre/lib/** – */opt/ankey/logger/current/local/pgsql/bin/** – */opt/ankey/logger/current/local/pgsql/lib/** – */opt/ankey/logger/current/local/sysstat/** – */opt/ankey/logger/current/local/tomcat/bin/** – */opt/ankey/logger/current/local/tomcat/jarball/jars/** – */opt/ankey/logger/current/local/tomcat/lib/** – */opt/ankey/logger/data/mysql/my.cnf* – */opt/ankey/logger/data/pgsql/** – */opt/ankey/logger/logger_ver.ank* – */opt/ankey/logger/userdata/connector/user/agent/acp/** – */opt/ankey/logger/userdata/connector/user/agent/agent.properties* – */opt/ankey/logger/userdata/connector/user/agent/agent.wrapper.conf* – */opt/ankey/logger/userdata/connector/user/agent/flexagent/** – */opt/ankey/logger/userdata/connector/user/connectorappliance/** – */opt/ankey/nodejs/** **Исключения:** – */opt/ankey/ci/db/** – */opt/ankey/ci/logs/** – */opt/ankey/logger/current/arcsight/autopass/*.jar* – */opt/ankey/logger/data/pgsql/*.conf*
Ankey SIEM ESM	*Перечень контролируемых файлов:* – */etc/.SourceOSconfig/** – */etc/init.d/ankey_services* – */opt/ankey/backup/bin/** – */opt/ankey/bin/** – */opt/ankey/ci/** – */opt/ankey/java/** – */opt/ankey/kse/** – */opt/ankey/logger/current/arcsight/** – */opt/ankey/logger/current/local/** – */opt/ankey/logger/data/mysql/auto.cnf* – */opt/ankey/logger/data/mysql/ca.pem* – */opt/ankey/logger/data/mysql/ca-key.pem*

Наименование шаблона отчета	Контролируемые файлы
	– /opt/ankey/logger/data/mysql/client-cert.pem – /opt/ankey/logger/data/mysql/client-key.pem – /opt/ankey/logger/data/mysql/my.cnf – /opt/ankey/logger/data/mysql/private_key.pem – /opt/ankey/logger/data/mysql/public_key.pem – /opt/ankey/logger/data/mysql/server-cert.pem – /opt/ankey/logger/data/mysql/server-key.pem – /opt/ankey/logger/data/pgsql – /opt/ankey/logger/data/pgsql/pg_hba.conf – /opt/ankey/logger/data/pgsql/pg_hba.conf.orig – /opt/ankey/logger/data/pgsql/pg_ident.conf – /opt/ankey/logger/data/pgsql/PG_VERSION – /opt/ankey/logger/data/pgsql/postgresql.conf – /opt/ankey/logger/data/pgsql/postgresql.conf.bak – /opt/ankey/logger/data/pgsql/postgresql.conf.orig – /opt/ankey/logger/userdata/arcsight_license – /opt/ankey/logger/userdata/logger/user/logger/email_alert_forwarder_emailalertforwarder.xml – /opt/ankey/logger/userdata/logger/user/logger/esm_forwarder_esmalertforwarder.xml – /opt/ankey/logger/userdata/logger/user/logger/preconfigured_receivers – /opt/ankey/logger/userdata/logger/user/logger/primarystoragepath – /opt/ankey/logger/userdata/logger/user/logger/version.txt – /opt/ankey/logger/userdata/platform/esm_proxy.conf – /opt/ankey/logger/userdata/platform/fips.conf – /opt/ankey/logger/userdata/platform/ssl.crt/CA.srl – /opt/ankey/logger/userdata/platform/ssl.crt/request.csr – /opt/ankey/logger/userdata/platform/ssl.crt/server.crt – /opt/ankey/logger/userdata/platform/ssl.crt/server.pem – /opt/ankey/manager/ancillary.txt – /opt/ankey/manager/arcsight-dm/dmapps/* – /opt/ankey/manager/arcsight-dm/plugins/* – /opt/ankey/manager/bin/* – /opt/ankey/manager/config/* – /opt/ankey/manager/copyright.txt – /opt/ankey/manager/esm_ver.ank – /opt/ankey/manager/i18n/* – /opt/ankey/manager/jre/* – /opt/ankey/manager/lib/* – /opt/ankey/manager/mbus/* – /opt/ankey/manager/reports/repository.defaults.xml – /opt/ankey/manager/reports/sree.properties – /opt/ankey/manager/reports/templatechart.3.0.xml – /opt/ankey/manager/reports/templatechart.xml – /opt/ankey/manager/reports/templatechartlandscape.3.0.xml – /opt/ankey/manager/reports/templatechartlandscape.xml – /opt/ankey/manager/reports/templatecharttable.3.0.xml – /opt/ankey/manager/reports/templatecharttable.xml – /opt/ankey/manager/reports/templatecharttablelandscape.3.0.xml – /opt/ankey/manager/reports/templatecharttablelandscape.xml

Наименование шаблона отчета	Контролируемые файлы
	– */opt/ankey/manager/reports/templateCustomCanvas1.srt* – */opt/ankey/manager/reports/templateCustomTable.srt* – */opt/ankey/manager/reports/templateMvgAvg.xml* – */opt/ankey/manager/reports/templateSecurityMetric.srt* – */opt/ankey/manager/reports/templateStatusRpt.srt* – */opt/ankey/manager/reports/templatetable.xml* – */opt/ankey/manager/reports/templatetablelandscape.xml* – */opt/ankey/manager/schema/** – */opt/ankey/manager/system/** – */opt/ankey/manager/user/manager/license/arcsight.lic* – */opt/ankey/manager/user/manager/license/userdata/autopass/data/LicFile.txt* – */opt/ankey/manager/user/manager/version.txt* – */opt/ankey/manager/user/manager/vname.txt* – */opt/ankey/manager/utilities/** – */opt/ankey/manager/version.txt* – */opt/ankey/manager/vname.txt* – */opt/ankey/manager/webpages/** – */opt/ankey/services/** – */opt/ankey/suite/bin/scripts/** **Исключения:** – */opt/ankey/ci/db/** – */opt/ankey/logger/current/arcsight/*.log* – */opt/ankey/logger/current/arcsight/logger/tmp/** – */opt/ankey/logger/current/arcsight/logger/run/** – */opt/ankey/logger/current/arcsight/aps/webapps/platform-ui/locale_code.property* – */opt/ankey/logger/current/arcsight/aps/webapps/platform-ui/product.property* – */opt/ankey/logger/current/arcsight/service/arcsight.config"* – */opt/ankey/logger/current/local/apache/logs/error_log* – */opt/ankey/logger/current/local/tomcat/temp/** – */opt/ankey/logger/current/local/tomcat/webapps/logger/export/** – */opt/ankey/logger/current/local/tomcat/work/Catalina/localhost/soap/** – */opt/ankey/manager/config/history/** – */opt/ankey/manager/webpages/work/** – */opt/ankey/services/monit/data/monit.log*
Ankey SIEM FC	*Перечень контролируемых файлов:* – */etc/init.d/ak_forward_** – */opt/$FC/agents-*-common.xml* – */opt/$FC/current/agents-*-linux64.xml* – */opt/$FC/current/agents-*-unix.xml* – */opt/$FC/current/bin/** – */opt/$FC/current/config/** – */opt/$FC/current/i18n/** – */opt/$FC/current/jre/** – */opt/$FC/current/lib/** – */opt/$FC/current/system/agent/acp/** – */opt/$FC/current/system/agent/config/** – */opt/$FC/current/system/agent/fcp/**

Наименование шаблона отчета	Контролируемые файлы
	– */opt/$FC/current/system/agent/web/** – */opt/$FC/current/UninstallerData/** – */opt/$FC/current/user/agent/agent.properties* – */opt/$FC/current/user/agent/agent.wrapper.conf* – */opt/$FC/current/user/connectorappliance/** – */opt/$FC/current/utilities/keytoolgui/** – */opt/$FC/current/version.txt* **Исключения:** – */opt/$FC/current/jre/lib/security/cacerts/**
Ankey SIEM SC	*Перечень контролируемых файлов:* – */etc/init.d/container_*/** – *$ANKEY_HOME/current/agents-*-common.xml* – *$ANKEY_HOME/current/agents-*-linux64.xml* – *$ANKEY_HOME/current/agents-*-unix.xml* – *$ANKEY_HOME/current/backup/bin/** – *$ANKEY_HOME/current/backup/config/** – *$ANKEY_HOME/current/bin/** – *$ANKEY_HOME/current/config/** – *$ANKEY_HOME/current/i18n/** – *$ANKEY_HOME/current/jre/** – *$ANKEY_HOME/current/lib/** – *$ANKEY_HOME/current/system/agent/acp/** – *$ANKEY_HOME/current/system/agent/config/** – *$ANKEY_HOME/current/system/agent/fcp/** – *$ANKEY_HOME/current/system/agent/web/** – *$ANKEY_HOME/current/UninstallerData/** – *$ANKEY_HOME/current/user/agent/acp/categorizer/current/gis/ankey_siem_backup.csv* – *$ANKEY_HOME/current/user/agent/acp/categorizer/current/gis/ankey_siem_ci.csv* – *$ANKEY_HOME/current/user/agent/acp/categorizer/current/gis/ankey_siem_mysql.csv* – *$ANKEY_HOME/current/user/agent/acp/categorizer/current/gis/ankey_siem_postgresql.csv* – *$ANKEY_HOME/current/user/agent/agent.properties* – *$ANKEY_HOME/current/user/agent/agent.wrapper.conf* – *$ANKEY_HOME/current/user/agent/flexagent/ankeysiem/backup.sdkkeyvaluefilereader.properties* – *$ANKEY_HOME/current/user/agent/flexagent/ankeysiem/ci.sdkkeyvaluefilereader.properties* – *$ANKEY_HOME/current/user/agent/flexagent/ankeysiem/mysql_sub.sdkrfilereader.properties* – *$ANKEY_HOME/current/user/agent/flexagent/ankeysiem/postgresql_sub.sdkrfilereader.properties* – *$ANKEY_HOME/current/user/agent/flexagent/syslog/ankeysiem_backup.subagent.sdkrfilereader.properties* – *$ANKEY_HOME/current/user/agent/flexagent/syslog/ankeysiem_ci.subagent.sdkrfilereader.properties* – *$ANKEY_HOME/current/user/agent/flexagent/syslog/ankeysiem_mysql.subagent.sdkrfilereader.properties*

Наименование шаблона отчета	Контролируемые файлы
	– *$ANKEY_HOME/current/user/agent/flexagent/syslog/ankeysiem_postgresql.subagent.sdkrfilereader.properties* – *$ANKEY_HOME/current/user/connectorappliance/** – *$ANKEY_HOME/current/utilities/keytoolgui/** – *$ANKEY_HOME/current/version.txt* **Исключения:** – *$ANKEY_HOME/current/jre/lib/security/cacerts*
Ankey SIEM LB	*Перечень контролируемых файлов:* – */etc/.SourceOSconfig/** – */etc/init.d/ankey_lb** – */opt/$LB/Ankey-SIEM-LB-uninstall* – */opt/$LB/backup/bin/** – */opt/$LB/bin/** – */opt/$LB/ci/** – */opt/$LB/core.ver* – */opt/$LB/lb/current/bin/arcsight* – */opt/$LB/lb/current/bin/lb.wrapper.sh* – */opt/$LB/lb/current/bin/runlbsetup.sh* – */opt/$LB/lb/current/bin/scripts/** – */opt/$LB/lb/current/bin/wrapper/linux64/libwrapper-linux-x86-64.so* – */opt/$LB/lb/current/bin/wrapper/linux64/wrapper* – */opt/$LB/lb/current/config/** – */opt/$LB/lb/current/jre/** – */opt/$LB/lb/current/lib/** – */opt/$LB/lb/current/UninstallerData/** – */opt/$LB/lb/current/user/loadbalancer/lb.wrapper.conf* – */opt/$LB/lb/current/user/loadbalancer/lbConfig.xml* – */opt/$LB/lb/current/user/loadbalancer/loadbalancer.cer* – */opt/$LB/lb/current/user/loadbalancer/loadbalancer.p12* – */opt/$LB/lb/current/version.txt* – */opt/$LB/lb/lb_ver.ank* **Исключения:** – */opt/ankey/ci/db/** – */opt/ankey/ci/logs/** – */opt/ankey/ci/bin/ankey_ci.yml*
Ankey Console win	*Перечень контролируемых файлов:* – *%ANKEY_CONSOLE_HOME%\backup\backup.bat* – *%ANKEY_CONSOLE_HOME%\current\bin*.** – *%ANKEY_CONSOLE_HOME%\current\config*.** – *%ANKEY_CONSOLE_HOME%\current\i18n*.** – *%ANKEY_CONSOLE_HOME%\current\jre*.** – *%ANKEY_CONSOLE_HOME%\current\lib*.**
Ankey SC win	*Перечень контролируемых файлов:* – *%ANKEY_HOME%/current/user/agent/agent.properties* – *%ANKEY_HOME%/current/user/agent/agent.wrapper.conf* – *%ANKEY_HOME%\current\agents-*-common.xml* – *%ANKEY_HOME%\current\agents-*-linux64.xml* – *%ANKEY_HOME%\current\agents-*-unix.xml* – *%ANKEY_HOME%\current\backup\bin*.** – *%ANKEY_HOME%\current\backup\config*.**

Наименование шаблона отчета	Контролируемые файлы
	– *%ANKEY_HOME%\current\bin*.** – *%ANKEY_HOME%\current\config*.** – *%ANKEY_HOME%\current\i18n*.** – *%ANKEY_HOME%\current\jre*.** – *%ANKEY_HOME%\current\lib*.** – *%ANKEY_HOME%\current\system\agent\acp*.** – *%ANKEY_HOME%\current\system\agent\config*.** – *%ANKEY_HOME%\current\system\agent\fcp*.** – *%ANKEY_HOME%\current\system\agent\web*.** – *%ANKEY_HOME%\current\UninstallerData*.** – *%ANKEY_HOME%\current\user\agent\acp\categorizer\current\gis\ankey_siem_backup.csv* – *%ANKEY_HOME%\current\user\agent\acp\categorizer\current\gis\ankey_siem_ci.csv* – *%ANKEY_HOME%\current\user\agent\acp\categorizer\current\gis\ankey_siem_mysql.csv* – *%ANKEY_HOME%\current\user\agent\acp\categorizer\current\gis\ankey_siem_postgresql.csv* – *%ANKEY_HOME%\current\user\agent\flexagent\ankeysiem\backup.sdkkeyvaluefilereader.properties* – *%ANKEY_HOME%\current\user\agent\flexagent\ankeysiem\ci.sdkkeyvaluefilereader.properties* – *%ANKEY_HOME%\current\user\agent\flexagent\ankeysiem\mysql_sub.sdkrfilereader.properties* – *%ANKEY_HOME%\current\user\agent\flexagent\ankeysiem\postgresql_sub.sdkrfilereader.properties* – *%ANKEY_HOME%\current\user\agent\flexagent\syslog\ankeysiem_backup.subagent.sdkrfilereader.properties* – *%ANKEY_HOME%\current\user\agent\flexagent\syslog\ankeysiem_ci.subagent.sdkrfilereader.properties* – *%ANKEY_HOME%\current\user\agent\flexagent\syslog\ankeysiem_mysql.subagent.sdkrfilereader.properties* – *%ANKEY_HOME%\current\user\agent\flexagent\syslog\ankeysiem_postgresql.subagent.sdkrfilereader.properties* – *%ANKEY_HOME%\current\user\connectorappliance*.** – *%ANKEY_HOME%\current\utilities\keytoolgui*.** – *%ANKEY_HOME%\current\version.txt* **Исключения:** – *%ANKEY_HOME%\jre\lib\security\cacerts*.**
zVirt	1. *На виртуальной машине с менеджером управления:* – */etc/ovirt-engine* – */etc/ovirt-engine-dwh* – */etc/ovirt-engine-extension-aaa-ldap-setup.conf.d* – */etc/ovirt-engine-metrics* – */etc/ovirt-engine-setup.conf.d* – */etc/ovirt-engine-setup.env.d* – */etc/ovirt-host-deploy.conf.d* – */etc/ovirt-imageio-proxy* – */etc/ovirt-provider-ovn* – */etc/ovirt-vmconsole*

Наименование шаблона отчета	Контролируемые файлы
	– */etc/ovirt-web-ui* 2. *На хосте виртуализации:* – */etc/ovirt-host-deploy.conf.d* – */etc/ovirt-hosted-engine* – */etc/ovirt-hosted-engine-ha* – */etc/ovirt-hosted-engine-setup.env.d* – */etc/ovirt-imageio-daemon* – */etc/ovirt-vmconsole*
СУБД Jatoba	1. *На ОС Linux:* – */etc/systemd/system/jatoba-3.service* – */etc/pam.d/jatoba* – */usr/lib/tmpfiles.d/jatoba-3.conf* – */var/lib/jatoba/*/*/postgresql.auto.conf* – */usr/jatoba-*/bin/** – */usr/jatoba-*/lib/** – */usr/jatoba-*/share/extension/** 2. *На ОС Windows* – *<c:\Program Files\GIS\Jatoba*.*>*