GIS ГАЗИНФОРМ СЕРВИС

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

Руководство пользователя
Часть 2

Настройки контроля

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 пользователей ПК «Efros Config Inspector» v.4 с правами *Просмотр* и *Управление* в категории *Настройки контроля*.

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 (МЭ) 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);
- Primo RPA (Primo RPA Orchestrator);
- WatchGuard Technologies, Inc. (WatchGuard Fireware OS, WatchGuard Fireware XTM OS);
- Rockwell Automation, Inc (Rockwell Cisco IOS);
- TFortis (PSW);Siemens AG (Siemens Scalance X-300, X-400 series, Simatic WinCC);
- ОС Unix/Linux (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 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 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 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;
- резервирование серверов ПК.

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.

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

- проверка/создание базы данных (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;

[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

- Windows 10 Pro;
- Windows 10 Enterprise;
- Windows 11 Home;
- Windows 11 Pro;
- Windows 11 Enterprise.

Клиентская консоль подключается к серверу ПК по протоколу HTTPS и 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[1]:

– 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, построение отчетов).

5) Настройка комплекса:

а) настройки сервера ПК:

– задание триггеров для обработки событий системы и устройств, включение/выключение аудита изменений отчетов для привязки произведенных на устройствах изменений к пользователям (с возможностью подключения к Системе контроля действий поставщиков ИТ-услуг (СКДПУ));
– управление профилями для гибкой настройки параметров контроля устройств;
– управление отчетами, проверками, контролем устройств и групп;

[1] Если в используемой версии ПК «Efros Config Inspector» v.4 настроена иерархия серверов ПК, то к клиентской консоли одновременно могут быть подключены не более трех серверов, входящих в иерархию

- 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 ПК 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.

ПК «Efros Config Inspector» v.4 выполняется периодический контроль целостности компонентов комплекса: сервера ПК, windows-агентов, коллекторов, клиентской консоли, с отображением соответствующих уведомлений для пользователей в клиентской консоли и фиксацией событий нарушения (кроме консоли) в журнале событий комплекса.

ПК «Efros Config Inspector» v.4 хранятся во внешней системе управления базами данных (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.

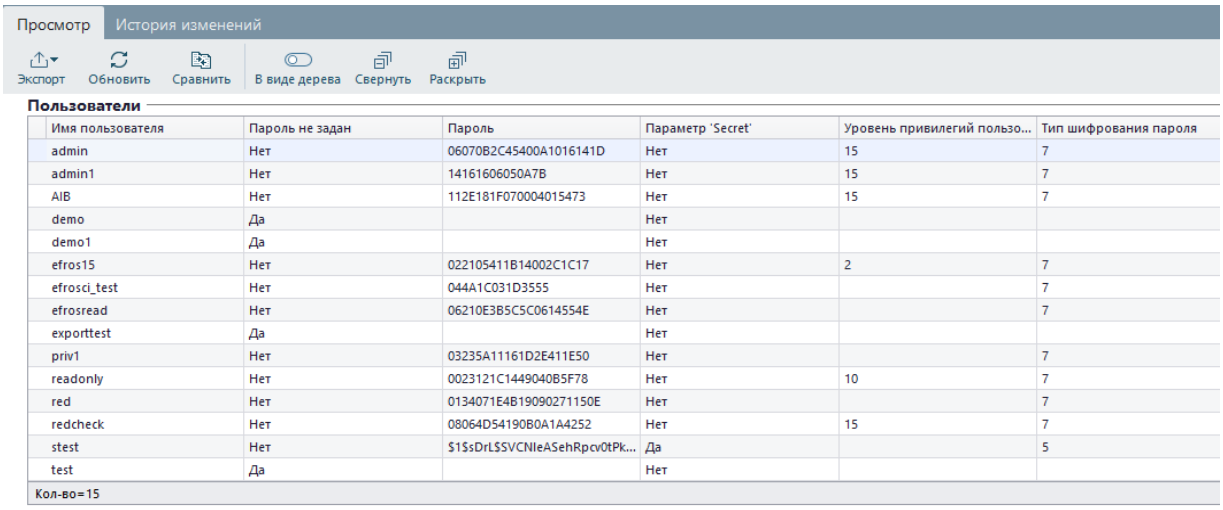
Для межсетевых экранов (МЭ) кроме встроенных отчетов пользователем с правами *Управление* в категории ***Настройки контроля*** при настройке проверок МЭ могут быть созданы стандарты безопасности, содержащие требования для контроля наличия/отсутствия правил МЭ по заданным параметрам, и назначены устройства, 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:

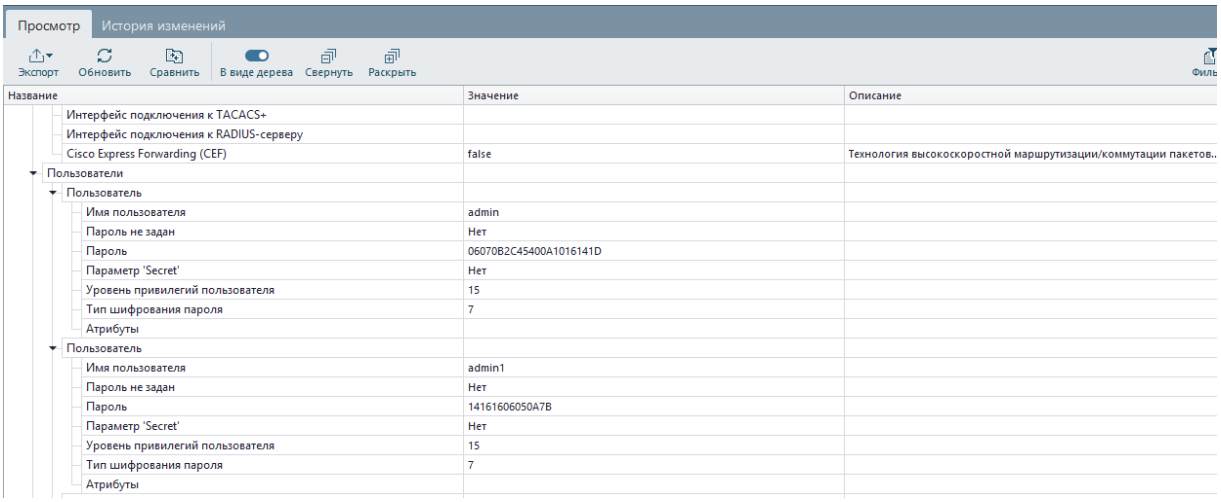
- отчеты о конфигурации, включающие в себя текстовые и структурированные отчеты;

- отчеты о проверках (политик безопасности, наличия уязвимостей, синхронизации рабочей и загрузочной конфигураций).

Данные отчетов 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.



а)



б)

Рисунок 1 – Примеры представлений отчета

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

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 двух типов ***Личные*** (доступные только пользователю) и ***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.

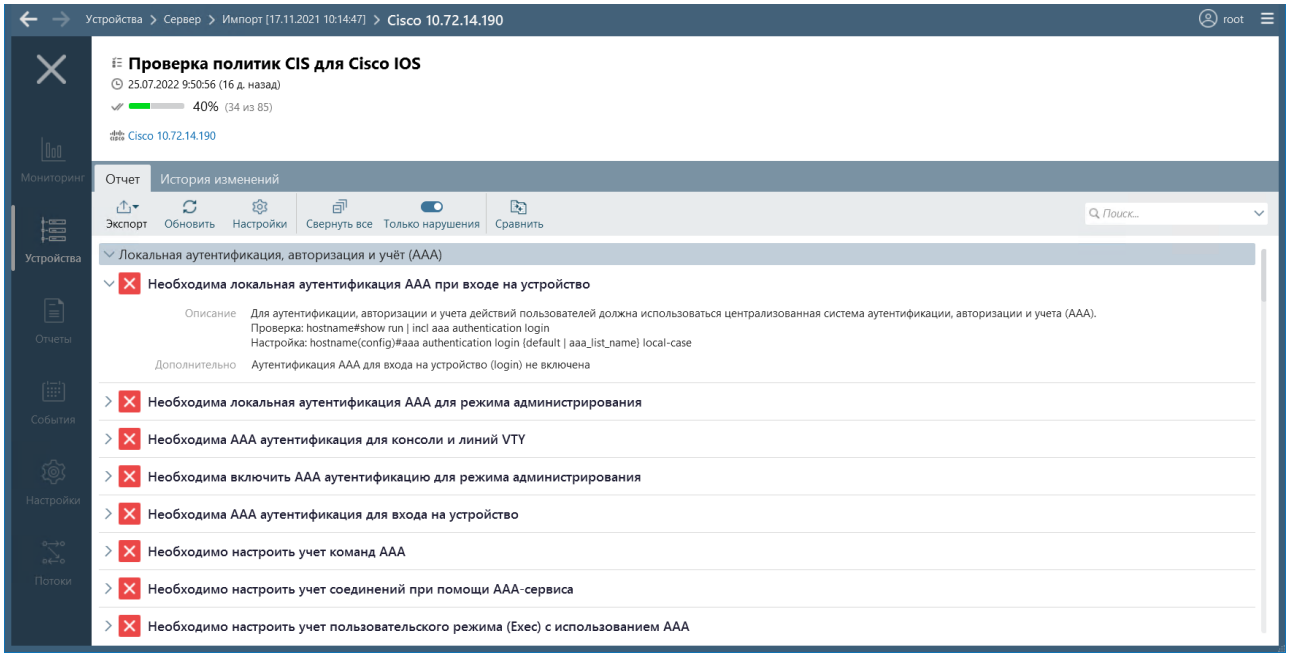


Рисунок 2 – Отчет о результате проверки

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).

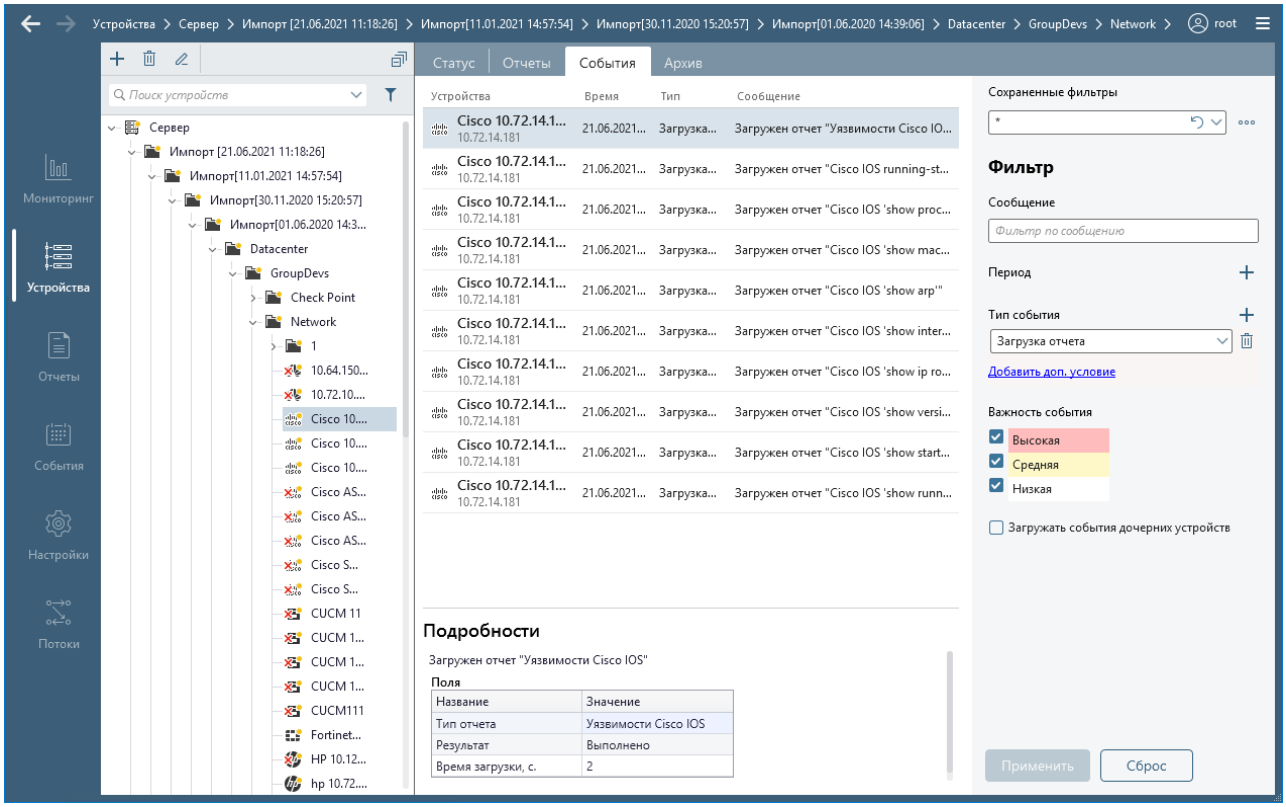


Рисунок 3 – Фильтрация событий

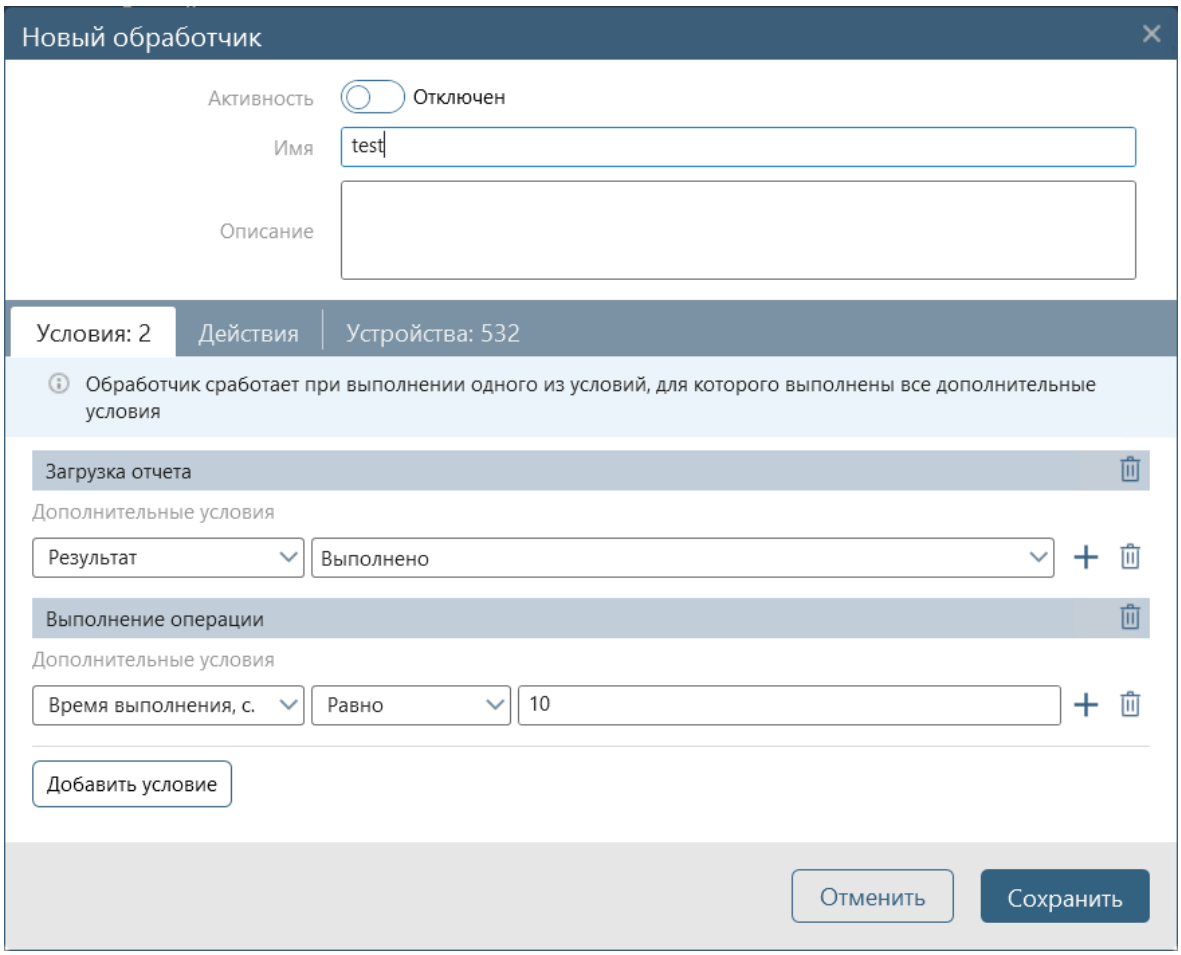


Рисунок 4 – Задание условий при настройке обработчика событий

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.

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 пользователями и группами пользователей;
- задание параметров хранения отчетов и событий;
- просмотр списка резервных серверов;
- просмотр списка задач ПК «Efros Config Inspector» v.4;
- управление распределением нагрузки (подключение коллекторов);
- настройка иерархии серверов;
- настройка параметров подключения к БДУ и обновление БДУ;
- настройка подключения к БДУ через прокси-сервер;
- настройка и проверка подключения к серверу «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.

Право доступа	Описание
	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 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 программного 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 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство администратора (далее – 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. руководство администратора).

4) Добавить в список устройств комплекса контролируемое оборудование (подробнее о добавлении контролируемого оборудования, настройке его параметров см. документ 643.72410666.00082-01 96 01-03 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 3. Работа с устройствами»).

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) в соответствии с настоящим руководством.

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***.

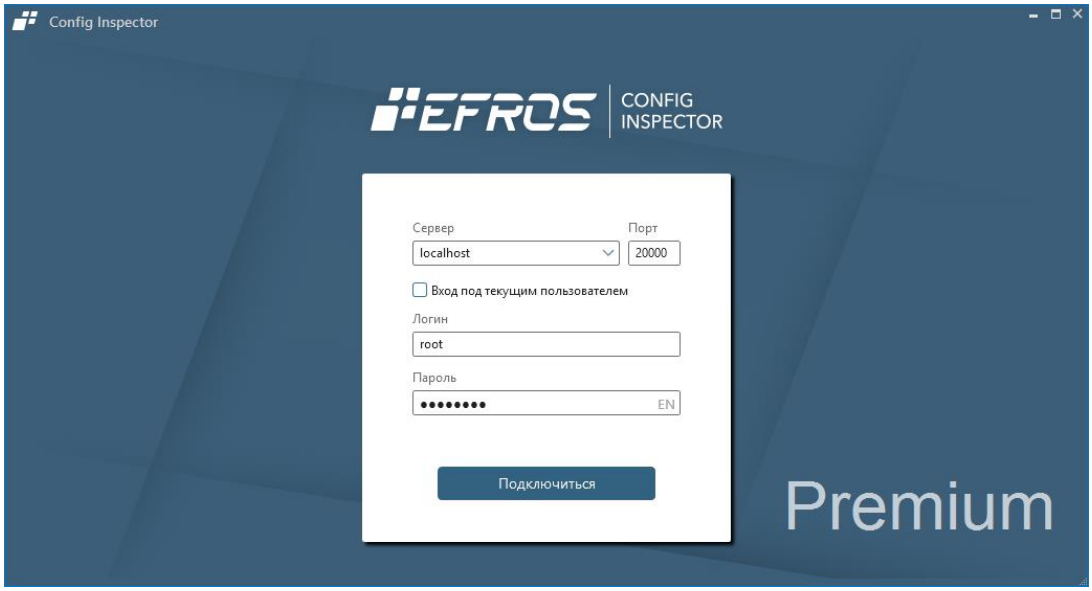


Рисунок 5 – Окно **Подключение**

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

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).

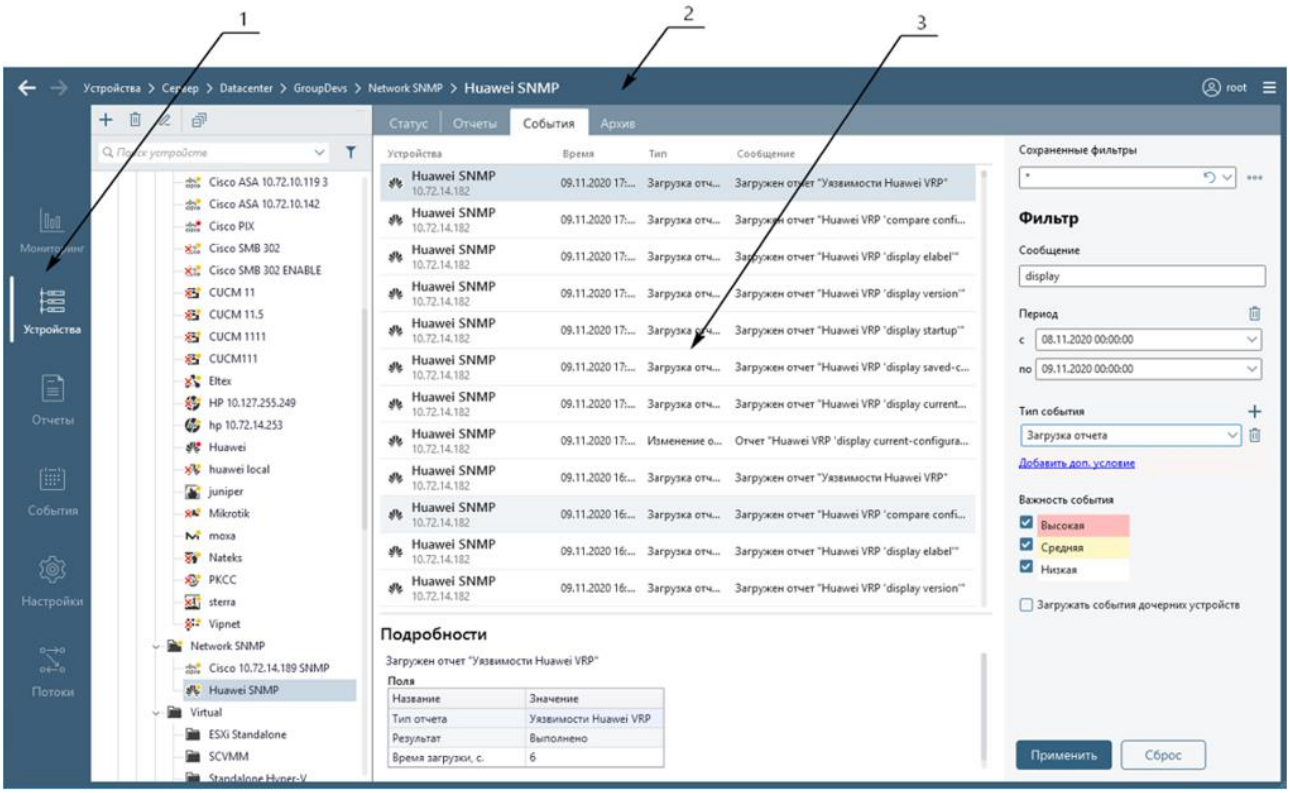


Рисунок 6 – Клиентская консоль. Раздел **Устройства**

Консоль имеет заголовок, панель выбора раздела и рабочую область.

В панели выбора раздела консоли (рис. 2, поз. 1) расположены кнопки выбора разделов:

- **Мониторинг** – в разделе представлена обобщенная информация о состоянии всех устройств, контролируемых комплексом, в графическом виде и в виде списка уведомлений;
- **Устройства** – раздел предназначен для работы с устройствами: ведения списка устройств, загрузки отчетов устройств, просмотра уведомлений, последних и архивных отчетов и событий устройств;
- **Отчеты** – раздел предназначен для создания шаблонов и формирования на их основе пользовательских отчетов для выбранных устройств, по выбранным отчетам и за выбранный период;

- **События** – в разделе отображены события, произошедшие на всех контролируемых текущим сервером комплекса устройствах, а также действия пользователей клиентской консоли;
- **Настройки** – раздел предназначен для доступа к настройкам комплекса и администрированию серверной части комплекса (подробнее описание раздела см. в п. 2.2 «Настройка комплекса»);
- **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».

Все разделы консоли доступны всем пользователям комплекса, кроме раздела **Настройки**, в котором функции настройки контроля доступны только пользователям с правами *Просмотр* и *Управление* категории *Настройки контроля*, функции администрирования – пользователям с правами *Просмотр* и *Управление* категории *Администрирование* (далее – администраторы).

Подробное описание и правила работы пользователей в разделах **Мониторинг**, **Устройства**, **Отчеты** и **События** приведены в документе «643.72410666.00082-01 96 01-03 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 3. Работа с устройствами»).

Подробное описание и правила выполнения административных функций пользователями, которым назначен доступ к настройкам комплекса в категории **Администрирование,** приведены 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»).

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

- наименование и номер версии программного комплекса, имя (IP-адрес или DNS, например, localhost) сервера ПК, к которому выполнено подключение;
- строку навигации по разделам и вкладкам консоли;
- логин пользователя. При нажатии на имя пользователя открывается меню (рис. 7), описание пунктов которого приведено в таблице 2;
- кнопку вызова меню «  » (рис. 8), описание пунктов которого приведено в таблице 3.

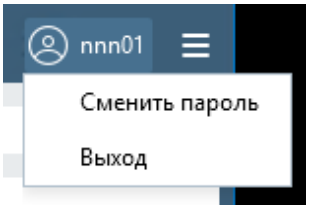


Рисунок 7 – Меню пользователя в клиентской консоли

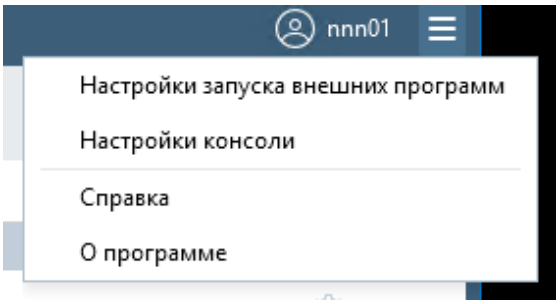


Рисунок 8 – Заголовок клиентской консоли с раскрытым меню

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

Пункт	Описание/Назначение
	(ссылка доступна только для пользователей комплекса с правами *Управление* категории *Администрирование*);

Рисунок 9 – Окно просмотра сведений о программе

В рабочей области (см. рис. 6, поз. 3) 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).

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*).

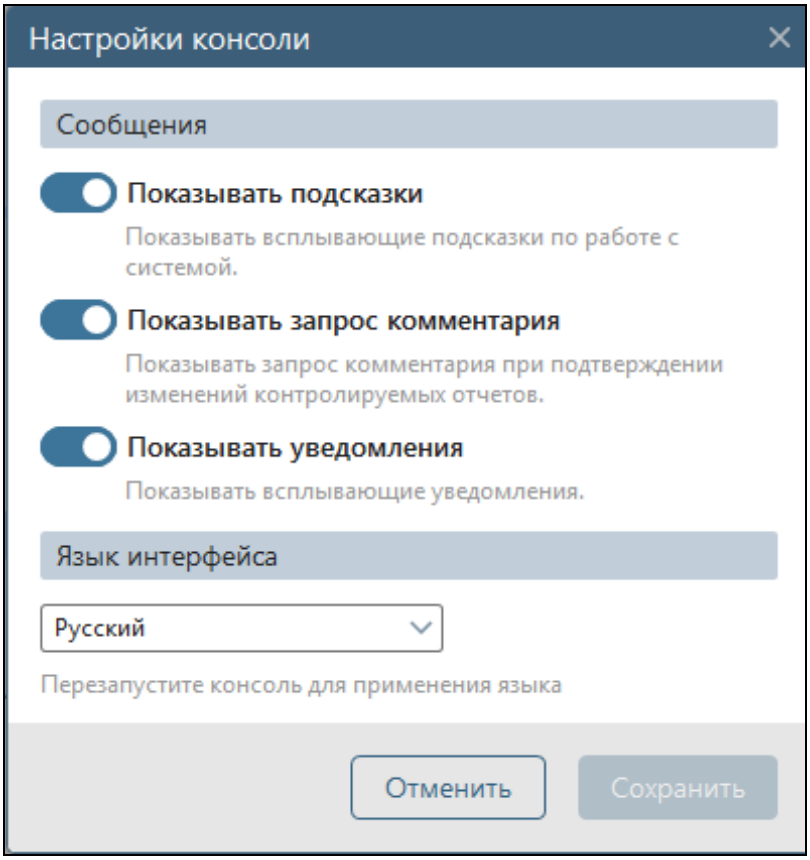


Рисунок 10 – Окно настройки параметров работы клиентской консоли

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.

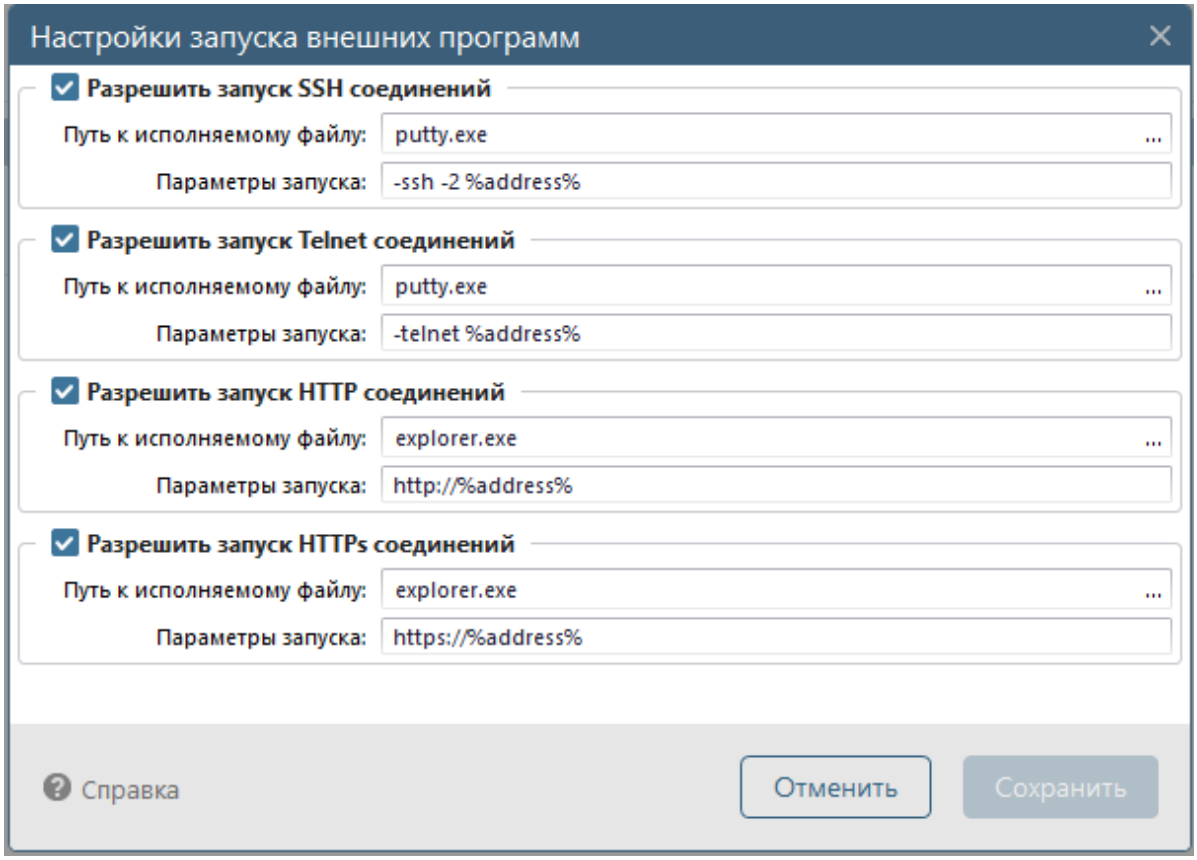


Рисунок 11 – Окно **Настройки запуска внешних программ**

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.

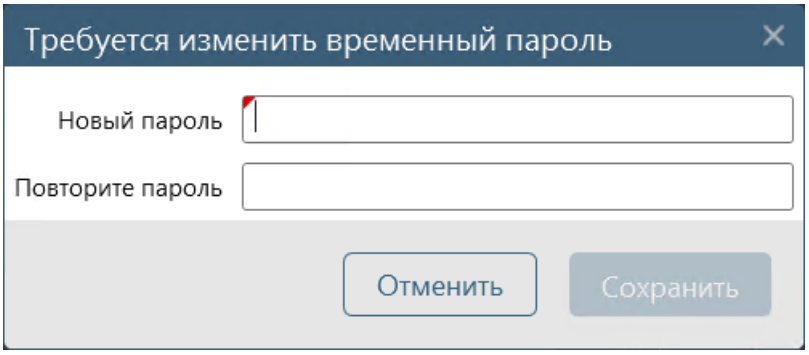


Рисунок 12 – Окно принудительной смены пароля пользователя

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. Настройка комплекса

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

Для перехода в раздел необходимо нажать на соответствующую кнопку в панели выбора раздела клиентской консоли. Откроется форма раздела **Настройки** (рис. 13).

В заголовке панели расположена кнопка ***Сервер***, по нажатию которой открывается окно выбора сервера (рис. 14) со списком доступных для настройки в соответствии с иерархией серверов – текущий сервер и подчиненные ему сервера (если в ПК «Efros Config Inspector» v.4 настроена иерархия подключенных серверов). Выбор сервера выполняется установкой курсора в строке с наименованием требуемого сервера и сохраняется после нажатия кнопки *Выбрать*.

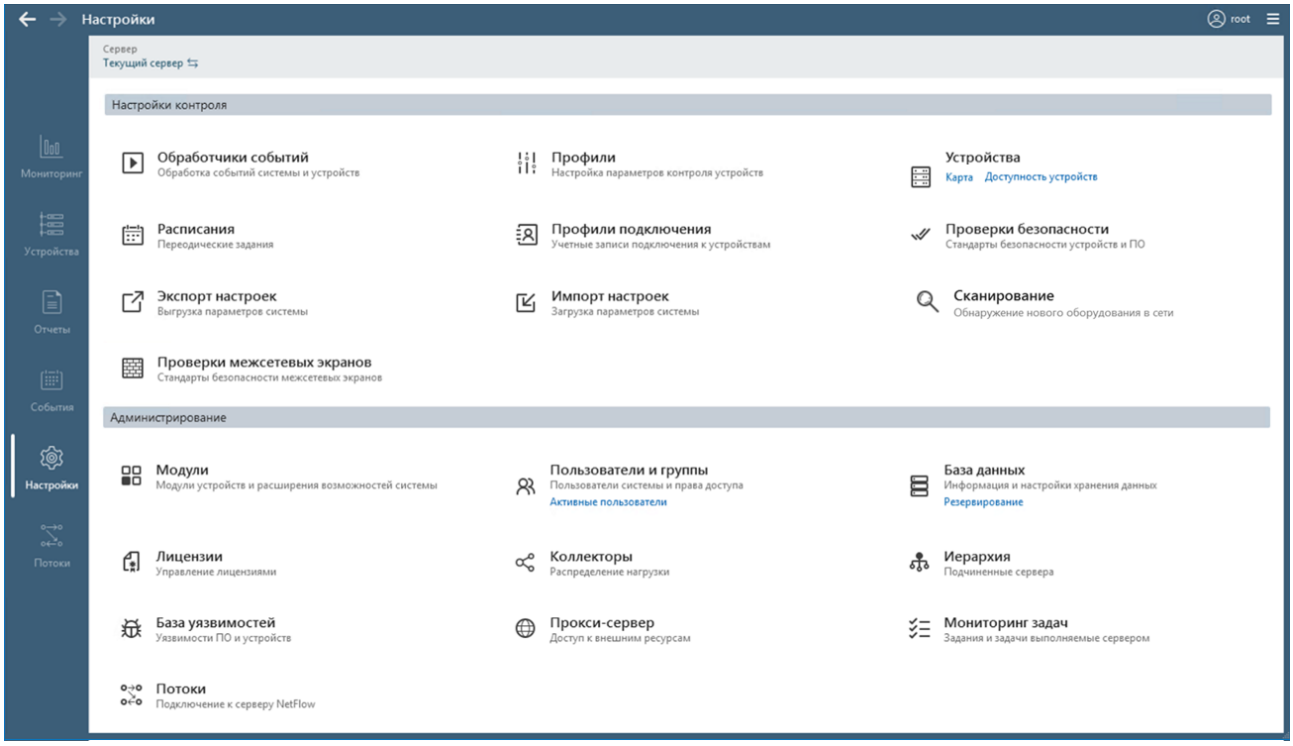


Рисунок 13 – Раздел **Настройки** для текущего сервера (главный в иерархии)

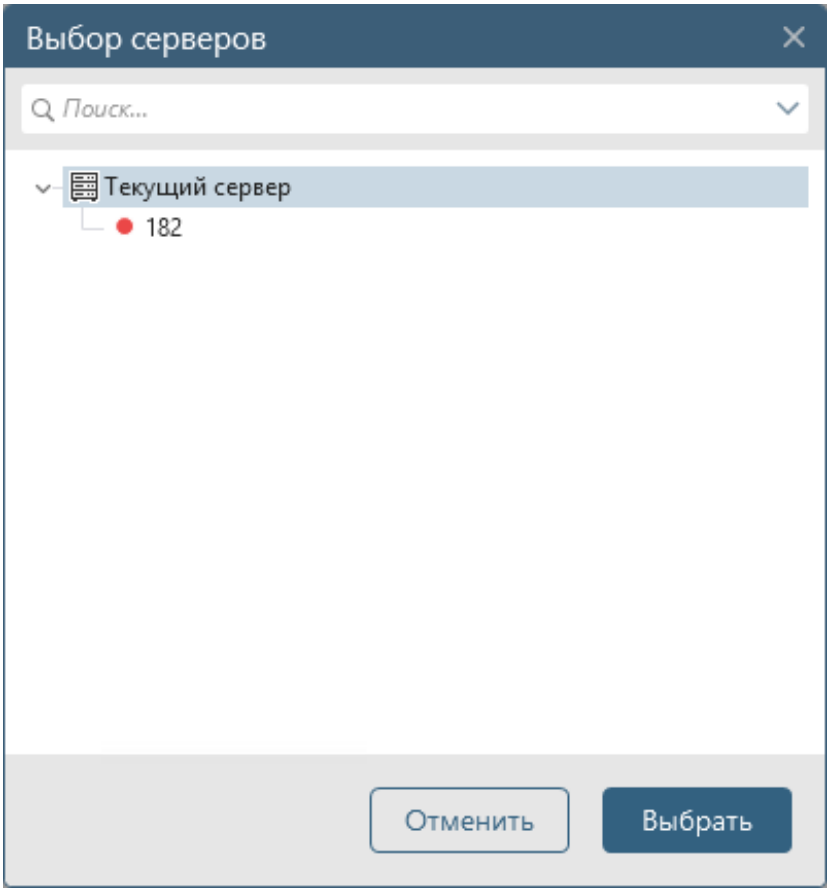


Рисунок 14 – Окно выбора сервера для настройки

Форма раздела **Настройки** содержит панели:

1) Панель **Настройки контроля**. Панель активна только для пользователей с правами *Просмотр* и *Управление* в категории *Настройки контроля* и содержит ссылки для перехода в формы настройки комплекса для работы с контролируемыми устройствами (для пользователей с правами *Просмотр* данные форм настройки доступны только для просмотра, для пользователей с правами *Управление* – для внесения изменения):

- ***Обработчики событий*** – задание триггеров для реакции комплекса на события, которые произошли на устройствах или в комплексе, включение/выключение аудита изменений отчетов для привязки произведенных на устройствах изменений к пользователям (с возможностью подключения к СКДПУ);
- ***Профили*** – управление профилями устройств для гибкой настройки параметров контроля устройств;
- ***Устройства*** – управление и формирование списка устройств, контроль доступности устройств. Дополнительно доступны ссылки:
  а) ***Карта –*** для графического представления топологической карты локальной сети на основе информации контролируемых текущей серверной частью комплекса устройств;
  б) ***Доступность устройств –*** для включения (отключения) функции проверки доступности устройств с указанием интервала в минутах;
- ***Профили подключения*** – настройка параметров аутентификации пользователя на контролируемом текущим сервером ПК оборудовании;
- ***Расписания*** – настройка расписаний загрузки отчетов и выполнения операций с устройствами. Настройка параметров обновления сигнатур уязвимостей ПК «Efros Config Inspector» v.4 из БДУ производителей устройств;
- ***Проверки безопасности –*** создание стандартов и настройка требований проверок безопасности для устройств;
- ***Экспорт настроек*** – экспорт выбранных настроек в файл формата .eci (профилей устройств, пользовательских отчетов и проверок, стандартов проверок МЭ, списка устройств);
- ***Импорт настроек*** – импорт настроек комплекса из выбранного файла формата .eci (поддерживается также импорт списка устройств из файла формата xml от более ранних версий ПК «Efros Config Inspector» v.4);
- ***Сканирование –*** поиск сетевых устройств в локальной сети с возможностью добавления обнаруженных устройств в список устройств, контролируемых комплексом;
- ***Проверки межсетевых экранов*** – добавление стандартов проверок с возможностью анализа движения трафика по зонам (подсетям) и правил МЭ, настройка требований проверок безопасности МЭ.

2) Панель **Администрирование**. Панель активна только для пользователей с правами *Просмотр* и *Управление* в категории *Администрирование* и содержит ссылки для перехода в формы настройки комплекса (для

пользователей с правами *Просмотр* данные форм настройки доступны только для просмотра, для пользователей с правами *Управление* – для внесения изменения):

- ***Модули*** – установка, подключение, отключение, создание пользовательских модулей и настройка внешних модулей комплекса, обеспечивающих работу с устройствами;
- ***Пользователи и группы*** – управление пользователями комплекса и правами доступа (список пользователей комплекса определяет, какие пользователи могут подключаться к серверной части из консоли клиентской части). Дополнительно под кнопкой ***Пользователи и группы*** доступна ссылка ***Активные пользователи*** для просмотра активных в текущий момент сессий пользователей. Возможность изменения настроек пользователя (доступа к настройкам контроля, администрирования комплекса, отключение пользователя);
- ***База данных*** – настройка сроков хранения данных в БД комплекса (используется для экономии места на жестком диске), просмотр информации о БД. Дополнительно под кнопкой ***База данных*** доступна ссылка ***Резервирование*** для просмотра списка резервных серверов;
- ***Лицензии –*** управление лицензионной информацией комплекса;
- ***Коллекторы –*** управление коллекторами: добавление новых коллекторов, настройка коллекторов;
- ***Иерархия –*** управление и настройка главного и подчиненных серверов;
- ***База уязвимостей*** – информация о БДУ ПО и устройств, настройка подключения сервера обновлений;
- ***Прокси-сервер*** – настройка подключения комплекса к прокси-серверу БДУ;
- ***Мониторинг задач*** – просмотр списка задач, текущих и выполненных комплексом;
- ***Потоки*** – настройка и проверка подключения комплекса к серверу «Flow Server».

Перед выполнением настроек необходимо выбрать настраиваемый сервер в поле ***Сервер***. После выбора подчиненного сервера в форме становятся не доступны функции (рис. 15):

- сканирование сети;
- просмотр списка резервных серверов;
- просмотр и управление лицензионной информацией комплекса.

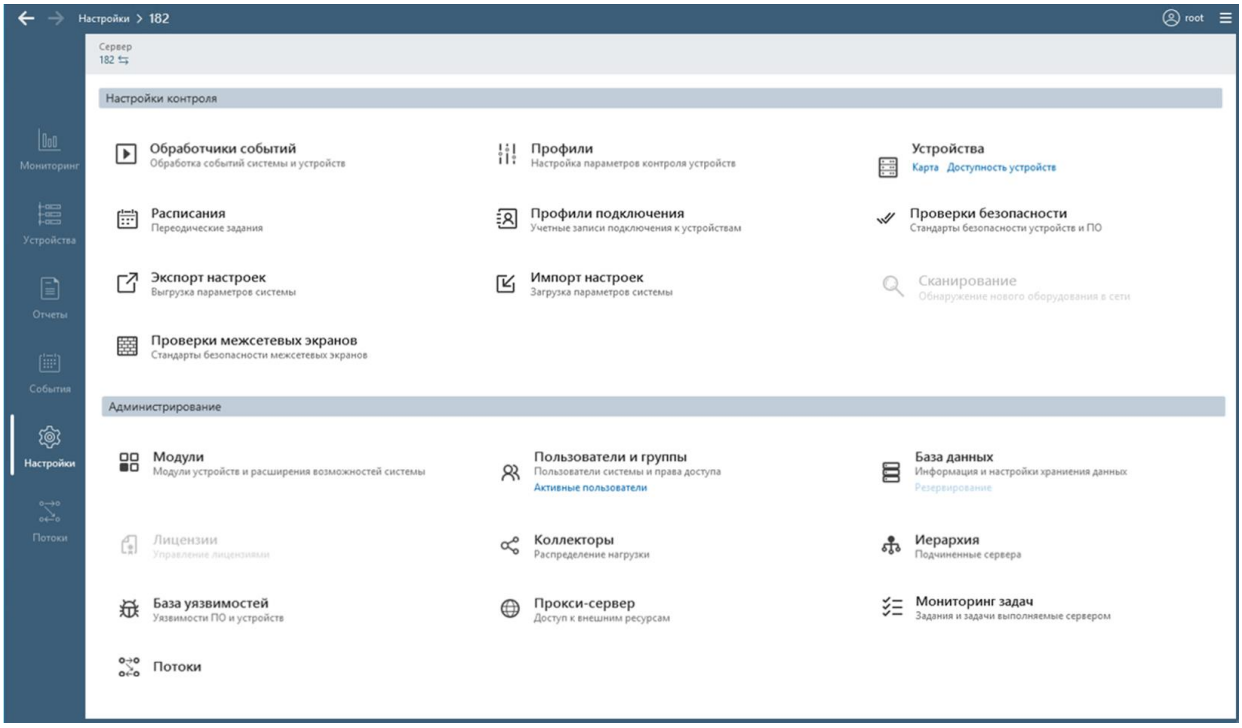


Рисунок 15 – Раздел **Настройки** для подчиненного сервера

Описание выполнения настройки контроля устройств приведено в разделах настоящего документа:

- ***Формирование списка подключенных к комплексу устройств*** (п. 2.3). Настройки задают параметры формирования списка устройств (экспорт, импорт), построения карты сети, доступности устройств;
- ***Сканирование сети –*** поиск сетевых устройств в сети (п. 2.3):
- ***Настройка обработчиков событий (триггеров)*** (п. 2.4). Настройка триггеров задает параметры контроля устройств;
- ***Настройка профилей контроля устройств*** (п. 2.5). Настройка профилей параметров контроля устройств;
- ***Настройка параметров проверок устройств*** (п. 2.8). Настройка задает разрешение/запрет использования для каждого типа проверки правил проверок и исключений из правил проверок;
- ***Настройка расписаний загрузки отчетов устройств*** (п. 2.9). Настройка задает перечень используемых серверной частью комплекса расписаний загрузки отчетов с устройств;
- ***Настройка профилей подключения*** (п. 2.10). Настройка задает параметры авторизации пользователя на контролируемых устройствах, если для аутентификации на устройствах используется одна и та же учетная запись;
- ***Настройка проверок межсетевых экранов*** (п. 2.11). Задание и настройка стандартов зонного анализа, задание требований для стандартов проверок МЭ;
- ***Экспорт настроек комплекса*** (п. 2.12). Экспорт выбранных пользователем настроек комплекса;
- ***Импорт настроек комплекса*** (п. 2.13). Импорт выбранных пользователем настроек комплекса.

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».

2.3. Формирование списка и управление списком устройств

При запуске клиентской консоли и при выборе кнопки ***Устройства*** в клиентской консоли открывается раздел **Устройства**.

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

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).

Описание вкладок и порядок выполнения операций в разделе **Устройства** подробно изложены в документе 643.72410666.00082-01 96 01-03 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 3. Работа с устройствами».

Выполнение действий с устройствами также возможно в разделе **Настройки**. (доступно пользователям с правами *Управление* в категории *Настройки контроля*):

1) Под кнопкой ***Устройства*** в области ***Настройки контроля*** доступны ссылки:
   - ***Карта*** – отображает карту всех устройств сети и связи между ними (п. 2.3.2);
   - ***Доступность устройств*** **–** установка параметров для проверки доступности устройств за определенный период (п. 2.3.3).
2) По нажатию кнопки ***Экспорт настроек*** доступен экспорт списка устройств, а также профилей устройств, пользовательских отчетов и проверок, стандартов проверок МЭ в файл отчета (подробнее см. п. 2.12 «Экспорт настроек комплекса»).
3) По нажатию кнопки ***Импорт настроек*** доступен импорт списка устройств, а также профилей устройств, пользовательских отчетов и проверок, стандартов проверок МЭ из файл (п. 2.13 «Импорт настроек комплекса»)
4) По нажатию кнопки ***Сканирование*** доступно задание параметров сканирования для поиска устройств в сети (п. 2.3.1).

2.3.1. Сканирование устройств

Осуществлять сканирование устройств могут только пользователи с правами *Управление* в категории *Настройки контроля*.

Для сканирования устройств необходимо перейти в раздел **Настройки.** В области *Настройки контроля* нажать кнопку ***Сканирование***. Откроется страница **Сканирование сети** (рис. 16). Страница содержит:

- кнопку ***Сканирование*** (+) – для перехода в окно ввода параметров и запуска нового сканирования сети (см. п. 2.3.3.1 «Запуск нового сканирования»);
- список выполненных ранее сканирований сети.

Для каждого сканирования в списке отображаются данные:

- пиктограмма статуса сканирования:
  - «C» – выполняется;
  - «✓» – успешно завершено;
  - «✕» – завершено с ошибкой или досрочно остановлено пользователем;
- диапазоны сканирования и текущий статус сканирования;
- тип проверки (SSH (с указанием порта), SNMP);
- дата и время начала сканирования и продолжительность сканирования;
- количество обнаруженных устройств (всего и новых), если сканирование завершено с ошибкой, то поле пустое.

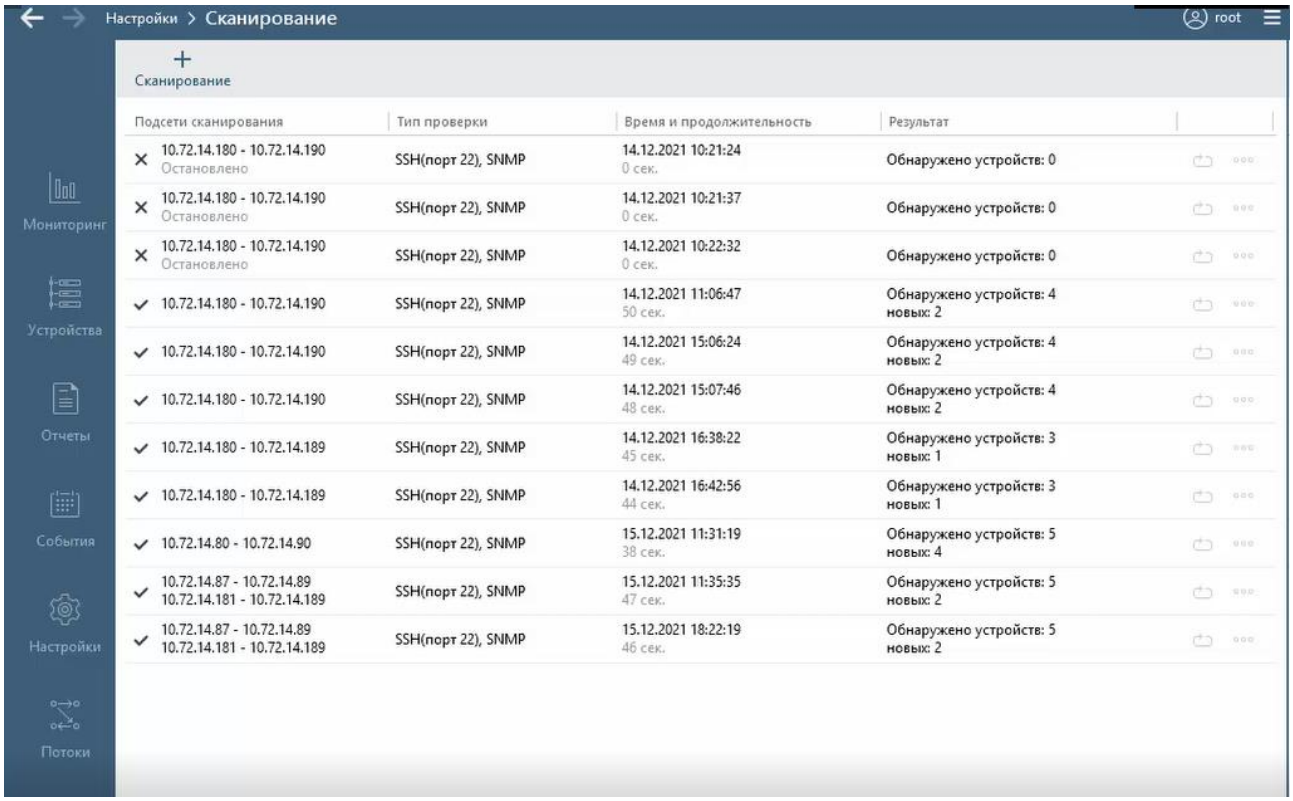


Рисунок 16 – Страница **Сканирование сети**

В списке сканирований пользователь имеет возможность:

- перейти на страницу просмотра результатов сканирования, дважды щелкнув левой кнопкой «мыши» в строке требуемого сканирования, и

добавить новые обнаруженные устройства (подробнее см. п. 2.3.1.3 «Просмотр результатов сканирования и добавление устройств»);
- просмотреть параметры сканирования, нажав в строке требуемого сканирования кнопку ***Меню*** (•••) и выбрав пункт ***Настройки сканирования***;
- удалить запись из списка, нажав в строке удаляемого сканирования кнопку ***Меню*** (•••) и выбрав пункт ***Удалить***;
- запустить сканирование с прежними или новыми параметрами в окне **Параметры сканирования**, которое открывается по нажатию в строке сканирования кнопки ***Повтор сканирования*** ( ) (подробнее см. п. 2.3.1.2 «Повторный запуск сканирования»).

2.3.1.1. Запуск нового сканирования

Для запуска нового сканирования необходимо нажать на странице **Сканирование** кнопку ***Сканирование*** ( ) (см. рис. 16). При этом откроется окно **Новое сканирование** (рис. 17, таблица 4).

В окне необходимо настроить параметры для нового сканирования устройств: задать диапазон (один или несколько) IP-адресов для поиска устройств, выбрать тип и профили подключения (один или несколько) к оборудованию (по SNMP и/или SSH), и нажать кнопку ***Запустить***. В списке сканирований добавится новая строка с данными запущенного сканирования, до завершения процесса сканирования в строке будет отображаться пиктограмма статуса *Выполняется*.

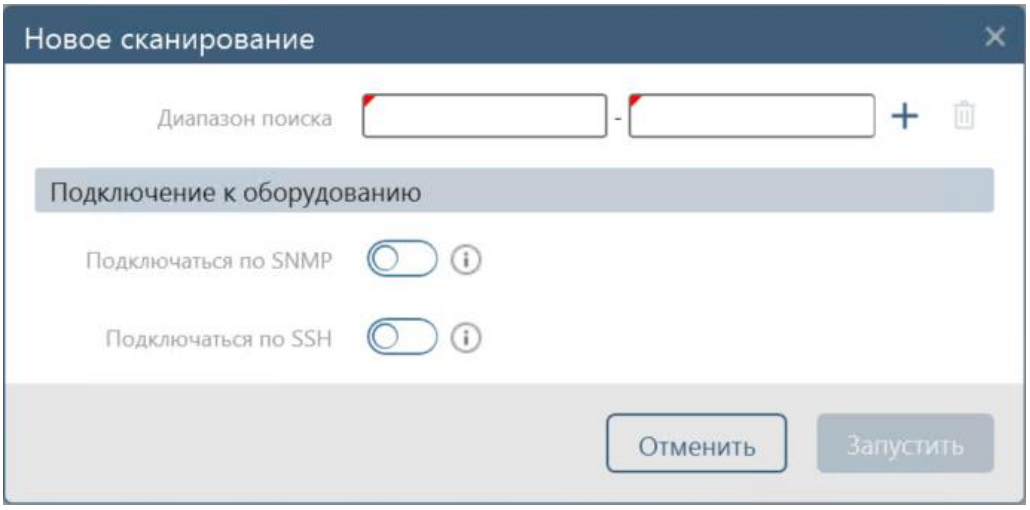


Рисунок 17 – Окно **Новое сканирование**

Таблица 4 – Состав и описание полей окна **Новое сканирование**

Поле	Описание/Назначение
Диапазон поиска	Поля для ввода диапазона сканирования – вводятся IP-адреса, с которых начинается и которыми заканчивается поиск устройств в формате: 0-255.0-255.0-255.0-255 (за исключением 0.0.0.0 и 255.255.255.255). Указать можно несколько диапазонов, поля для ввода нового диапазона добавляются нажатием кнопки «+», ошибочно добавленный диапазон удаляется нажатием кнопки «🗑»

Поле	Описание/Назначение
Блок ***Подключение к оборудованию***	Выбор типа и профилей подключения (один или несколько) к оборудованию
Подключиться по SNMP	Переключатель для включения/отключения режима проверки доступности по протоколу SNMP и выполнения попытки подключения к обнаруженным при сканировании устройствам по выбранным в поле *SNMP профили* (см. ниже) профилям подключения
SNMP профили	Поле со списком профилей подключения типа *Профили SNMP* (ведется в форме управления профилями аутентификации пользователей на устройствах (см. п. 2.10 «Настройка профилей подключения»)). Выбор профилей выполняется установкой флагов в строках требуемых профилей и сохраняется после нажатия кнопки ***Применить***
Подключиться по SSH	Переключатель для включения/отключения режима проверки доступности по протоколу SSH и выполнения попытки подключения к обнаруженным при сканировании устройствам по выбранным в поле *Профили аутентификации* (см. ниже) порту и профилям подключения
Порт подключения	Поле для ввода порта подключения к обнаруженным при сканировании устройствам (по умолчанию порт – 22)
Профили аутентификации	Поле со списком профилей подключения типа *Профили аутентификации* (ведется в форме управления профилями аутентификации пользователей на устройствах (см. п. 2.10 «Настройка профилей подключения»)). Выбор профилей выполняется установкой флагов в строках требуемых профилей и сохраняется после нажатия кнопки ***Применить***

Для просмотра результатов текущего сканирования необходимо дважды щелкнуть левой кнопкой «мыши» в строке сканирования, откроется форма просмотра результатов сканирования со списком найденных на текущий момент времени устройств (рис. 18).

Пользователь имеет возможность:

- просмотреть настройки сканирования, нажав кнопку ***Настройки сканирования***;
- остановить процесс сканирования, для чего навести курсор на кнопку ***Сканирование*** (кнопка заменится кнопкой ***Остановить***) и нажать кнопку ***Остановить***;
- просмотреть результаты сканирования и добавить, при необходимости, найденные новые устройства в соответствии с п. 2.3.1.3 «Просмотр результатов сканирования и добавление устройств».

Рисунок 18 – Форма просмотра результатов текущего сканирования

После завершения сканирования в строке сканирования отобразится пиктограмма:

- ✓ – при успешном завершении сканирования;
- ✕ – при завершении сканирования с ошибкой или при досрочной остановке сканирования пользователем.

2.3.1.2. Повторный запуск сканирования

Для повторного запуска сканирования необходимо;

1) Перейти в раздел **Настройки**.
2) В области *Настройки контроля* нажать кнопку ***Сканирование***.
3) В списке открывшейся страницы сканирований нажать кнопку ***Повтор сканирования*** (↻) в строке повторяемого сканирования.
4) В открывшемся окне **Настройки сканирования** (рис. 19) просмотреть заданные ранее параметры сканирования, внести, при необходимости, изменения в соответствии с таблицей 4.
5) Нажать кнопку ***Запустить***.

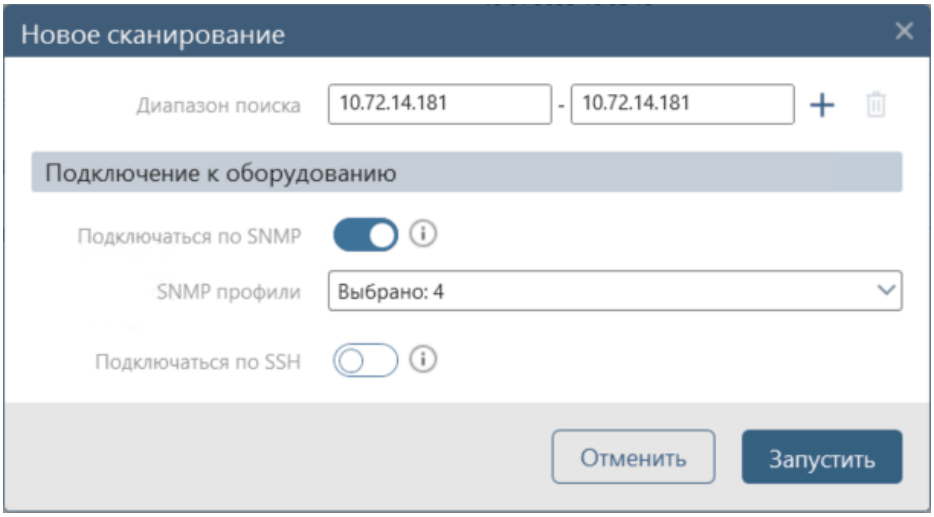


Рисунок 19 – Окно **Новое сканирование**

В списке сканирований добавится новая строка с данными запущенного сканирования, до завершения процесса сканирования в строке будет отображаться пиктограмма статуса *Выполняется*.

После завершения сканирования в строке сканирования отобразится пиктограмма:

- ✓ – при успешном завершении сканирования;
- ✕ – при завершении сканирования с ошибкой или при досрочной остановке сканирования пользователем.

Пользователь имеет возможность просмотреть результаты сканирования, дважды щелкнув левой кнопкой «мыши» в строке сканирования, и добавить, при необходимости, найденные новые устройства в соответствии с п. 2.3.1.3 «Просмотр результатов сканирования и добавление устройств».

2.3.1.3. Просмотр результатов сканирования и добавление устройств

Для просмотра результатов сканирования сети пользователю необходимо в списке сканирований страницы **Сканирование** дважды щелкнуть левой кнопкой «мыши» в строке требуемого сканирования. Откроется форма просмотра результатов сканирования со списком найденных при сканировании устройств (рис. 20).

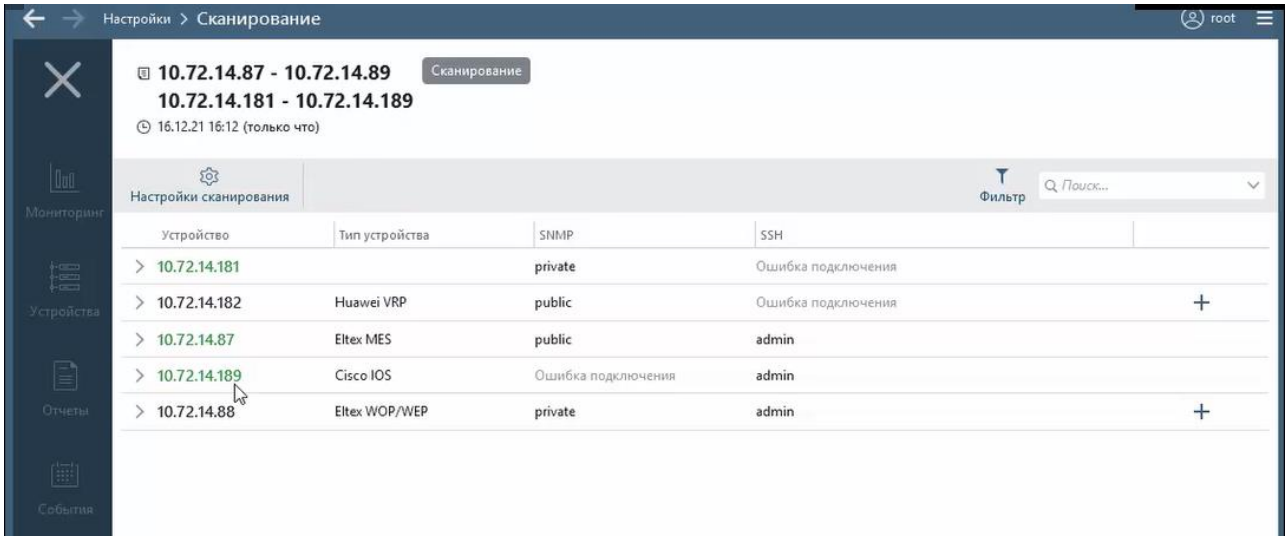


Рисунок 20 – Форма просмотра результатов сканирования

Форма содержит:

- заголовок – диапазоны сканирования, дата и время запуска сканирования;
- кнопку ***Настройки сканирования*** (+) – для перехода в окно просмотра параметров сканирования (рис. 21);
- кнопку ***Фильтр*** (▼) – для перехода в окно фильтрации списка устройств по результату попытки подключения по SNMP и SSH (*успешное подключение, порт недоступен, ошибка подключения*), по наличию устройства в списке комплекса (*новое, есть в системе*) и сброса настройки фильтра;
- поле поиска устройств;

– список найденных устройств – представлен в виде таблицы (описание граф таблицы приведено в таблице 5), каждой строке таблицы соответствует результат выполнения поиска по данному адресу. Зеленым цветом шрифта выделены устройства уже имеющиеся в списке устройств комплекса, черным – найденные новые устройства.

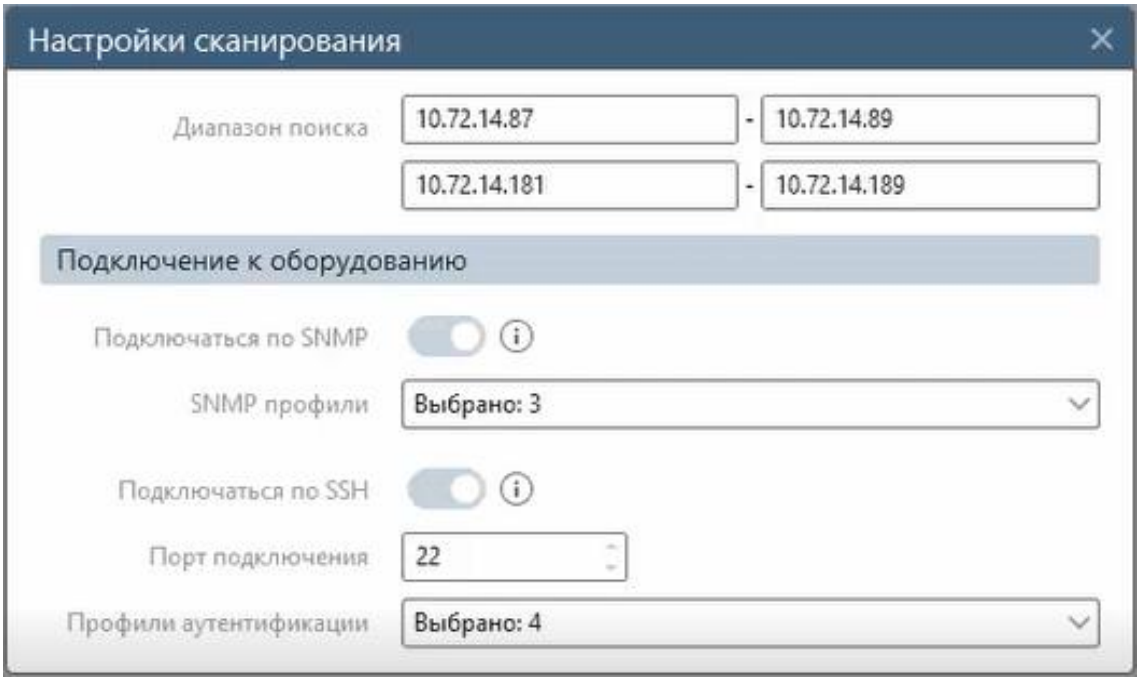


Рисунок 21 – Окно **Настройки сканирования**

Таблица 5 – Описание граф таблицы результатов сканирования

Пункт	Описание/Назначение
Устройство	IP-адрес обнаруженного устройства
Тип устройства	Тип обнаруженного устройства (список поддерживаемых типов устройств можно посмотреть в разделе 1)
SNMP	Наименование профиля SNMP, по которому выполнено подключение по протоколу *SNMP.* Значение *Ошибка подключения* означает, что выполнение запроса по протоколу SNMP показало, что по данному IP-адресу устройство, поддерживающее протокол SNMP, не обнаружено
SSH	Наименование профиля аутентификации, по которому выполнено подключение по протоколу *SSH.* Значение *Ошибка подключения* означает, что выполнение запроса по протоколу SSH показало, что по данному IP-адресу устройство, поддерживающее протокол SSH, не обнаружено

Для просмотра подробной информации об устройстве (рис. 22) необходимо нажать слева от его IP-адреса кнопку «›».

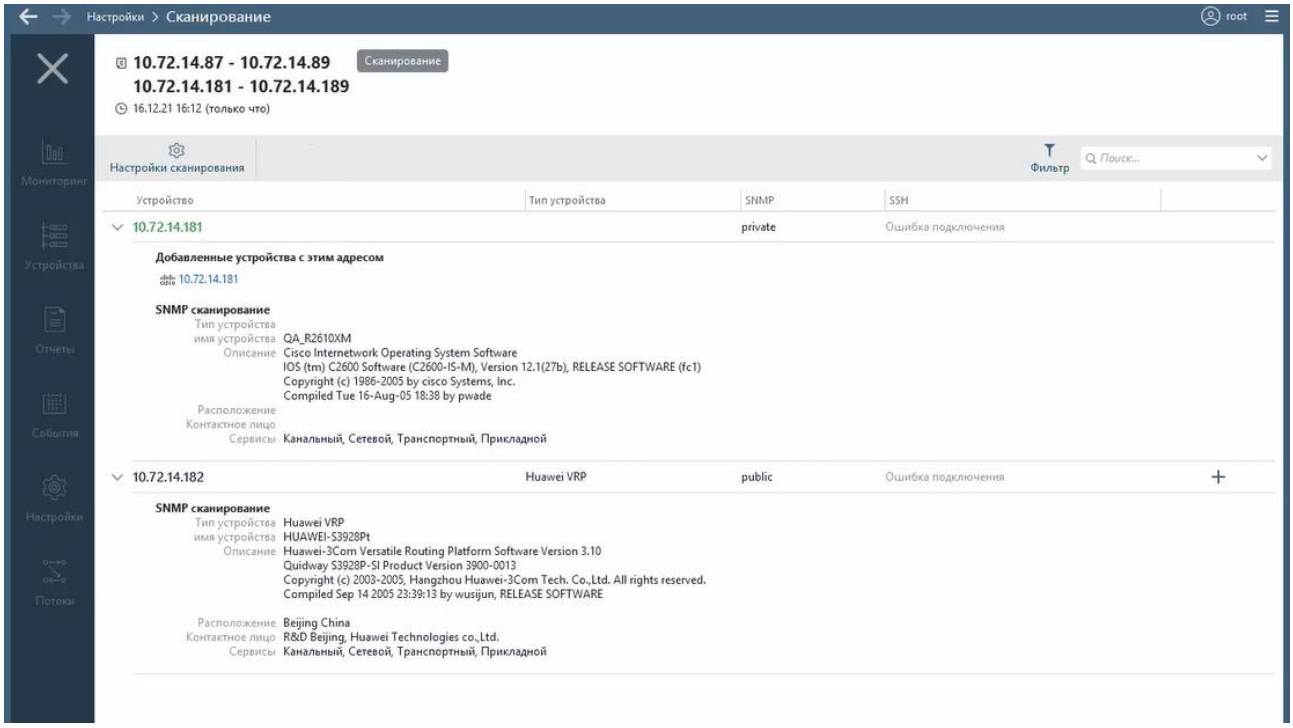


Рисунок 22 – Таблица найденных устройств с подробной информацией об устройствах

В строке каждого нового обнаруженного устройства находится кнопка ***Добавить.*** Для добавления в список устройств комплекса нового устройства необходимо:

- нажать кнопку ***Добавить***. Откроется окно добавления нового устройства (рис. 23);
- поля окна автоматически будут заполнены данными устройства. Если не распознан тип устройства, то поле ***Тип*** не заполняется;
- проверить корректность отобразившихся данных, внести, при необходимости, изменения в данные и добавить отсутствующие данные;
- нажать кнопку ***Добавить***.

Подробное описание полей окна и правил добавления устройств в список устройств, контролируемых комплексом, приведено в документе 643.72410666.00082-01 96 01-03 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 3. Работа с устройствами».

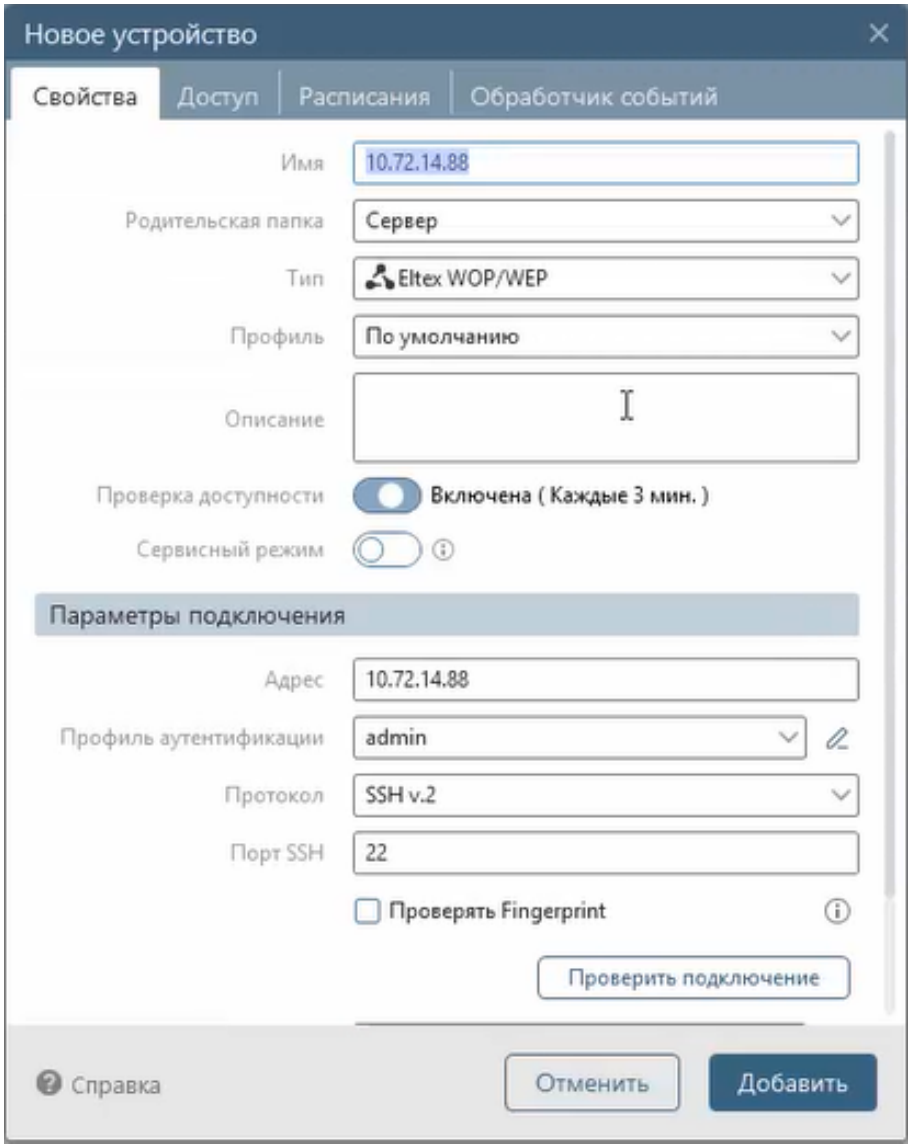


Рисунок 23 – Окно **Новое устройство**

2.3.1.4. Удаление записи о сканировании

Для удаления записи о сканировании необходимо:

1) Перейти в раздел **Настройки**.
2) В области *Настройки контроля* нажать кнопку ***Сканирование***.
3) В списке открывшейся страницы сканирований нажать кнопку ***Меню*** (•••) в строке удаляемого сканирования.
4) В открывшемся меню выбрать пункт ***Удалить***.
5) Нажать в окне подтверждения кнопку ***Удалить***.

2.3.2. Карта сети

Просмотр карты сети доступен пользователям с правами *Просмотр* и *Управление* в категории *Настройки контроля.*

Для просмотра карты сети необходимо перейти в раздел **Настройки.** В области *Настройки контроля* нажать на ссылку ***Карта*** под кнопкой ***Устройства***. Откроется окно **Карта сети** (рис. 24), в котором содержится карта всех устройств,

подключенных к комплексу (их имена, статус, а также связи между ними через подсети).

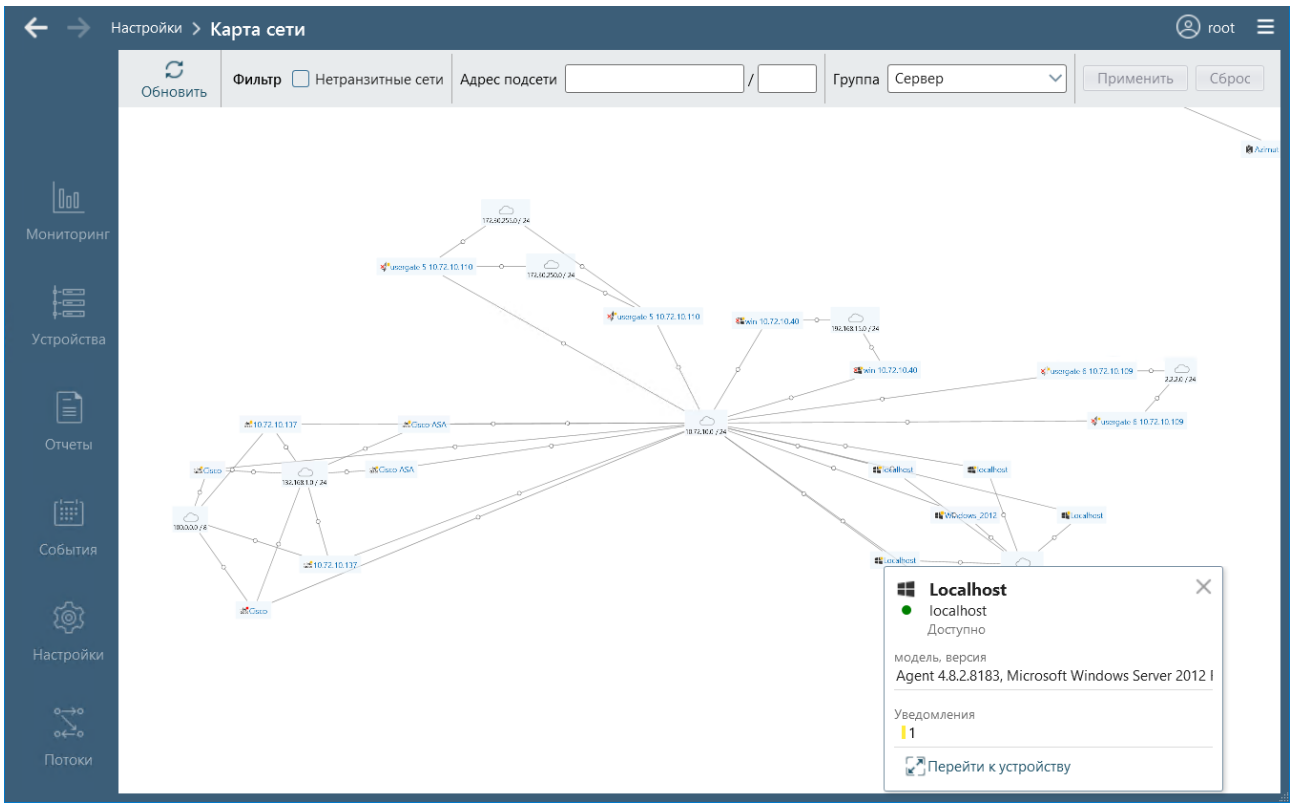


Рисунок 24 – Окно **Карта сети**

Связи устройств строятся на основании данных, полученных из последних загруженных конфигураций.

Окно **Карта сети** содержит следующие настраиваемые параметры:

- кнопка ***Обновить*** (🔄) – обновляет отображение элементов **Карты сети**;
- фильтр ***Нетранзитные сети*** – при установке данного параметра, в окне **Карта сети** будут отображены в том числе и сети, через которые не происходит взаимодействие устройств;
- в поле ***Адрес*** вводится диапазон IP-адресов устройств, которые необходимо отобразить;
- ***Группа*** – раскрывающийся список (отображается в соответствии с группировкой устройств во вкладке ***Устройства***), в котором можно выбрать отображаемую группу устройств;
- кнопка ***Применить*** – используется для применения выбранных параметров фильтрации.

При нажатии на любое отображенное устройство, доступна к просмотру карточка устройства (см. рис. 24), 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). Из карточки устройства можно перейти на вкладку ***Статус*** раздела **Устройства**, нажав кнопку ***Перейти к устройству***, расположенную в нижней части карточки.

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

2.3.3. Доступность устройств

Настройка доступности устройств доступна пользователям с правами *Управление* в категории *Настройки контроля.*

Для установки параметров проверки доступности устройств необходимо перейти в раздел **Настройки.** В области *Настройки контроля* нажать на ссылку ***Доступность устройств*** под кнопкой ***Устройства***.

Откроется форма установки параметров для проверки доступности устройств в ПК «Efros Config Inspector» v.4 (рис. 25), содержащая:

- переключатель ***Статус проверки*** – включает или отключает функцию проверки доступности устройств;
- поле ***Период*** – для выбора периода, через который происходит проверка доступности всех устройств (возможные значения – от 1 до 1440 минут);
- кнопку ***Применение для устройств*** – для перехода в окно просмотра/настройки применимости разрешения проверки доступности для типов устройств (рис. 26).

Доступность устройств проверяется с помощью ICMP Ping и учитывает последние данные о работе комплекса с устройством (подключение и задачи по выбранным протоколам).
При нажатии на кнопку ***Сохранить*** с включенным **Статусом проверки** проверка доступности устройств будет осуществляться автоматически через заданный промежуток времени в параметре **Период**.

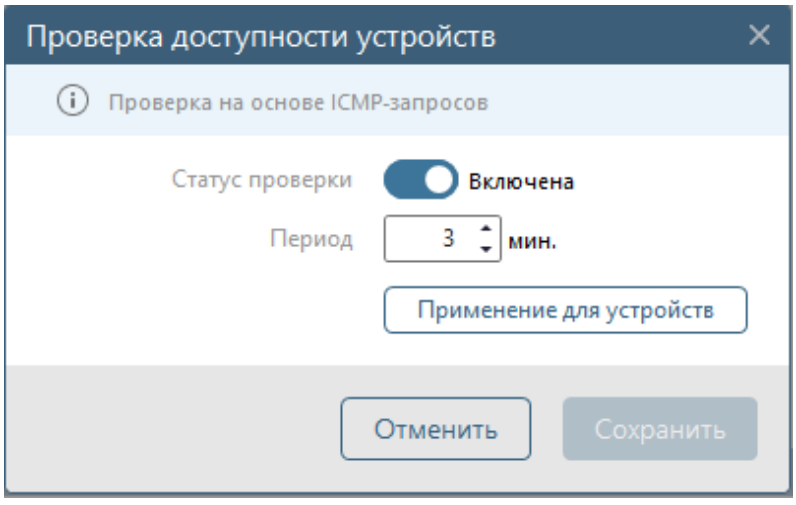


Рисунок 25 – Форма **Проверка доступности устройств**

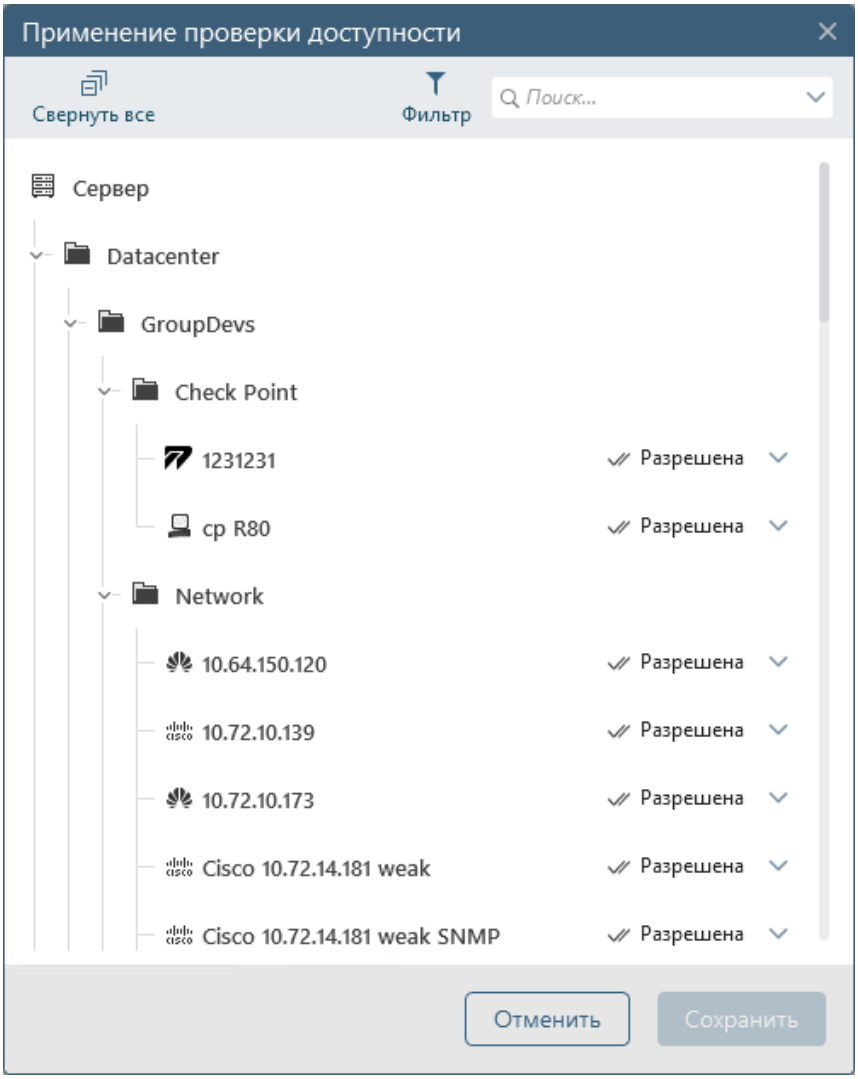


Рисунок 26 – Окно просмотра/настройки применимости разрешения проверки доступности для типов устройств

2.4. Настройка обработчиков событий

2.4.1. Просмотр списка триггеров

Для просмотра списка триггеров необходимо перейти в раздел **Настройки**, для чего в консоли нажать соответствующую кнопку на панели выбора раздела, выбрать сервер, список обработчиков событий которого просматривается (нажать кнопку ***Сервер*** и выбрать в открывшемся окне **Выбор сервера** строку требуемого сервера), и в панели ***Настройки контроля*** нажать ссылку *Обработчики событий*. Откроется форма настройки обработчиков событий (триггеров) выбранного сервера.

Форма содержит (рис. 27):

- кнопку ***Обработчик*** (+) – для перехода в форму добавления триггера (см. п. 2.4.2 «Добавление триггера»);
- кнопку ***Аудит изменений*** () – для перехода в окно включения/выключения загрузки отчетов при получении событий об изменении конфигурации устройства и включения/выключения режима подключения к СКДПУ (см. п. 2.4.6 «Аудит изменений»);

- кнопку ***Фильтр*** (▼) – для перехода в окно фильтрации триггеров по их активности (выбор выполняется установкой флагов одном или обоих полях: *Активные*, *Отключенные*) и сброса настройки фильтра;
- поле поиска триггеров;
- список имеющихся в текущей серверной части комплекса обработчиков событий (триггеров).

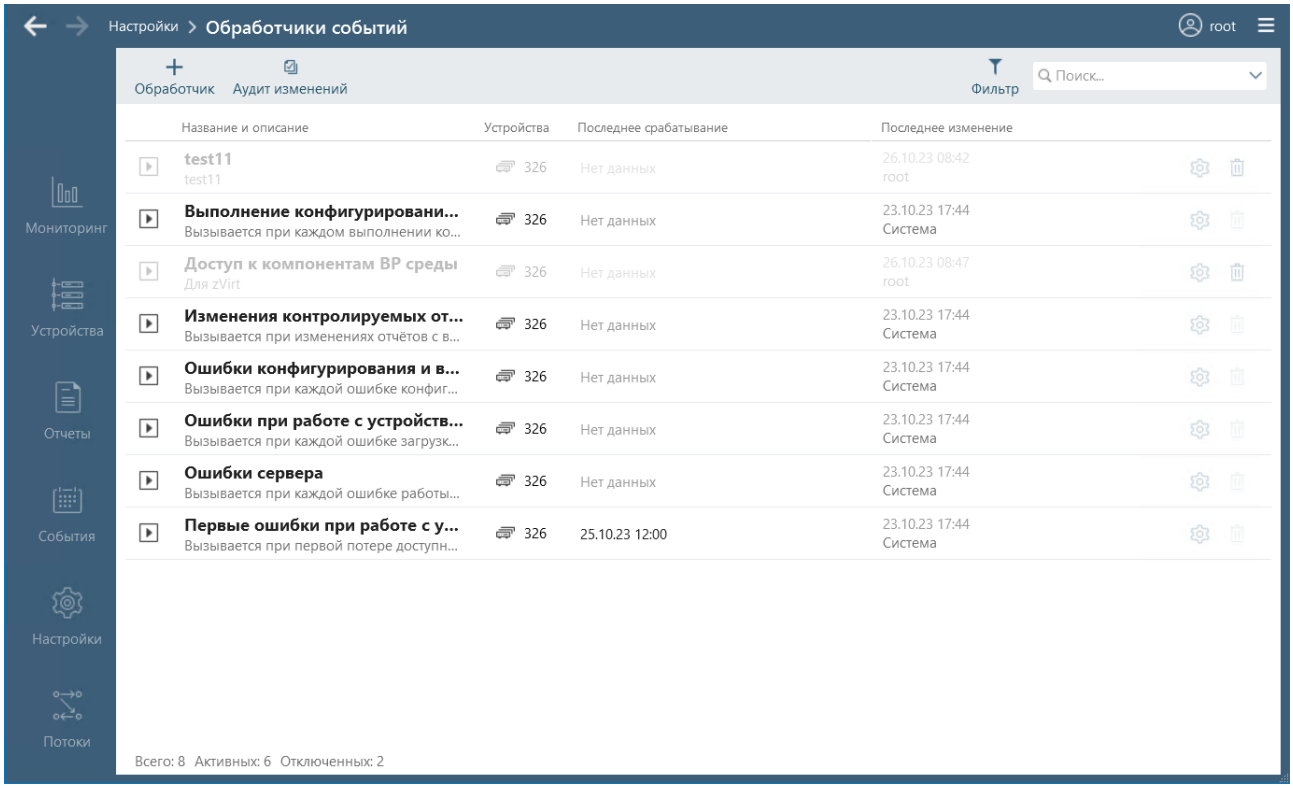


Рисунок 27 – Форма настройки триггеров

По умолчанию в списке триггеров отображаются как активные, так и отключенные триггеры. В нижней части вкладки приведены данные об общем количестве триггеров, количестве активных и отключенных на текущий момент времени триггеров.

Наименования неактивных обработчиков событий отображаются затененными. Активность триггера настраивается при внесении изменений в триггер (см. п. 2.4.3 «Изменение триггера»). При выборе встроенного триггера возможно добавление и настройка действий триггера.

Пользователь имеет возможность в окне фильтрации (открывается по нажатию кнопки ***Фильтр***) установкой флагов задать отображение только активных или только отключенных триггеров. Для отмены фильтрации – нажать в окне фильтрации ссылку ***Сбросить фильтр***.

Для каждого триггера в списке отображаются:

- название и описание;
- количество устройств, для которых триггер применяется;
- дата и время последнего срабатывания триггера в формате: дд.мм.гггг чч:мм;

- дата и время последнего изменения триггера в формате: дд.мм.гггг чч:мм;
- кнопка ***Изменить*** (⚙) – для перехода в форму настройки использования триггера для устройств (см. п. 2.4.3 «Изменение триггера»);
- кнопка ***Удалить*** (🗑) – для удаления триггера (см. п. 2.4.5 «Удаление триггера»).

Примечание – При двойном щелчке в строке триггера открывается окно настройки триггера (см. п. 2.4.3 «Изменение триггера»).

Триггеры ***Выполнение конфигурирования и восстановления***, ***Изменения контролируемых отчетов, Ошибки конфигурирования и восстановления, Ошибки при работе с устройством, Ошибки сервера, Первые ошибки при работе с устройством*** являются встроенными (автоматически создаются при инсталляции комплекса) – удалить их, изменить их название, описание и условия их выполнения невозможно.

2.4.2. Добавление триггера

Добавлять и настраивать триггеры на сервере ПК могут только пользователи с правами *Управление* в категории *Настройки контроля*.

Для добавления обработчика событий на сервер ПК пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, для чего в консоли нажать соответствующую кнопку на панели выбора раздела.
2) Выбрать сервер, для которого добавляется триггер.
3) В области ***Настройки контроля*** нажать ссылку *Обработчики событий*.
4) Нажать в заголовке открывшейся формы ***Обработчики событий*** кнопку ***Обработчик*** (+) (см. рис. 27).
5) В открывшемся окне добавления нового триггера (рис. 28, состав и описание вкладок и полей формы приведены в таблице 6) необходимо:

а) в панели общих параметров:

- установить переключатель в поле ***Активность*** в положение *Включено* (🔘);
- заполнить поля ***Имя*** и, при необходимости, ***Описание***.

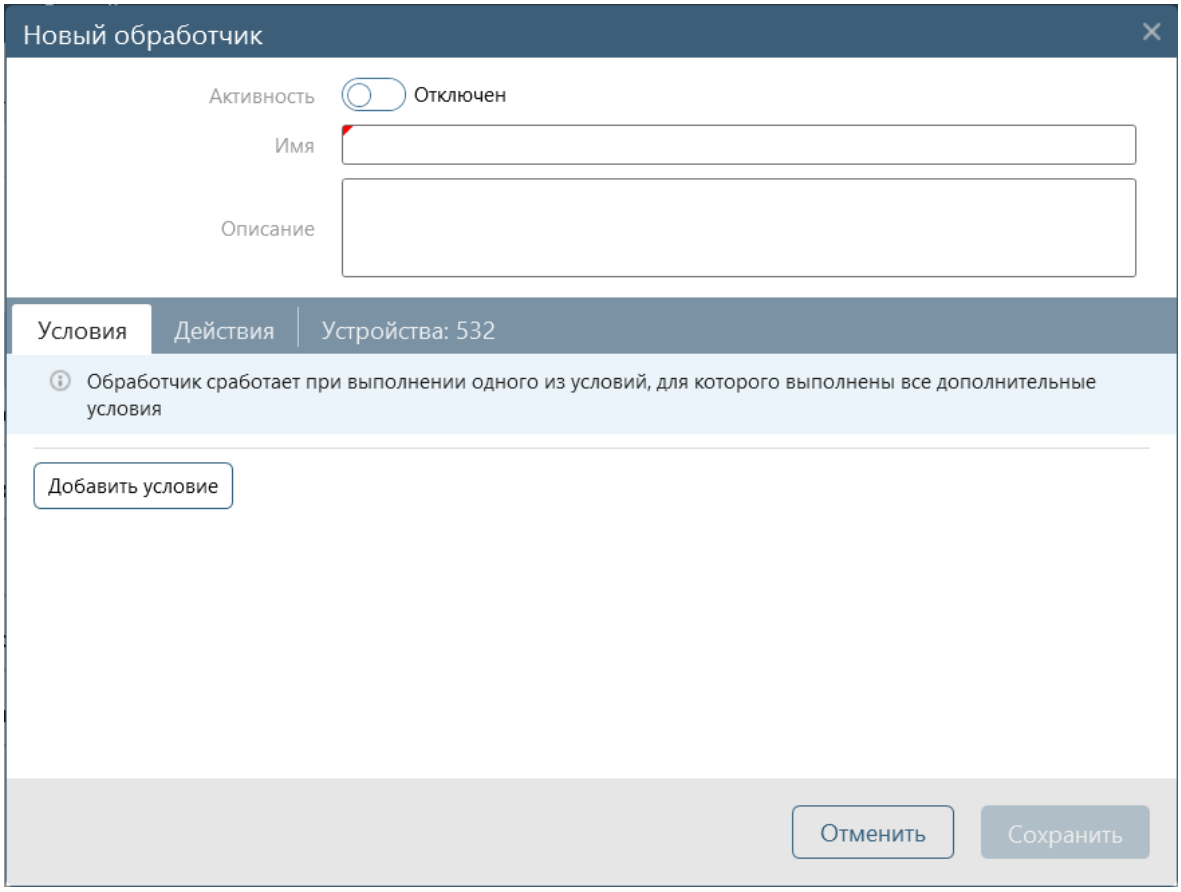


Рисунок 28 – Форма создания триггера

Таблица 6 – Состав и описание вкладок и полей формы создания правил обработки событий

Поле	Описание/Назначение
Панель общих параметров	
Активность	При установленном переключателе осуществляется обработка событий, при снятом – триггер выключен
Имя	Название триггера
Описание	Описание триггера
Вкладка Условия	Выбор условий для выполнения правил обработки событий
Кнопка *Добавить условие*	По нажатию кнопки открывается список событий для выбора типа контролируемого события. Доступные для выбора события: – *Восстановление конфигурации;* – *SVMM/Hyper-V Доступ субъектов доступа к компонентам виртуальной среды;* – *Запуск Windows агента;* – *vCenter/ESXi Доступ субъектов доступа к компонентам виртуальной среды;* – *Выполнение конфигурирования;* – *SVMM/Hyper-V Изменения правил разграничения доступа к компонентам среды виртуализации;* – *vCenter/ESXi Запуск (завершение) работы компонентов виртуальной среды;* – *Изменение доступности;* – *Обновление словаря уязвимостей;*

Поле	Описание/Назначение
	– *Переключение основного сервера;* – *DATAPK инцидент;* – *SNMP Trap сообщение;* – *SVMM/Hyper-V Запуск (завершение)работы компонентов виртуальной среды;* – *vCenter/ESXi Изменения правил разграничения доступа к компонентам среды виртуализации;* – *Запуск действий по триггеру;* – *Syslog сообщение;* – *Загрузка отчета;* – *Экспорт отчетов;* – *Аудит;* – *Изменение результата проверки;* – *Изменение результата последней операции;* – *Нарушение целостности;* – *Выполнение операции;* – *Запуск задания по расписанию;* – *Syslog сообщение;* – *DATAPK сообщение;* – *Изменение отчета.* После выбора события его наименование отображается во вкладке, ниже вновь отображается кнопка *Добавить условие*. Пользователь имеет возможность добавить следующее событие
Дополнительные условия	Ссылка, отображается для каждого добавленного события. По нажатию ссылки отображаются поля для ввода дополнительных условий для соответствующего типа события
Вкладка Действия	Для определения действий, которые должны быть выполнены комплексом при выполнении условий, заданных во вкладке ***Условия***
Кнопка *Добавить действие*	По нажатию кнопки открывается список для выбора действия, которое должно быть выполнено при срабатывании триггера. Доступные для выбора действия: – *Создать уведомление;* – *Выполнить операцию «Проверить соединение»;* – *Отправить Syslog-сообщение* (при условии подключения модуля); – *Загрузить отчеты;* – *Отправить сообщение через Lync* (при условии подключения модуля); – *Отправить сообщение через Exchange* (при условии подключения модуля); – *Отправить письмо* (при условии подключения модуля); – *Экспортировать событие* (при условии подключения модуля). После выбора действия его наименование отображается во вкладке, ниже отображаются поля для настройки его выполнения и кнопка ***Добавить действие***. Пользователь имеет возможность добавить следующее действие. Для выбранного типа действия необходимо задать настройки для его выполнения. В зависимости от типа действия доступны настройки: – *Создать уведомление* – поле выбора статуса уведомления. Возможные значения: *Критично*, *Предупреждение*,

Поле	Описание/Назначение
	Информация; – *Выполнить операцию 'Проверить соединение', Загрузить отчеты* – выбор устройств для которых будет выполняться указанное действие: *На источнике события* или *на определенных устройствах*; – *Экспортировать событие* – не содержит настроек; – *Отправить сообщение через Lync, Отправить письмо* – поле ввода адресов получателей сообщений (писем), разделенные точкой с запятой; – *Отправить Syslog-сообщение* – поля *Адрес Syslog сервера, Протокол, TCP/UDP порт*, *Важность* и флаг *Добавить в сообщение IP-адрес и имя устройства* соответственно для задания адреса Syslog сервера, протокола обмена *(TCP* или *UDP (*по умолчанию*))*, порта Syslog сервера (по умолчанию для протокола *TCP – 1468,* для протокола *UDP – 514*), уровня важности, присваиваемого сообщению (значения от *Emergency* до *Debug,* по умолчанию *Notice*) и установки необходимости добавления в сообщение IP-адреса и имени устройства. Существует также возможность отправки тестового сообщения из окна создания триггера, нажав ссылку ***Выполнить проверочное действие***
Вкладка Устройства	Для настройки использования триггера для устройств (групп) сервера ПК. Вкладка содержит всю иерархию папок и устройств, контролируемых текущей серверной частью комплекса, с текущим статусом использования триггера

б) во вкладке ***Условия*** окна добавления триггера:
- нажать кнопку ***Добавить условие*** и выбрать в раскрывшемся списке тип события, при совершении которого ожидается реакция системы;
- при необходимости указать для выбранного события дополнительные условия, для чего:
  - нажать ссылку ***Дополнительные условия***;
  - в добавленной строке (рис. 29) из раскрывающегося списка первого поля выбрать параметр события, для которого задается условие, во втором поле (при его наличии) выбрать требуемое условие из списка и ввести значение параметра;
  - при необходимости, добавить еще дополнительные условия, нажав кнопку «+»;
  - удалить неактуальные дополнительные условия, нажав соответствующую кнопку «🗑»;
- при необходимости добавить еще типы событий, на которые будет реагировать комплекс, и задать для них условия;
- удалить неактуальные типы событий, нажав соответствующую кнопку «🗑».

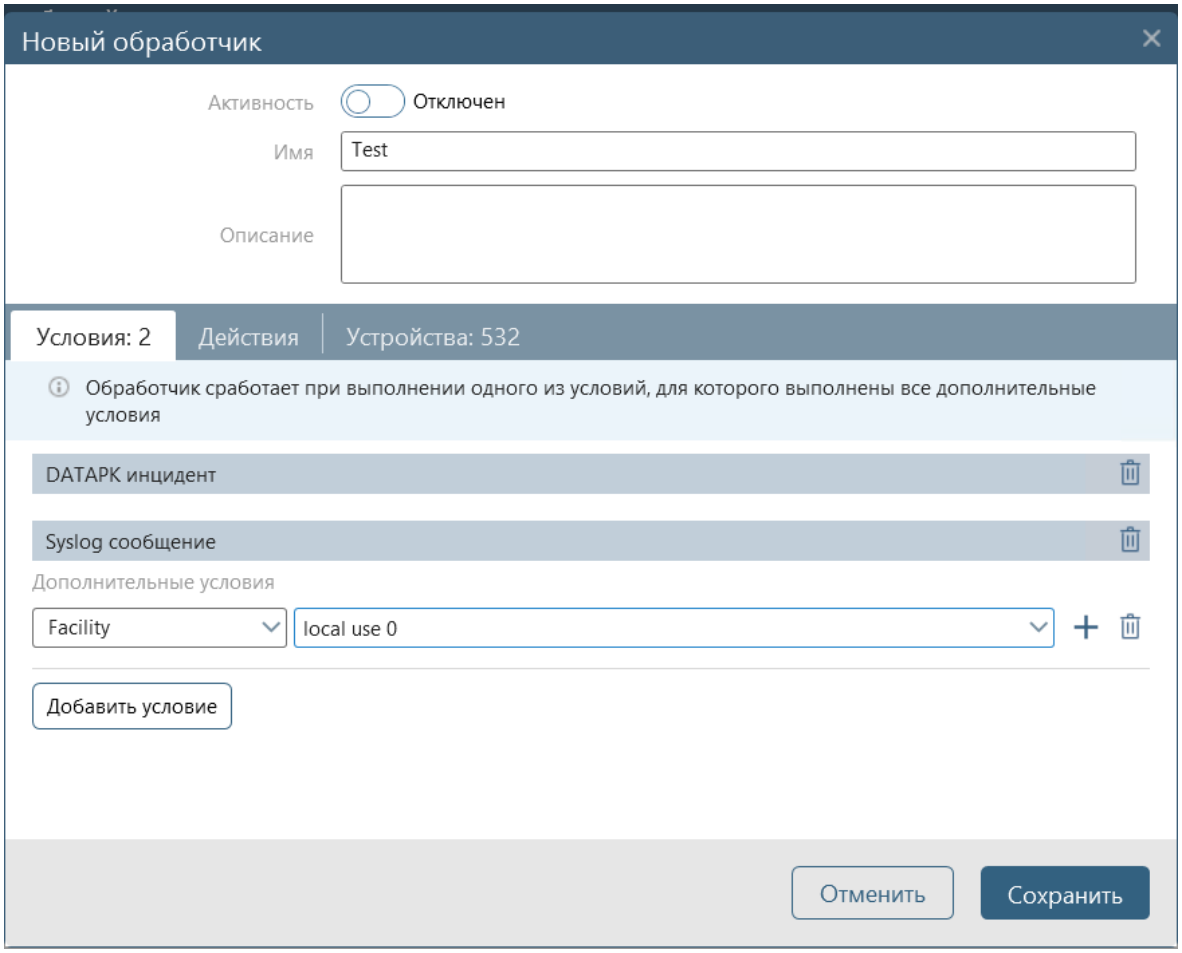


Рисунок 29 – Выбор типа события и дополнительных условий для задания условия триггера

в) во вкладке ***Действия*** окна добавления триггера (рис. 30):
- нажать кнопку ***Добавить действие*** и выбрать в раскрывшемся списке тип действия, которое будет выполнено на сервере ПК в ответ на произошедшее событие (рис. 31);
- задать для выбранного типа действия настройки (описание параметров настроек и их возможные значения приведено в таблице 6);
- при необходимости добавить действия, которые будут выполняться в ответ на события, указанные во вкладке ***Условия;***
- удалить неактуальные действия, нажав соответствующую кнопку «🗑».

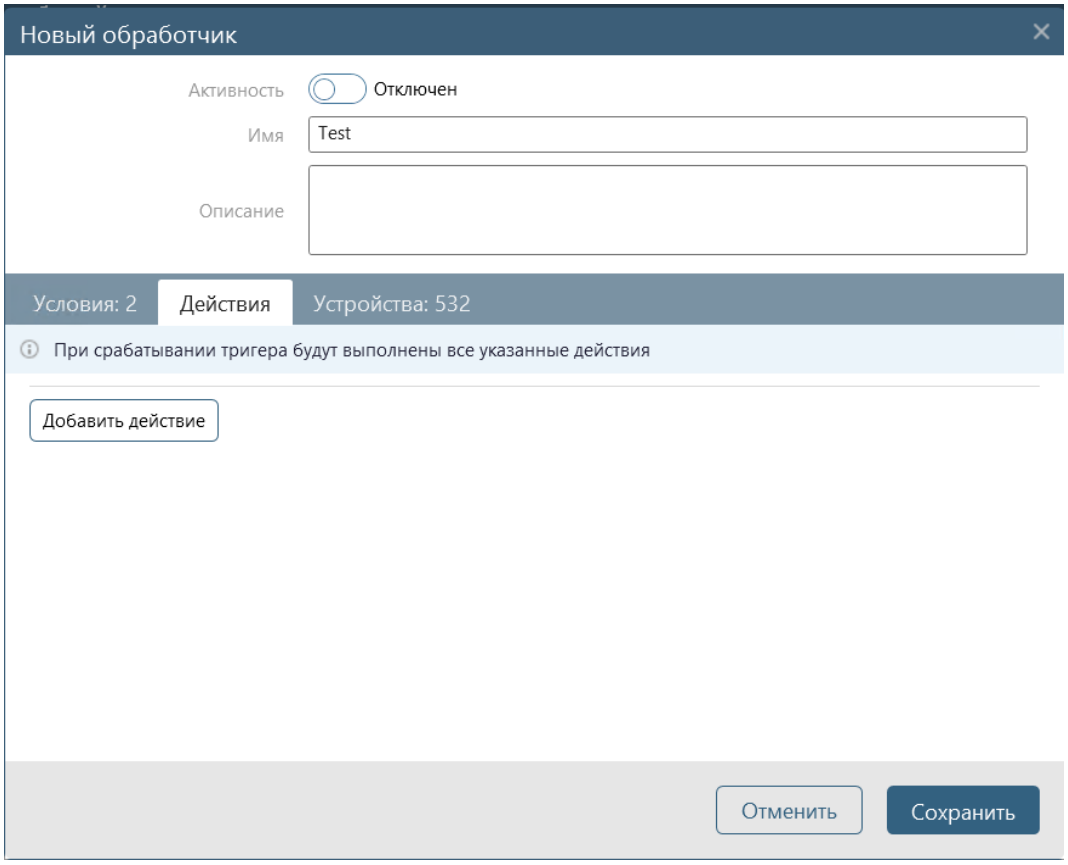


Рисунок 30 – Вкладка ***Действия*** создаваемого триггера

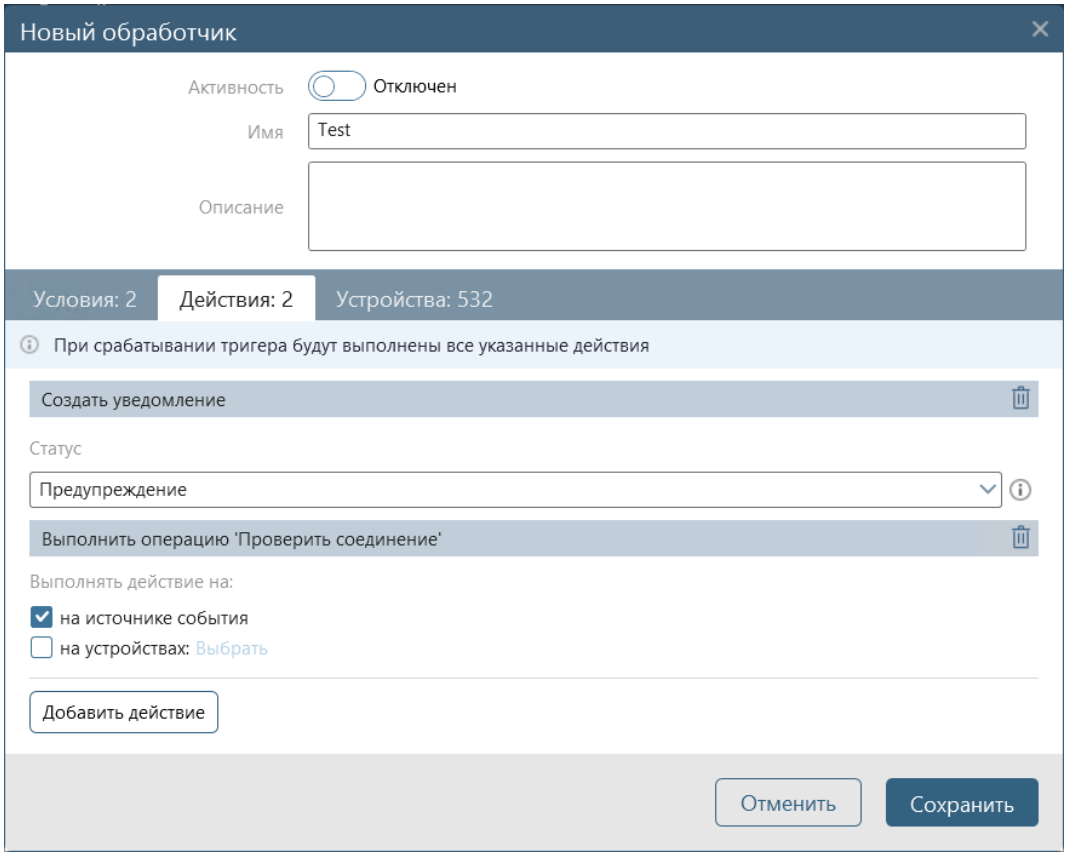


Рисунок 31 – Вкладка ***Действия*** создаваемого триггера с выбранными типам действий

г) во вкладке ***Устройства*** формы добавления триггера (рис. 32) выбрать установкой флагов устройства, для которых будет использоваться триггер (подробнее см. п. 2.4.4 «Настройка использования триггеров»).

6) Нажать кнопку ***Сохранить***. Произойдет возврат во вкладку ***Обработка событий***, в которой появится строка с именем и данными добавленного триггера.

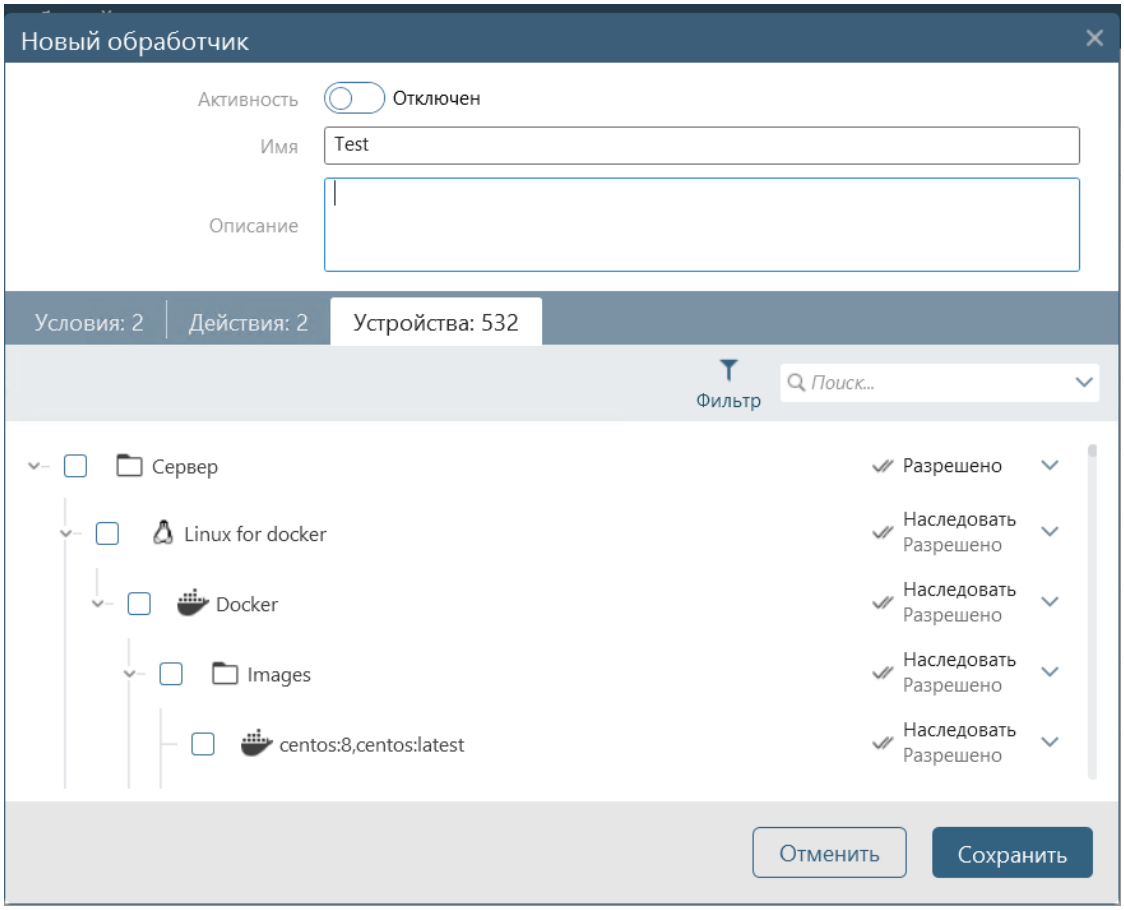


Рисунок 32 – Вкладка ***Устройства*** создаваемого триггера

При создании триггера необходимо обратить особое внимание на возможность зацикливания его выполнения. Например, если определить в качестве условия выполнения триггера событие ***Загрузка отчета***, а в качестве реакции на него комплекса указать действие ***Загрузить отчеты***, то в результате выполнения такого триггера начнется постоянная операция загрузки отчетов с указанных устройств.

2.4.3. Изменение триггера

Изменять можно только созданные пользователем на сервере ПК триггеры. Обработчики событий ***Выполнение конфигурирования и восстановления***, ***Изменения контролируемых отчетов, Ошибки конфигурирования и восстановления, Ошибки при работе с устройством, Ошибки сервера, Первые ошибки при работе с устройством*** являются встроенными и их изменение невозможно. Изменять триггеры могут только пользователи с правами *Управление* в категории *Настройки контроля*.

Для изменения существующего на сервере ПК триггера пользователю необходимо выполнить следующие действия:

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

2) Выбрать сервер, триггер которого должен быть изменен.

3) В области *Настройки контроля* нажать кнопку ***Обработчики событий***.

4) В открывшейся форме ***Обработчики событий*** дважды щелкнуть в строке изменяемого триггера или нажать кнопку ***Изменить*** (). Откроется окно редактирования параметров триггера.

5) Внести в панели общих параметров необходимые изменения в название и описание триггера.

6) Для включения или выключения триггера установить/снять переключатель ***Активность***.

7) Добавить новые или удалить неактуальные типы событий во вкладке ***Условия***. Для удаления события – нажать соответствующую ему кнопку ***Удалить*** ().

ВНИМАНИЕ: Во вкладке ***Условия*** нельзя добавить новые или удалить существующие типы событий для созданных при инсталляции сервера ПК (системных) триггеров!

8) Добавить новые или удалить неактуальные действия во вкладке ***Действия***. Для удаления действия – нажать соответствующую ему кнопку ***Удалить*** ().

9) Во вкладке ***Устройства*** установкой/отменой установки флагов скорректировать перечень устройств, для которых будет использоваться триггер (подробнее см. п. 2.4.4 «Настройка использования триггеров»).

10) Нажать кнопку ***Сохранить***. Произойдет возврат в форму настройки обработки событий, внесенные изменения будут сохранены.

2.4.4. Настройка использования триггеров

Настройка использования триггеров может быть выполнена как в списке триггеров формы ***Обработчики событий*** для всех устройств (групп) сервера ПК, так и в списке устройств раздела ***Устройства*** для каждого устройства (группы) отдельно (см. руководство пользователя по работе с устройствами).

Для настройки использования триггера для всех устройств (групп) сервера ПК пользователю необходимо выполнить следующие действия:

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

2) Выбрать сервер, триггер которого должен быть изменен.

3) В области ***Настройки контроля*** нажать кнопку ***Обработчики событий***.

4) В открывшейся форме ***Обработчики событий*** дважды щелкнуть в строке изменяемого триггера либо нажать кнопку ***Изменить*** (). Откроется окно редактирования параметров триггера.

5) Для настройки использования триггера для одного устройства/группы необходимо:

- перейти на вкладку ***Устройства*** (рис. 33);
- отфильтровать список устройств, нажав кнопку ***Фильтр*** () и выбрав в окне фильтрации (рис. 34) параметры требуемых устройств по их типу и текущему состоянию параметра *Проверка доступности*;
- выполнить поиск устройства/группы с использованием поля **Поиск**;
- выбрать в строке найденного устройства/группы требуемую настройку использования триггера. Перечень возможных значений настройки для групп устройств и устройств приведен в таблице 7.

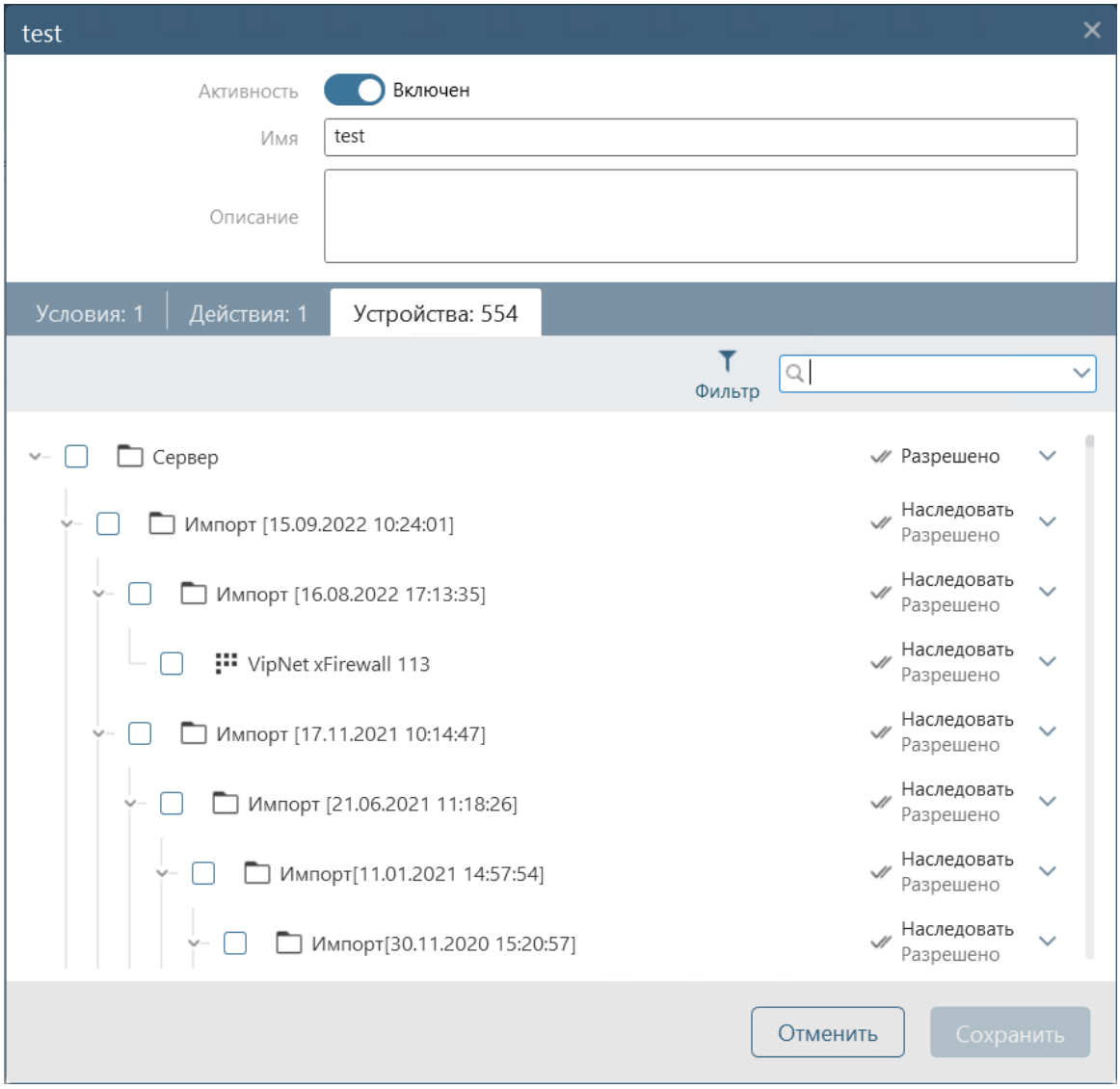


Рисунок 33 – Окно редактирования параметров триггера с активной вкладкой ***Устройства***

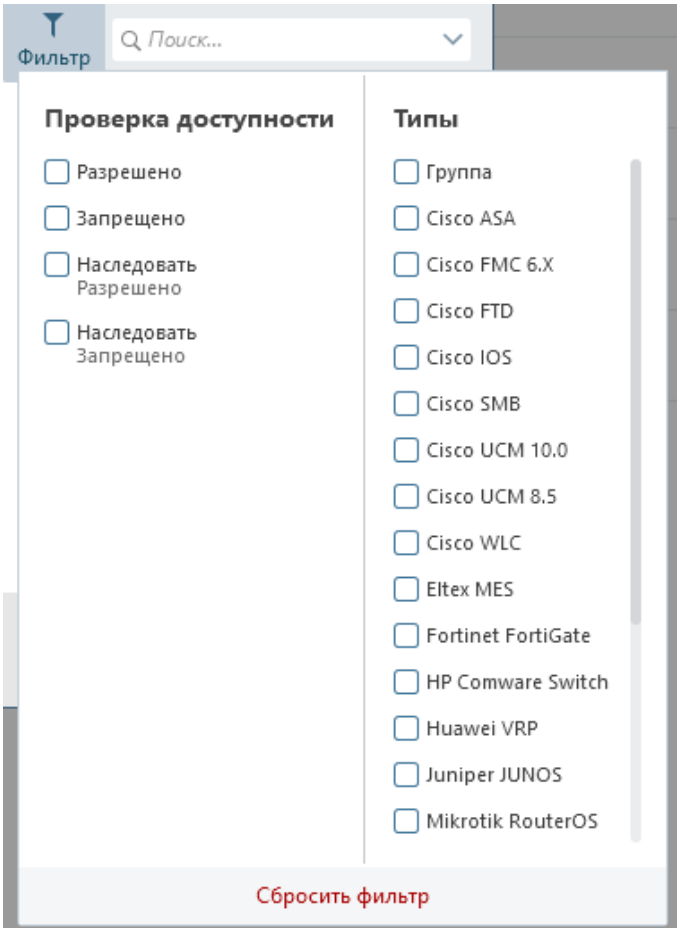


Рисунок 34 – Окно фильтрации списка устройств при настройке использования изменяемого триггера

Таблица 7 – Перечень возможных значений настройки для групп устройств и устройств

Тип объекта	Значение настройки
Корневая группа	Возможные значения: – *Разрешено* – разрешить использование триггера; – *Запрещено* – запретить использование триггера
Другие группы и устройства	Возможные значения: – *Разрешено* – разрешить использование триггера вне зависимости от настроек родительской группы; – *Запрещено* – запретить использование триггера вне зависимости от настроек родительской группы; – *Наследовать (XXXXXX)* – применить настройки родительской группы. В скобках отображается значение, установленное в родительской группе: *Разрешено* или *Запрещено*

6) Для настройки использования триггера для нескольких устройств/групп необходимо:

– отфильтровать список устройств, нажав кнопку ***Фильтр*** (▼) и выбрав в окне фильтрации (см. рис. 34) параметры требуемых устройств по их типу и текущему состоянию *параметра Проверка доступности*;

– выполнить поиск устройств/группы с использованием поля **Поиск**;
– установить флаги в строках требуемых устройств/групп устройств. В заголовке окна отобразится общее количество выбранных групп и устройств (рис. 35) и поле выбора настройки использования триггера. Если текущая настройка для выбранных устройств/групп различная, то в поле отображается значение Разные значения, если одинаковая, то – текущее значение настройки;
– выбрать в поле выбора настройки использования триггера требуемую настройку использования триггера (см. таблицу 6).

7) Нажать кнопку ***Сохранить***. Окно редактирования параметров триггера закроется, внесенные изменения будут применены.

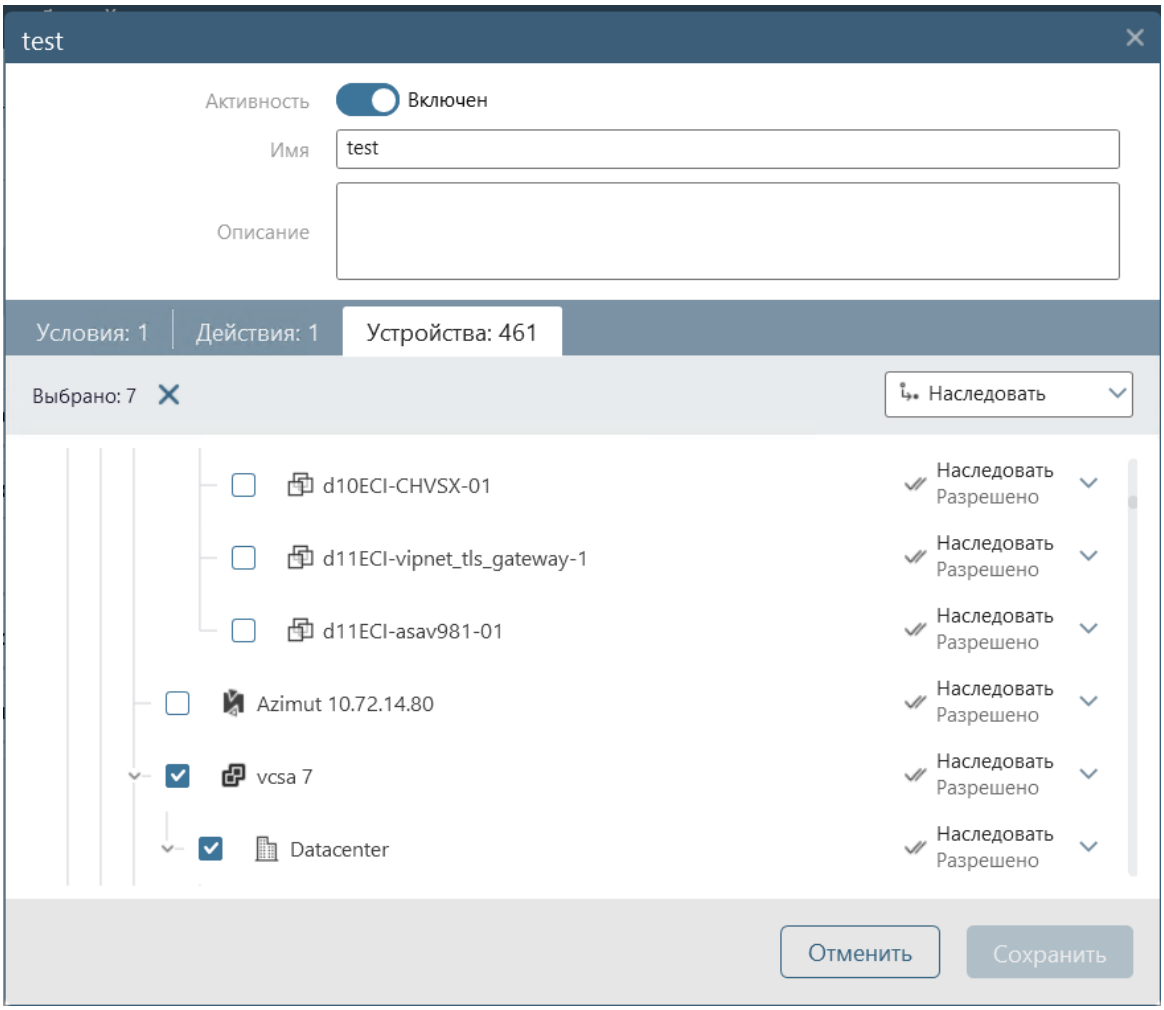


Рисунок 35 – Окно настройки использования изменяемого триггера с выбранными устройствами

2.4.5. Удаление триггера

С сервера ПК можно удалить только триггеры, которые созданы пользователями комплекса. Удалить триггеры, созданные при инсталляции комплекса (системные), нельзя. Удалять триггеры могут только пользователи с правами *Управление* в категории *Настройки контроля*.

Для удаления триггера с сервера ПК пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выбрать сервер, триггер которого должен быть удален.
3) В области *Настройки контроля* нажать кнопку ***Обработчики событий***.
4) В открывшейся форме ***Обработчики событий*** в строке триггера нажать кнопку ***Удалить*** ( ).
5) В открывшемся окне с запросом на подтверждение удаления триггера с сервера ПК нажать кнопку ***Удалить.***

В результате триггер будет удален с сервера ПК.

2.4.6. Аудит изменений

При выборе в меню формы настройки обработчиков событий (триггеров) кнопки ***Аудит изменений*** открывается окно **Загрузка отчетов по событиям** (рис. 36) для более точной настройки привязки произведенных на устройствах изменений к пользователям. Включать/отключать настройки могут только пользователи с правами *Управление* в категории *Настройки контроля*.

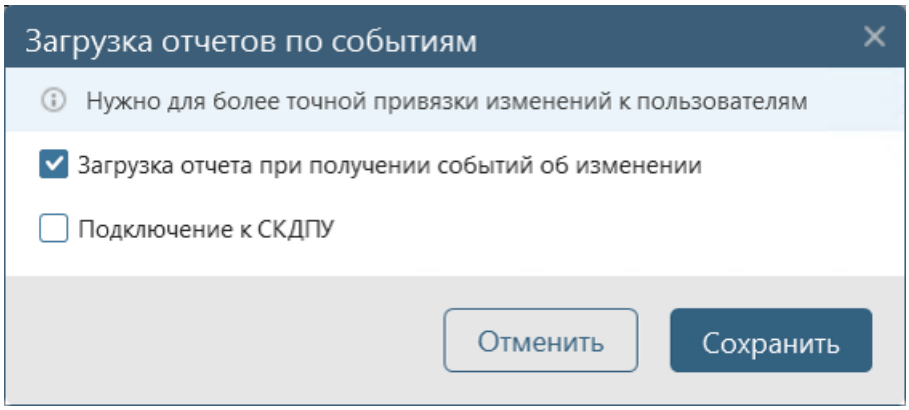


Рисунок 36 – Окно **Загрузка отчетов по событиям**

В окне **Загрузка отчетов по событиям** доступны:

1) Включение/выключение режима загрузки отчетов при получении событий об их изменении. Для включения режима необходимо:
   - установить флаг в поле ***Загрузка отчетов при получении событий об изменении***;
   - нажать кнопку **Сохранить**.
2) Включение/выключение режима подключения к Системе контроля действий поставщиков ИТ-услуг (СКДПУ). Для включения режима необходимо:
   - установить флаг в поле ***Подключение к СКДПУ***;
   - ввести в дополнительно отобразившихся в блоке ***Подключение к СКДПУ*** полях (рис. 37) адрес сервера СКДПУ (IP-адрес или имя хоста), логин и пароль пользователя для подключения;
   - проверить правильность введенных данных, нажав кнопку **Проверить подключение**. При успешном завершении проверки

слева от кнопки отобразится сообщение *Успешно*, иначе – сообщение *Ошибка*;
– скорректировать, при необходимости, данные в полях блока ***Подключение к СКДПУ***;
– нажать кнопку **Сохранить**.

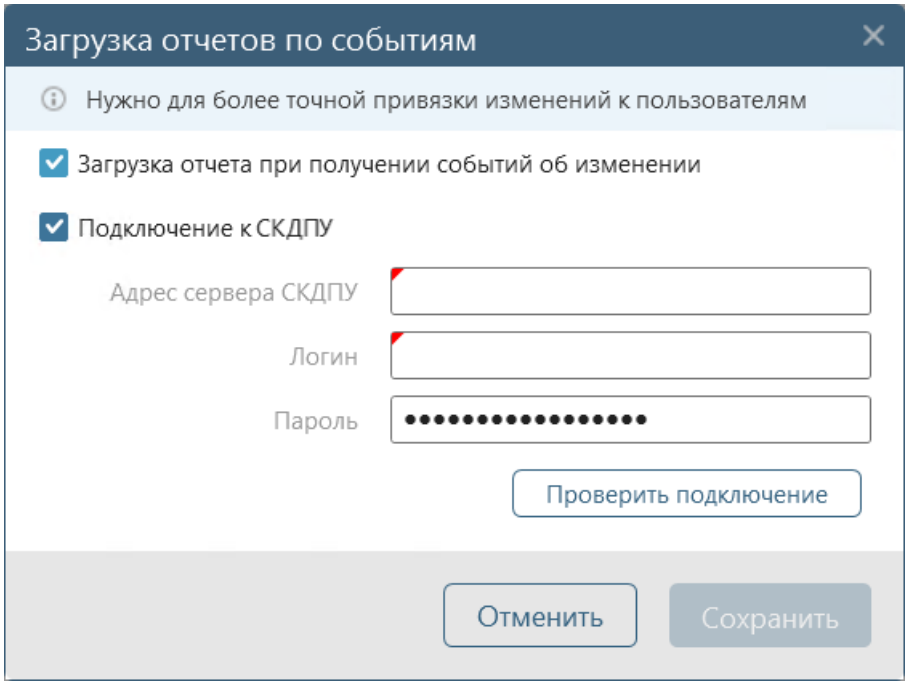


Рисунок 37 – Окно **Загрузка отчетов по событиям** с дополнительными полями

После включения режима подключения к СКДПУ с периодичностью в 10 секунд будет выполняться запрос из ПК «Efros Config Inspector» v.4 в СКДПУ для получения данных по сессиям (кто, когда и с каким устройством работал или ещё работает). В случае изменения какого-либо отчёта устройства и при условии, что изменение было зафиксировано ПК «Efros Config Inspector» v.4 в тот промежуток времени, когда с устройством работал или ещё работает пользователь через СКДПУ, то в отчёте будет указано имя этого пользователя (рис. 38).

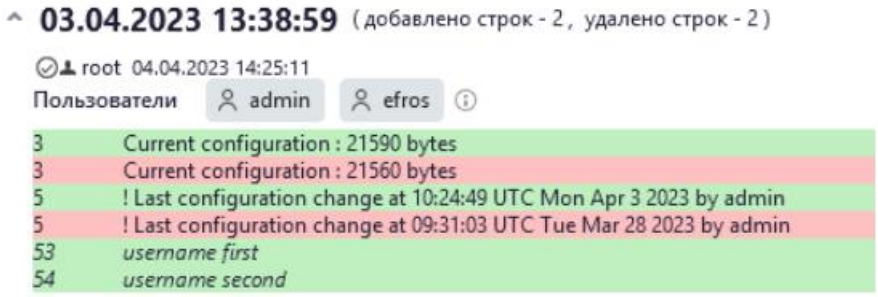


Рисунок 38 – Вкладка ***История изменений*** отчета с указанием имени пользователя

По нажатию кнопки «ⓘ» откроется раздел событий аудита, где можно посмотреть информацию о сессии в СКДПУ, которую привязали к изменению отчёта (рис. 39). По нажатию в строке события аудита ссылки ***Подробнее*** откроется страница веб-браузера с интерфейсом СКДПУ для детального ознакомления с логами сессии (рис. 40).

Рисунок 39 – События аудита

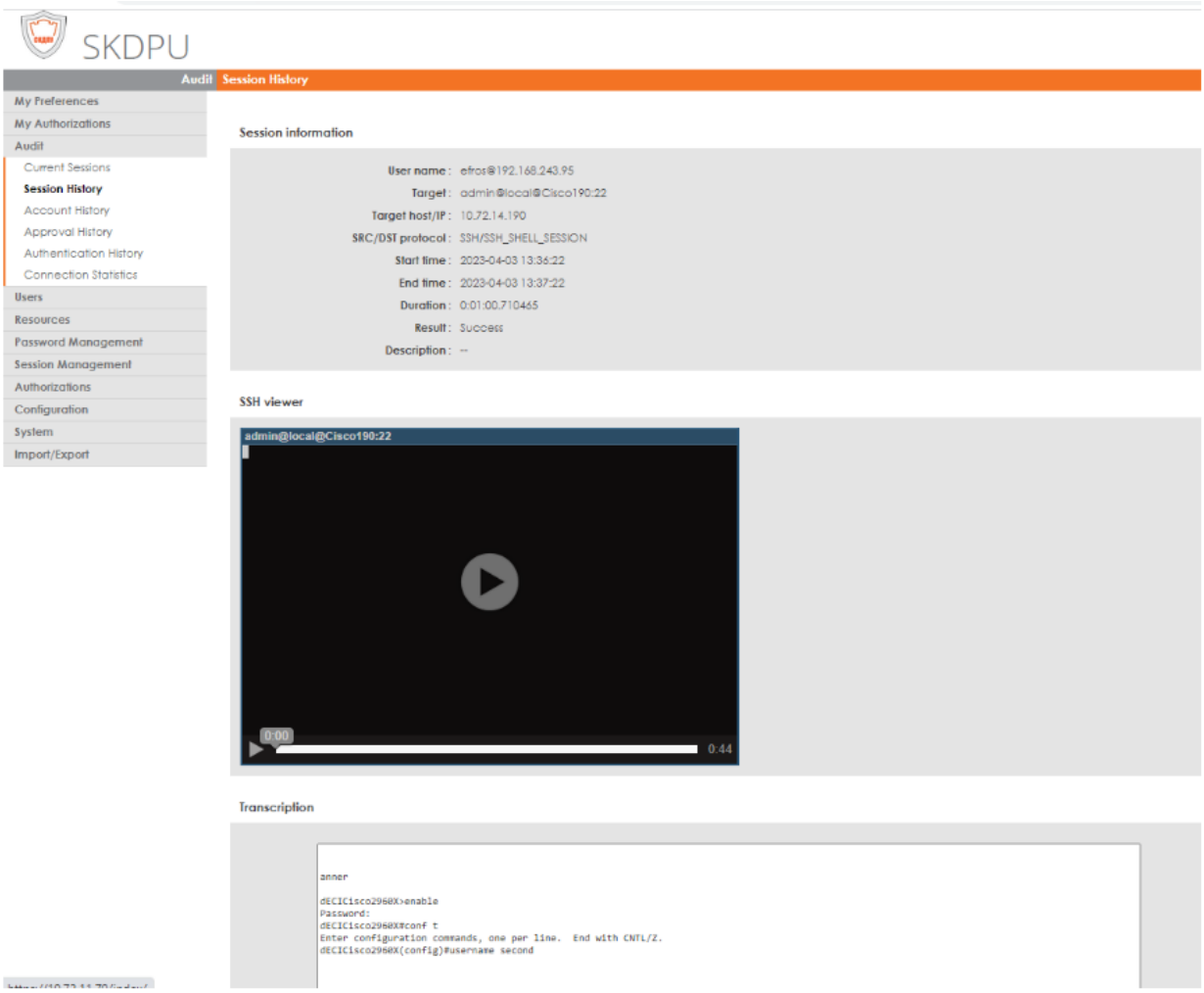


Рисунок 40 – Интерфейс СКДПУ

2.5. Настройки профилей

2.5.1. Просмотр списка профилей

Для просмотра списка профилей необходимо перейти в раздел **Настройки**, для чего в консоли нажать соответствующую кнопку на панели выбора раздела, выбрать сервер, список профилей которого просматривается (нажать кнопку ***Сервер*** и выбрать в открывшемся окне **Выбор сервера** строку требуемого сервера), и в панели ***Настройки контроля*** нажать ссылку *Профили*. Откроется форма управления профилями настройки параметров контроля устройств (рис. 41).

Рабочая область формы управления профилями комплекса разделена на:

- ***панель списка профилей*** (см. п. 2.5.1.1);
- вкладку ***Конфигурации*** (см. п. 2.5.1.2);
- вкладку ***Проверки*** (см. п. 2.5.1.3).

Примечание – До установки внешних модулей ПК «Efros Config Inspector» v.4 панель списка профилей содержит информационное сообщение «*Модули устройств отсутствуют*», вкладки содержат сообщения «*Данные отсутствуют*».

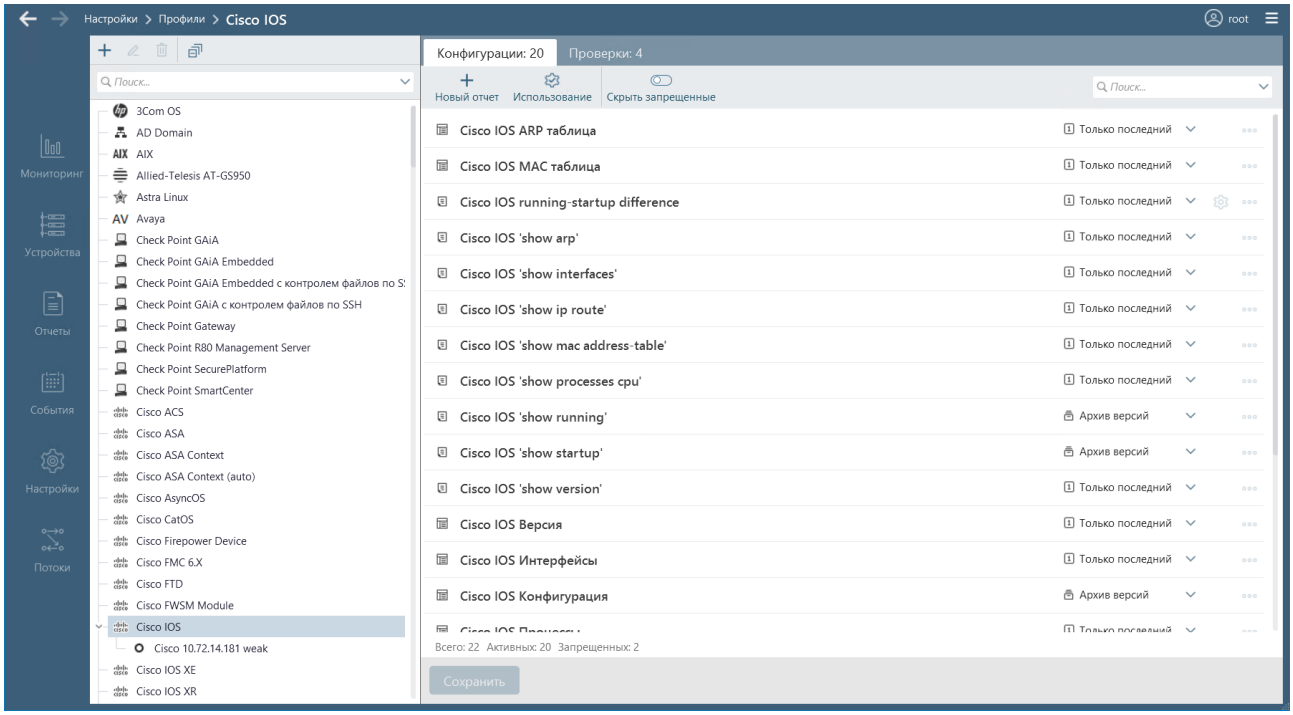


Рисунок 41 – Форма управления профилями устройств

2.5.1.1. Панель списка профилей

Панель списка профилей формы редактирования профилей комплекса содержит:

- кнопки:
  - а) ***Добавить*** (+) – активна только при выборе профилей, добавленных в комплекс в результате подключения внешних модулей (далее – основной профиль). Позволяет перейти к окну создания нового пользовательского профиля (см. п. 2.5.2 «Добавление профиля»);
  - б) ***Свойства*** (✎) – активна только при выборе пользовательского профиля. Служит для изменения параметров профиля. (см. п. 2.5.3 «Изменение профиля»);
  - в) ***Удалить*** (🗑) – активна только при выборе пользовательского профиля. Служит для удаления профиля (см. п. 2.5.4 «Удаление профиля»);
  - г) ***Свернуть все*** (⧉) – активна всегда. Служит для сворачивания дерева профилей до первого уровня – наименований основных профилей;
- поле поиска профилей;
- древовидный список профилей настройки параметров контроля устройств текущей серверной части комплекса. Список профилей формируется в результате подключения к комплексу внешних модулей и создания пользовательских профилей.

Каждый из профилей обладает контекстным меню для быстрого доступа к основным функциям (см. рис. 41). Описание пунктов контекстного меню профиля приведено в таблице 8.

Основные профили (профили, добавленные в комплекс в результате подключения внешних модулей) в форме управления профилями доступны только для внесения изменений в настройки отчетов и проверок типов устройств, контролируемых текущей серверной частью комплекса, во вкладках соответственно ***Конфигурации*** и ***Проверки***.

При удалении профиля, являющегося родительским для других профилей, удаляются выбранный профиль и все дочерние для него профили.

Таблица 8 – Контекстное меню профиля

Пункт меню	Назначение
Добавить	Переход в окно добавления пользовательского профиля
Удалить	Удаление профиля. Пункт активен только при выборе пользовательского профиля
Свойства	Переход в форму редактирования общих данных профиля. Пункт активен только при выборе пользовательского профиля

2.5.1.2. Вкладка Конфигурации

Вкладка ***Конфигурации*** открывается при переходе в форму редактирования профилей (см. пример на рис. 41) и содержит:

- кнопку ***Новый отчет*** (+) – для перехода в окно создания нового отчета (см. п. 2.6.1 «Добавление пользовательских отчетов»);
- кнопку ***Использование*** () – для перехода в окно просмотра и настройки использования профилей для устройств (в окне выведена вся иерархия папок и устройств комплекса с текущими используемыми профилями, с возможность переопределить используемый профиль);
- переключатель ***Скрыть запрещенные*** – для включения/отключения отображения в списке отчетов с режимом использования *Запрещено* (отображаются – / не отображаются –);
- поле поиска отчетов;
- список отчетов, предназначенных для загрузки с контролируемых устройств, которые связаны с профилем, выбранным в панели списка профилей.

Пользователь имеет возможность настроить режим использования отчета для выбранного профиля, выбрав в списке поля с вариантами использования отчетов необходимый режим использования (подробнее см. п. 2.5.3.1 «Настройка отчетов в профиле»).

В заголовке вкладки указано количество активных в текущий момент отчетов (не запрещенных для загрузки с устройства). В нижней части вкладки приведены данные об общем количестве отчетов, количестве активных и запрещенных на текущий момент времени отчетов.

Примечание – Строки отчетов, запрещенных к загрузке с выбранного устройства, отображаются затененными (см. рис. 41). Такие отчеты во вкладке ***Отчеты*** раздела **Устройства** не отображаются, доступны для просмотра и настройки только во вкладке ***Конфигурации*** раздела **Профили**.

По нажатию кнопки ***Меню*** (▫▫▫) в строке отчета открывается контекстное меню отчета с пунктами:

- ***Удалить*** – активен только для созданного пользователем отчета. Служит для удаления отчета из списка отчетов комплекса;

Примечание – При удалении используемого на устройствах пользовательского отчета откроется окно подтверждения со списком всех устройств, для которых он загружается. Пользователь имеет возможность подтвердить или отменить удаление.

- ***Клонировать*** – активен только для созданного пользователем отчета. При выборе пункта меню открывается окно создания отчета с данными выбранного отчета (подробнее см. п. 2.6.4 «Клонирование отчетов»);
- ***Настройки для устройств*** – активен для всех отчетов. При выборе пункта открывается окно просмотра/настройки режима использования отчета для устройств, которые связаны с профилем, выбранным в панели списка профилей.

Контекстное меню также можно открыть щелчком правой кнопки «мыши» в строке отчета. При этом контекстное меню отличается от меню, открывающегося по кнопке ***Меню***, отсутствием пункта ***Удалить.***

Для вступления в силу произведенных изменений режима использования отчетов для выбранного профиля необходимо нажать кнопку ***Сохранить***.

2.5.1.3. Вкладка Проверки

Во вкладке ***Проверки*** формы редактирования профилей отображен список проверок, предназначенных для выполнения на контролируемых устройствах, которые связаны с профилем, выбранным в панели списка профилей (рис. 42).

Заголовок вкладки содержит:

- кнопку ***Использование*** () – для перехода в окно просмотра и настройки использования профилей для устройств (в окне выведена вся иерархия папок и устройств комплекса с текущими используемыми профилями, с возможностью переопределить используемый профиль);
- переключатель ***Скрыть запрещенные*** – для включения/отключения отображения в списке проверок с режимом использования *Запрещено* (отображаются –  / не отображаются – );
- поле поиска проверок.

В заголовке вкладки указано количество разрешенных для выполнения для устройств в текущий момент проверок. В нижней части вкладки приведены данные об общем количестве проверок, количестве разрешенных и запрещенных на текущий момент времени проверок.

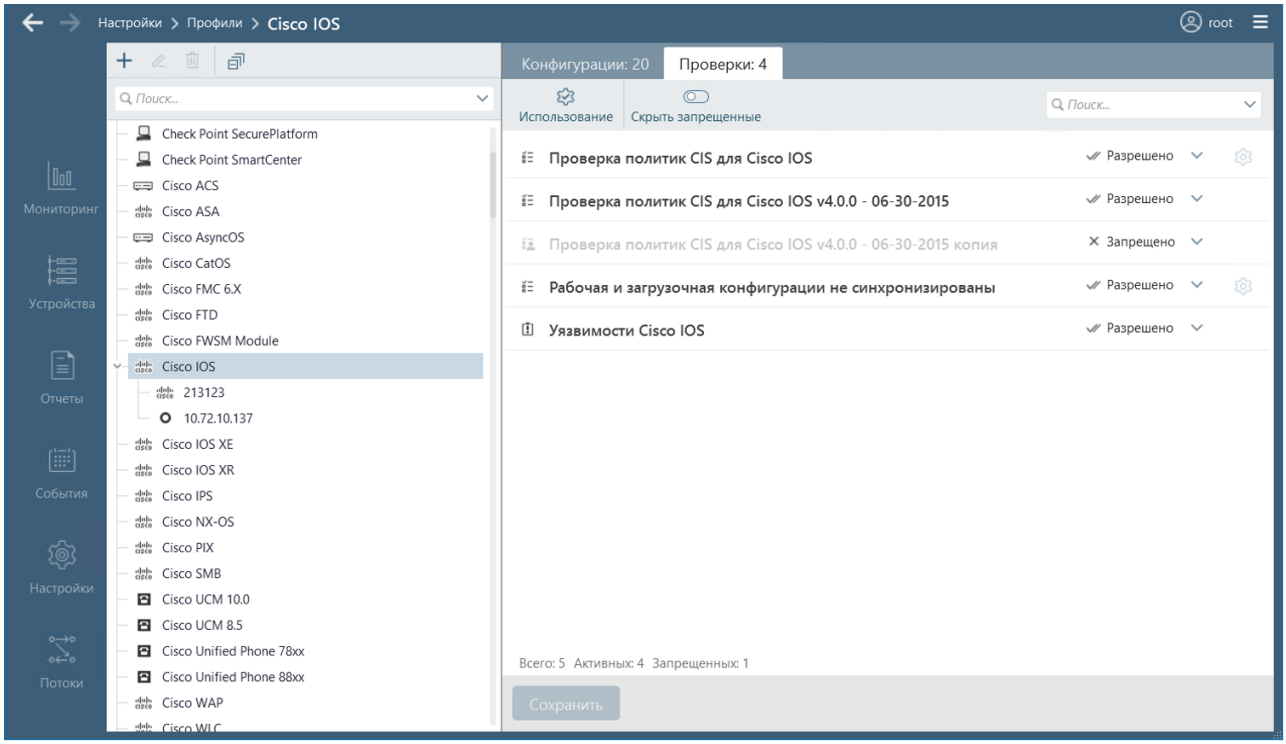


Рисунок 42 – Вкладка ***Проверки*** формы редактирования профилей

Примечание – Строки проверок, для которых загрузка отчетов с выбранного устройства запрещена, отображаются затененными (см. рис. 42). Такие отчеты во вкладке ***Отчеты*** раздела **Устройства** не отображаются, доступны для просмотра и настройки только во вкладке ***Проверки*** раздела **Профили**.

Во вкладке ***Проверки*** формы редактирования профилей можно настроить режим использования проверок для выбранного профиля (см. п. 2.5.3.2 «Настройка проверок в профиле») и просмотреть или изменить правила проверки, нажав в соответствующей строке кнопку ***Настройки правил*** (пиктограмма ⚙).

Для вступления в силу произведенных изменений режима использования проверок для выбранного профиля необходимо нажать кнопку ***Сохранить***.

2.5.2. Добавление профиля

Создавать новые профили настройки параметров контроля устройств на сервере ПК могут только пользователи с правами *Управление* в категории *Настройки контроля.*

Для добавления профиля пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выбрать сервер, для которого добавляется профиль.
3) В области ***Настройки контроля*** нажать кнопку ***Профили***.
4) В открывшейся форме управления профилями устройств (см. рис. 41) выделить основной профиль, который будет базовым по отношению к создаваемому профилю, и нажать в панели кнопок списка профилей кнопку ***Добавить*** (+) или выбрать пункт ***Добавить*** в контекстном меню выбранного базового профиля.

5) В открывшемся окне добавления профиля (рис. 43, состав и описание полей окна приведены в таблице 9):

- в поле ***Имя*** ввести имя создаваемого профиля;
- при необходимости, изменить базовый профиль, выбрав его в раскрывающемся списке поля ***Тип устройства***;
- при необходимости, в поле ***Описание*** ввести описание создаваемого профиля;
- нажать кнопку ***Сохранить***.

6) Произойдет возврат в форму настройки профилей, в которой появится строка с именем добавленного профиля. При этом для нового профиля будут отображены настройки использования отчетов и проверок устройств выбранного ранее базового профиля.

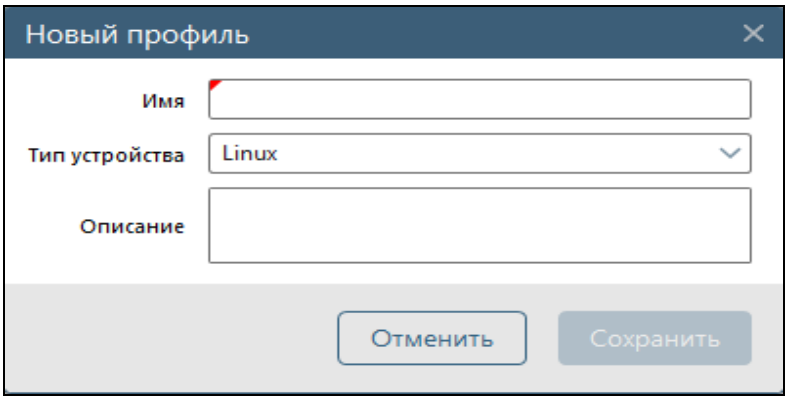


Рисунок 43 – Окно создания профиля

Таблица 9 – Состав и описание полей окна создания профиля

Поле	Описание/Назначение
Имя	Наименование создаваемого профиля
Тип устройства	Выбор базового профиля для создаваемого профиля. Список содержит наименования всех основных профилей, добавленных на сервер ПК при подключении внешних модулей. Новый профиль по умолчанию наследует все настройки, заданные в базовом профиле. Эти настройки доступны для внесения изменений
Описание	Текстовое поле, в которое можно ввести понятное описание создаваемого профиля

По умолчанию настройки использования входящих в созданный профиль отчетов и проверок устройств будут унаследованы от базового основного профиля. Все они доступны для изменения.

2.5.3. Изменение профиля

Изменять профили настройки параметров контроля устройств на сервере ПК могут только пользователи с правами *Управление* в категории *Настройки контроля*.

Для внесения изменений в настройки профиля пользователю необходимо выполнить следующие действия:

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

2) Выбрать, при необходимости, сервер, для которого изменяется профиль.

3) В области *Настройки контроля* нажать кнопку ***Профили***.

4) В открывшейся форме управления профилями устройств (см. рис. 41) выделить профиль, который будет редактироваться, и нажать в панели кнопок списка профилей кнопку ***Свойства*** () или выбрать пункт ***Свойства*** в контекстном меню выбранного профиля.

5) В открывшемся окне свойств профиля (аналогично окну добавления профиля (см. рис. 43)) изменить необходимые параметры (состав и описание полей окна приведены в таблице 9) и нажать кнопку ***Сохранить***.

6) Произойдет возврат в форму настройки профилей, в которой отобразятся внесенные в профиль изменения.

7) При необходимости, внести изменения в настройки использования отчетов и проверок для выбранного профиля в соответствии с пунктами 2.5.3.1 «Настройка отчетов в профиле» и 2.5.3.2 «Настройка проверок в профиле».

8) Для сохранения внесенных изменений в параметры профиля – нажать кнопку ***Сохранить*** во вкладке ***Конфигурации***.

2.5.3.1. Настройка отчетов в профиле

Изменять настройки отчетов в профилях на сервере ПК могут только пользователи с правами *Управление* в категории *Настройки контроля.*

Настройка отчетов в имеющихся профилях комплекса заключается в:

- разрешении/запрете загрузки отчетов с контролируемых устройств, которые используют настройки редактируемого профиля;
- задании необходимости 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 пользовательских отчетов могут быть изменены состав и условия отбора отображаемых данных).

Для внесения изменений в настройки отчетов в профилях пользователю необходимо выполнить следующие действия:

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

2) Выбрать, при необходимости, сервер, для которого изменяется профиль.

3) В области *Настройки контроля* нажать кнопку ***Профили***.

4) В открывшейся форме управления профилями устройств (см. рис. 41) выделить профиль, настройки отчетов которого будут изменяться.

5) Во вкладке ***Конфигурации*** выделенного профиля, выделить изменяемый отчет и раскрыть список поля с вариантами использования отчета (рис. 44, таблица 10).

6) Выбрать необходимый вариант использования отчета, загружаемого с устройств (варианты использования отчетов и их описание приведены в таблице 10).

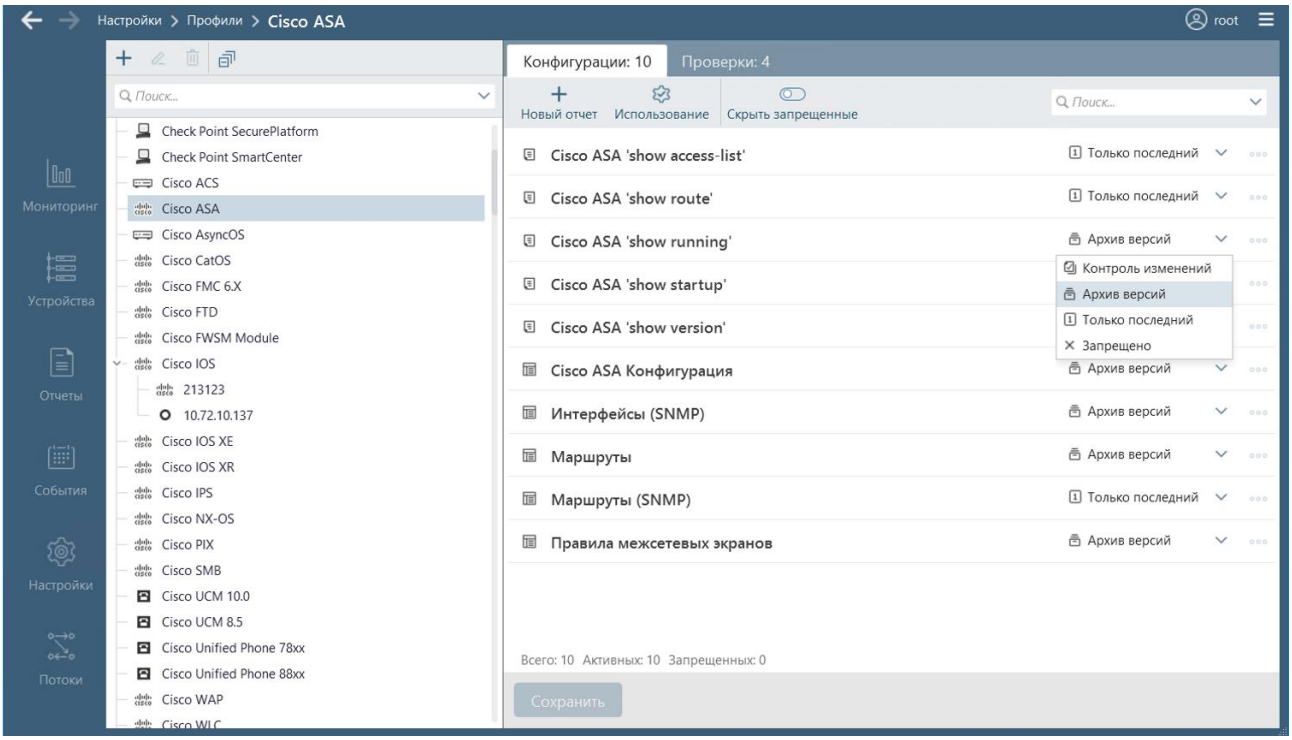
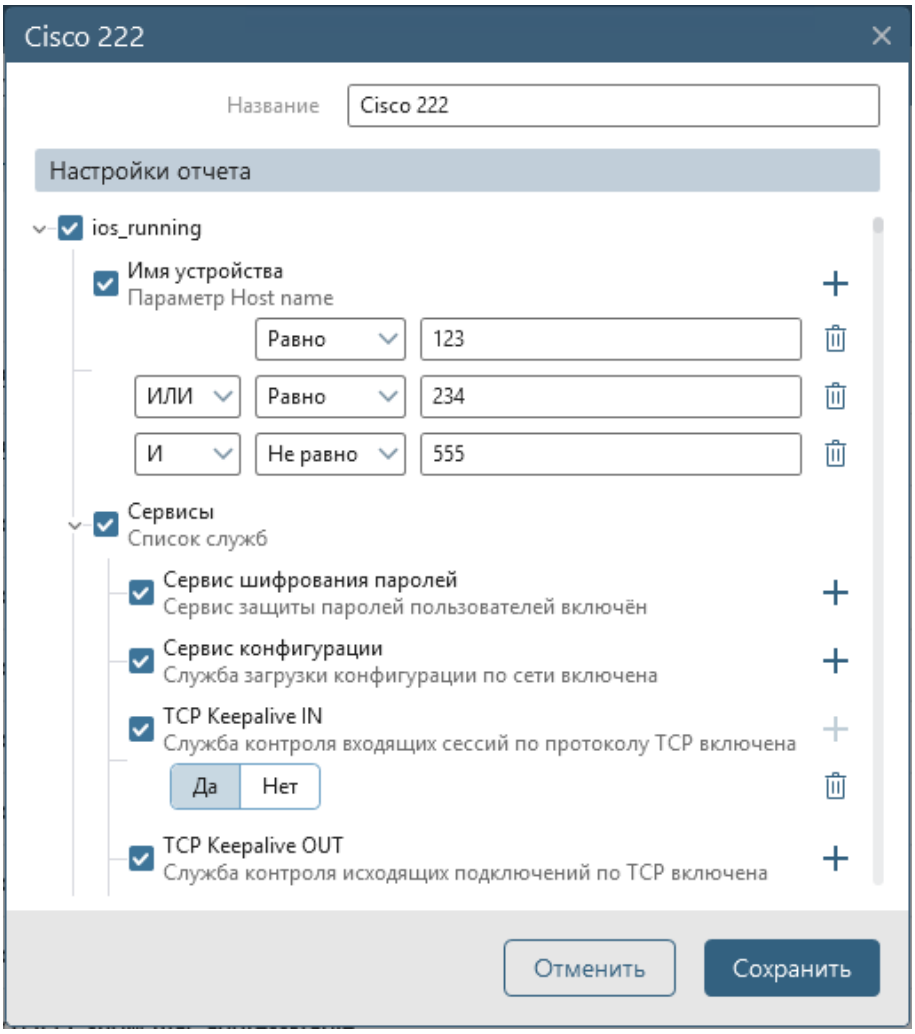


Рисунок 44 – Настройка отчетов выбранного профиля

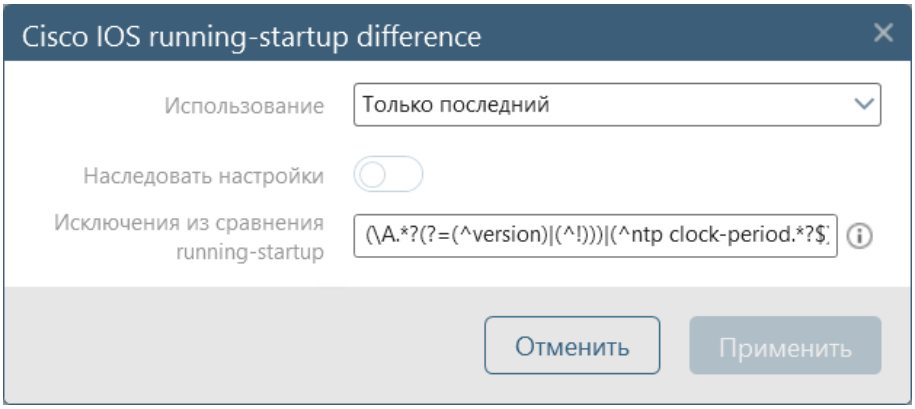
Таблица 10 – Состав и описание колонок вкладки ***Конфигурации*** формы настройки профиля

Поле	Описание/Назначение
Имя отчета	Наименование отчета
Варианты использования отчета	Выбор режима использования отчета. Возможные значения: – *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

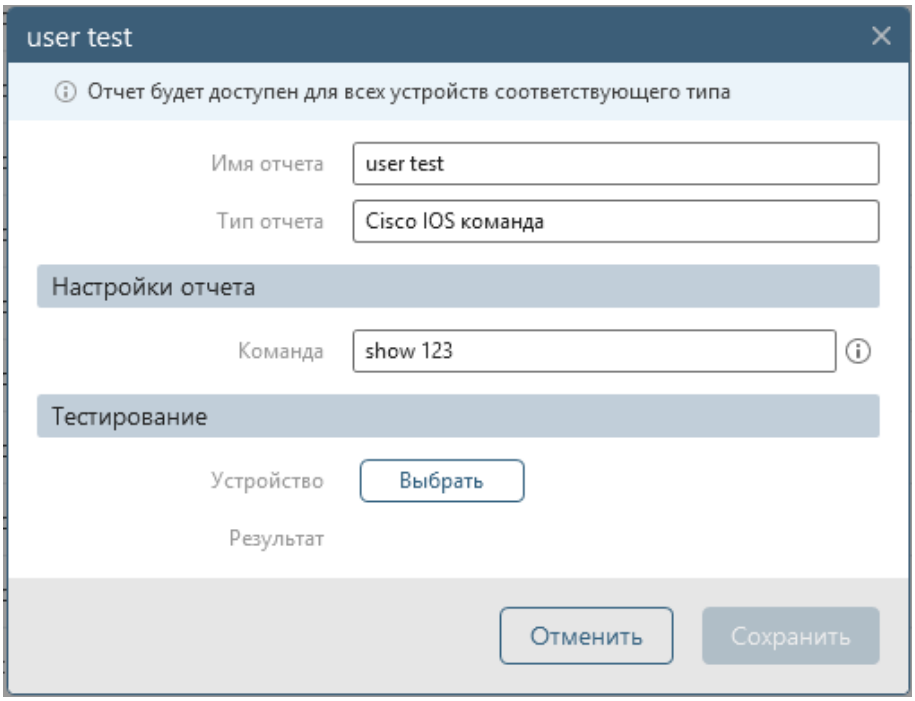
Поле	Описание/Назначение
Без названия	Содержит кнопку ***Меню*** (▫▫▫), по нажатию которой открывается контекстное меню отчета с пунктами: – ***Удалить*** – активен только для созданного пользователем отчета. Служит для удаления отчета из списка отчетов комплекса; – ***Клонировать*** – активен только для созданного пользователем отчета. При выборе пункта меню открывается окно создания отчета с данными выбранного отчета; – ***Настройки для устройств*** – активен для всех отчетов. При выборе пункта открывается окно просмотра/настройки режима использования отчета для устройств, которые связаны с профилем, выбранным в панели списка профилей. В строках отчетов, имеющих дополнительные настройки, содержит кнопку ***Изменить*** (⚙). По нажатию кнопки открывается окно настроек соответствующего отчета (см. рис. 45)



а) для отчета типа *Фильтр*



б) для общего отчета



в) для пользовательского отчета

Рисунок 45 – Окно дополнительных настроек отчета

7) Для изменения дополнительных настроек отчета (доступно для отдельных видов отчетов):

– нажать в строке изменяемого отчета кнопку ***Изменить*** ( );
– в открывшемся окне (пример приведен на рис. 45, а – для отчета типа *Фильтр*, б – для текстового общего отчета, в – для текстового пользовательского отчета):
  а) внести требуемые изменения в доступные параметры: наименование отчета, вариант использования отчета, дополнительные настройки отчета (см. таблицу 11), для возможности внесения изменений в дополнительные настройки отчета, снять предварительно переключатель в поле **Наследовать настройки**;

Таблица 11 – Состав и описание полей окна дополнительных настроек отчета для устройства

Поле	Описание/Назначение
Название/Имя отчета	Название отчета. Поле доступно для пользовательских отчетов и отчетов типа *Фильтр*
Использование	Выбор настройки использования отчета. Поле доступно для общих отчетов. Возможные значения перечислены в таблице 10
Наследовать настройки	Переключатель режима применения для дополнительных настроек отчета настройки базового профиля. Переключатель доступен для общих отчетов
Настройки отчета	Группа полей для настройки дополнительных параметров (например, масок контролируемых файлов, масок исключения файлов, состава фильтров). Группа полей доступна для всех видов отчетов. Группы в общих отчетах доступны для редактирования только после выключения переключателя в поле ***Наследовать настройки***. Примечание – Описание регулярных выражений стандарта PCRE, допустимых к применению в ПК «Efros Config Inspector» v.4 при внесении изменений в дополнительные настройки текстовых общих и пользовательских отчетов (см. рис. 45, б), приведено в Приложении 1. Подробнее правила изменения настроек для структурированных отчетов приведены в пункте 2.6.2.1 «Настройка условий фильтрации для структурированных отчетов» и для текстовых отчетов – в пункте 2.6.2.2 «Настройка условий фильтрации для текстовых отчетов»
Тестирование	Для выполнения тестового запуска отчета на выбранном устройстве (см. рис. 45, в). Группа полей доступна для пользовательских текстовых отчетов и отображается только при наличии в окне группы *Настройки отчета*

б) выполнить, при необходимости, тестовый запуск отчета, для чего нажать в блоке *Тестирование* кнопку ***Выбрать*** и выбрать в открывшемся окне **Выбор устройств** (рис. 46) устройство;

в) нажать кнопку ***Применить*** (в окне настройки общего отчета) или ***Сохранить*** (для остальных видов отчетов);

г) подтвердить для пользовательских отчетов и отчетов типа *Фильтр* внесение изменений в дополнительные настройки с удалением ранее загруженных с устройства отчетов, нажав кнопку ***Да*** в окне подтверждения (рис. 47).

8) Нажать на вкладке ***Конфигурации*** кнопку ***Сохранить*** для сохранения внесенных в профиль изменений.

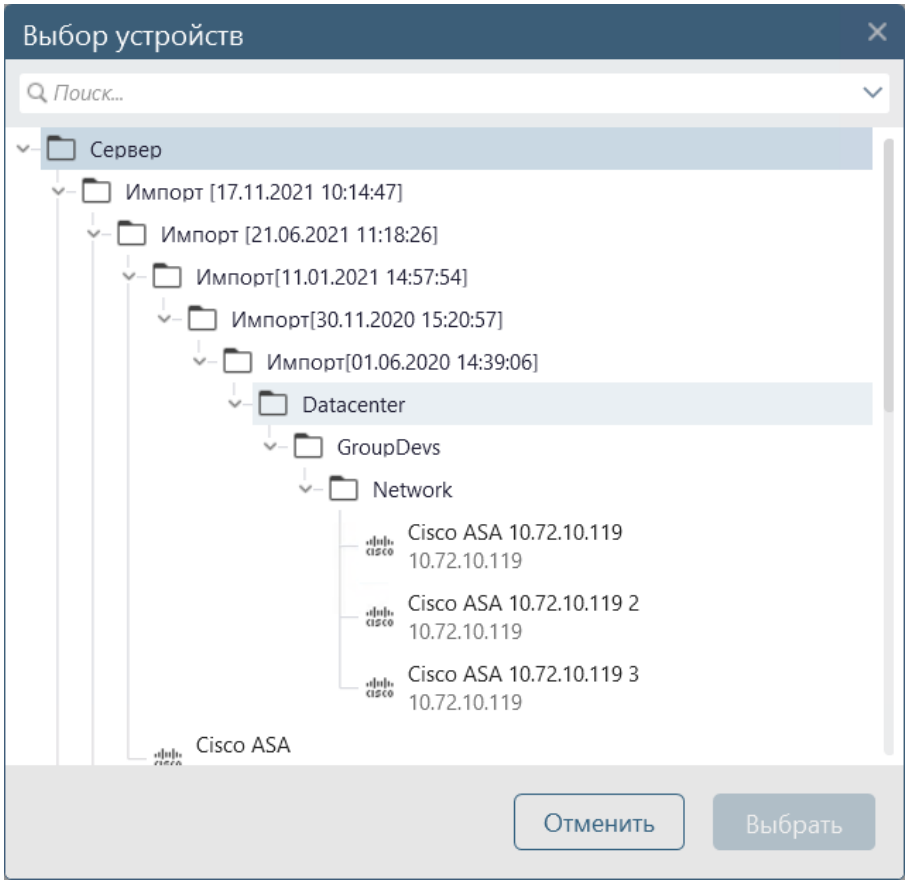


Рисунок 46 – Окно **Выбор устройств**

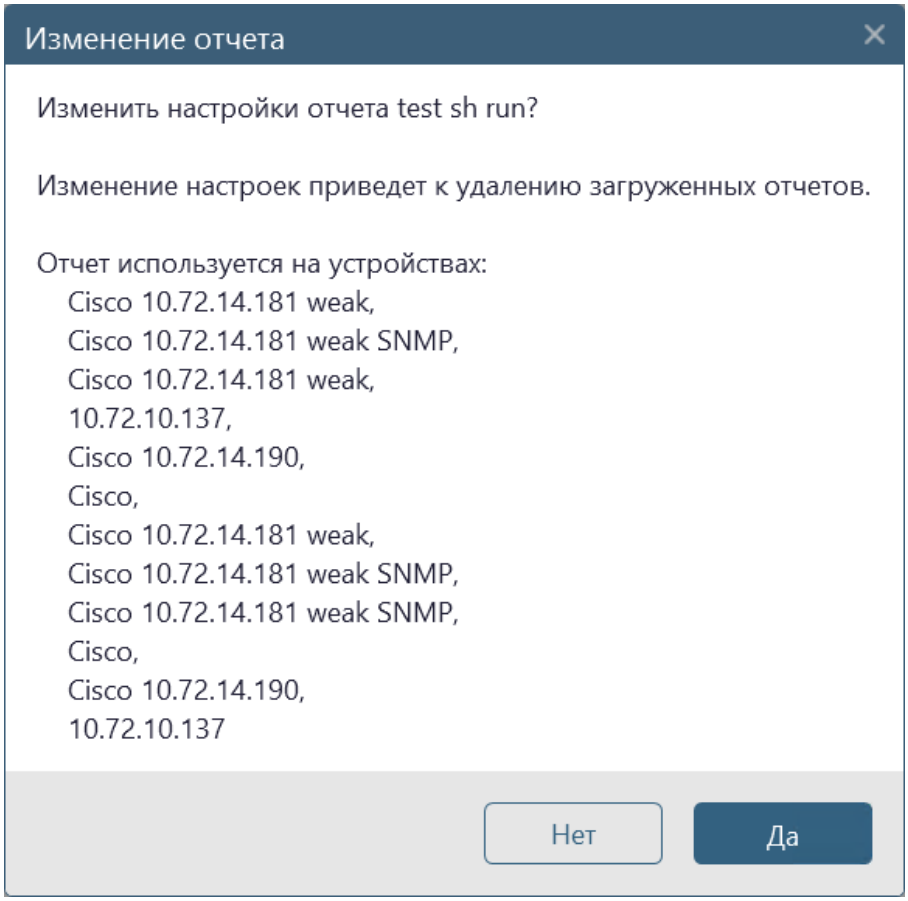


Рисунок 47 – Окно подтверждения внесения изменений

ВНИМАНИЕ: Изменения в настройках пользовательских отчетов и отчетов типа *Фильтр*, внесенные в окне дополнительных настроек, применяются сразу после нажатия кнопки ***Сохранить*** в окне дополнительных настроек, а изменения в настройках общих отчетов и в вариантах использования всех типов отчетов – после нажатия кнопки ***Сохранить*** во вкладке ***Конфигурации***!

На вкладке ***Конфигурации*** реализована возможность настройки отчетов для группы устройств. Для этого необходимо в контекстном меню выбранного отчета выбрать пункт ***Настройки для устройств*** или нажать в строке изменяемого отчета кнопку **Меню** (…) и выбрать в раскрывшемся меню пункт ***Настройки для устройств***.

В открывшемся окне **Настройки отчета** (рис. 48):

- в поле ***Использование*** выбрать требуемое значение варианта использования отчета для каждого из перечисленных устройств (см. таблицу 10);
- внести, при необходимости, изменения в дополнительные настройки отчета (доступно для отдельных видов отчетов), для чего:
  а) нажать в строке устройства, для которого в отчет вносятся изменения, кнопку ***Изменить*** (⚙);
  б) в открывшемся окне (пример см. на рис. 45), внести требуемые изменения в вариант использования отчета и дополнительные настройки отчета (описание полей приведено в таблице 11) для устройства;
  в) нажать кнопку ***Применить***.
- нажать в окне **Настройки отчета** кнопку ***Сохранить***.
- для сохранения внесенных изменений – нажать на вкладке ***Конфигурации*** кнопку ***Сохранить***.

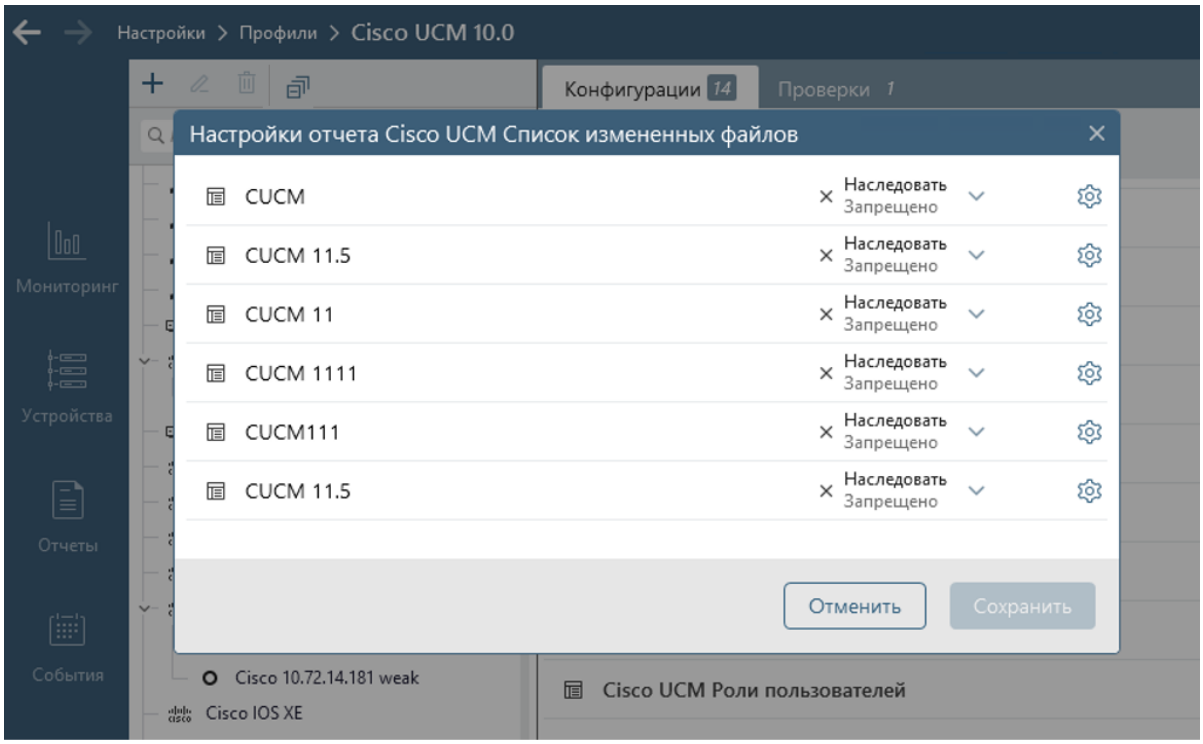


Рисунок 48 – Окно настройки использования отчета для устройств

Примечание – Если профиль не назначен ни для одного устройства, то в окне настройки использования отчета для устройств будет отображаться сообщение *Устройства отсутствуют*.

2.5.3.2. Настройка проверок в профиле

Изменять настройки проверок в профилях на сервере ПК могут только пользователи с правами *Управление* в категории *Настройки контроля.*

Для внесения изменений в настройки проверок в профилях пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выбрать сервер, для которого настраивается профиль.
3) В области *Настройки контроля* нажать кнопку ***Профили***.
4) В открывшейся форме управления профилями устройств (см. рис. 41) выделить профиль, настройки проверок которого будут изменяться.
5) Перейти на вкладку ***Проверки*** выделенного профиля, выделить изменяемую проверку и раскрыть список поля режимов использования проверки (рис. 49).

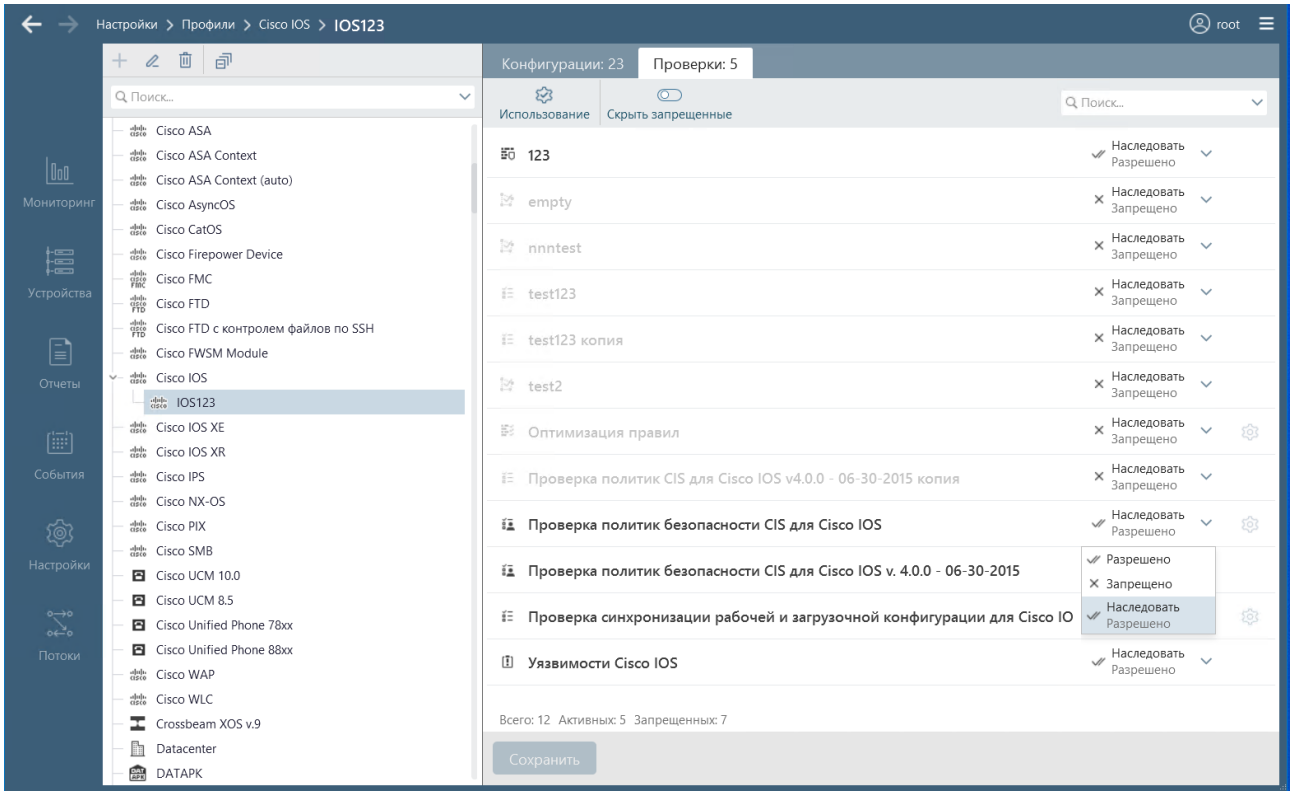


Рисунок 49 – Форма просмотра списка доступных проверок в профиле

6) Выбрать необходимый вариант использования проверки устройства:

– *Разрешено* – разрешить проверку вне зависимости от настроек родительского профиля;
– *Запрещено* – запретить проверку вне зависимости от настроек родительского профиля.

– *Наследовать (XXXXXX)* – применять настройки родительского профиля. В скобках отображается значение, установленное в родительском профиле: *Разрешено* или *Запрещено.*

Примечание – Вариант использования проверки *Наследовать (XXXXXX)* доступен только для пользовательских профилей.

7) Для изменения настроек правил выбранной проверки нажать кнопку ***Настройки правил*** (⚙) в строке настраиваемой проверки.

8) В открывшемся окне настройки правил выбранной проверки (рис. 50, состав и описание значений полей окна приведено в таблице 12):

– изменить, при необходимости, вариант использования проверки устройства;
– выключить переключатель ***Наследовать настройки***;
– изменить, при необходимости, режим выполнения для выбранных правил проверки, выбрав в поле ***Выполнение*** таблицы правил требуемое значение;
– изменить, при необходимости, настройки исключений для отдельных правил проверки;
– нажать кнопку ***Применить*** для сохранения внесенных изменений.

9) Нажать кнопку ***Сохранить*** для сохранения внесенных в профиль изменений.

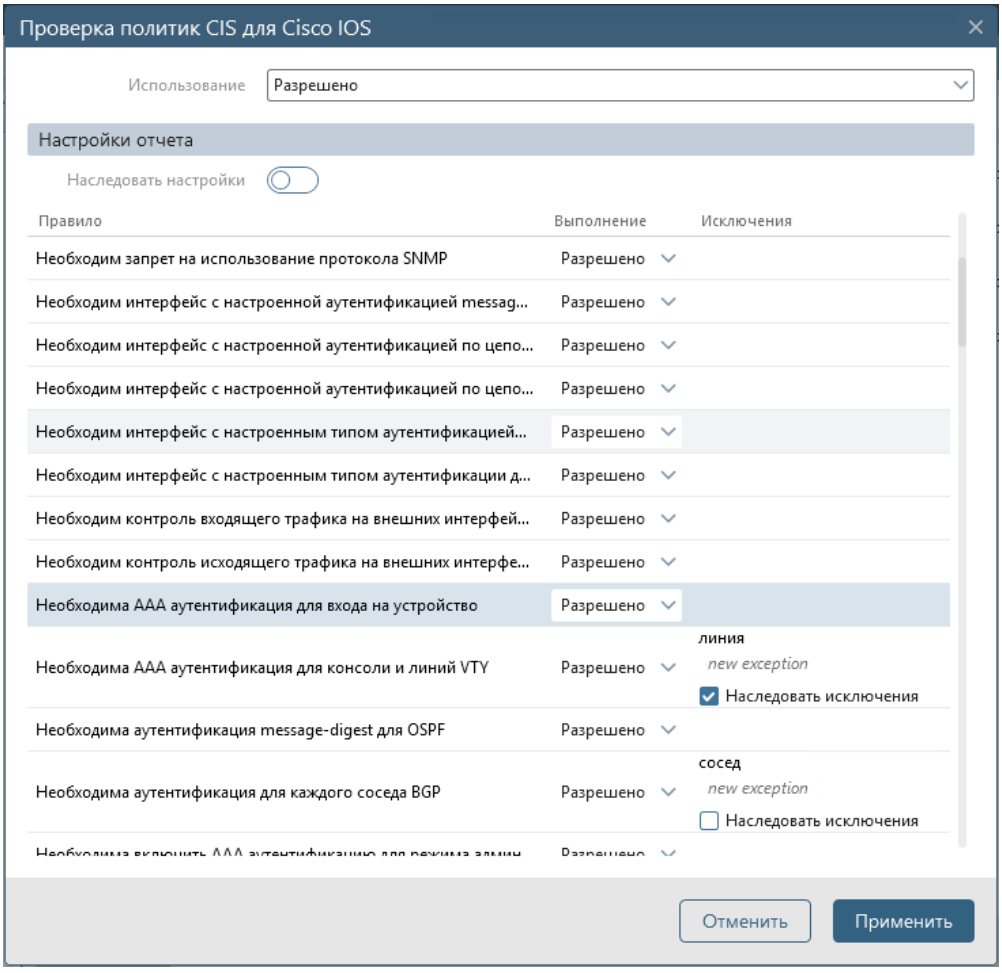


Рисунок 50 – Окно настройки правил проверки устройства

Таблица 12 – Состав и описание полей окна настройки правил выбранной проверки

Поле	Описание/Назначение
Использование	Выбор режима использования проверки. Возможные значения – *Разрешено* – разрешить использование; – *Запрещено* – запретить использование; – *Наследовать (XXXX)* – применить настройки родительского профиля. В скобках отображается значение, установленное для проверки в родительском профиле. Вариант доступен только для пользовательских профилей
Наследовать настройки	Переключатель. Активен только для пользовательских профилей. При включенном переключателе настройки правил профиля в окне не доступны для внесения изменений
Правило	Перечень правил проверки
Выполнение	При установленном переключателе ***Наследовать настройки*** содержит значения, установленные в родительском профиле, и не доступно для редактирования. При снятом переключателе – содержит список доступных для настройки значений режима выполнения отдельных правил в составе проверки: – *Разрешено* – разрешить выполнение правила; – *Запрещено* – запретить выполнение правила; – *Наследовать (XXXX)* – применить настройки родительского профиля. В скобках отображается значение, установленное для правила в родительском профиле. Вариант доступен только для пользовательских профилей
Исключения	Поле заполняется только для правил, в которых могут быть назначены исключения. При установленном переключателе ***Наследовать настройки*** содержит значения, установленные в родительском профиле, и не доступно для редактирования. При снятом переключателе – содержит список доступных для настройки исключений при выполнении правила. Для ввода нового исключения необходимо ввести новое значение в строке *новое значение* и нажать клавишу клавиатуры **ENTER**

Для настройки параметров отчета ***Оптимизация правил*** необходимо нажать кнопку ***Настройки правил*** (⚙) в строке отчета:

1) В открывшемся окне настройки параметров отчета (рис. 51, состав и описание значений полей окна приведено в таблице 13):

– изменить, при необходимости, вариант использования отчета;
– выключить переключатель ***Наследовать настройки***;
– изменить, при необходимости, период времени, в течение которого количество зафиксированных Hit Count правила не изменялось, после чего правило будет считаться неиспользуемым;
– включить/выключить переключатель «Нулевые Hit Count»;
– нажать кнопку ***Применить*** для сохранения внесенных изменений.

2) Нажать кнопку ***Сохранить*** для сохранения внесенных в профиль изменений.

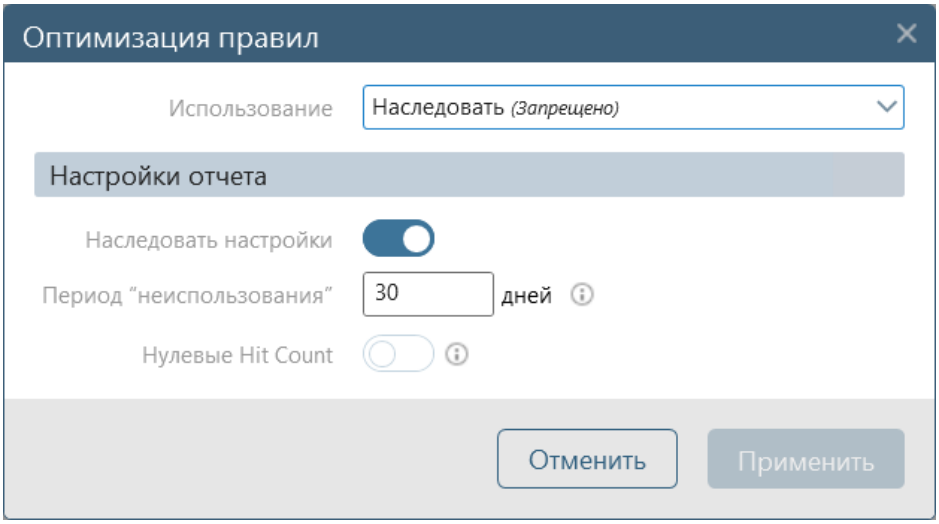


Рисунок 51 – Окно настройки параметров отчета ***Оптимизация правил***

Таблица 13 – Состав и описание полей окна настройки параметров отчета ***Оптимизация правил***

Поле	Описание/Назначение
Использование	Выбор режима использования отчета. Возможные значения – *Разрешено* – разрешить использование; – *Запрещено* – запретить использование; – *Наследовать (XXXX)* – применить настройки родительского профиля. В скобках отображается значение, установленное для правила в родительском профиле. Вариант доступен только для пользовательских профилей
Наследовать настройки	Переключатель. Активен только для пользовательских профилей. При включенном переключателе настройки отчета в окне не доступны для внесения изменений
Период «неиспользования»	Поле для выбора периода времени (в днях), в течение которого количество зафиксированных Hit Count правила не изменялось, после чего правило будет считаться неиспользуемым. Возможные значения: от 30 до 365 дней. Значение по умолчанию – 30. Настройка применяется только для устройств, в отчете ***Правила межсетевого экрана*** которых есть параметр «Hit Count»
Нулевые Hit Count	Переключатель. При включенном переключателе в отчете будут учитываться правила, Hit Count которых равен «0». Настройка применяется только для устройств, в отчете «Правила межсетевого экрана» которых есть параметр «Hit Count»

2.5.4. Удаление профиля

Удалять профили настройки параметров контроля устройств с сервера ПК могут только пользователи с правами *Управление* в категории *Настройки контроля*.

ВНИМАНИЕ: Для удаления с сервера ПК доступны только профили, созданные пользователями комплекса!

Для удаления профиля пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выбрать сервер, для которого удаляется профиль.
3) В области *Настройки контроля* нажать кнопку ***Профили***.
4) В открывшейся форме управления профилями устройств (см. рис. 41) выделить удаляемый профиль и нажать в строке меню списка профилей кнопку ***Удалить*** () или выбрать пункт ***Удалить*** в контекстном меню удаляемого профиля.
5) Подтвердить операцию удаления профиля с сервера ПК, нажав кнопку ***Удалить*** в открывшемся окне.
6) Произойдет возврат в форму настройки профилей.

ВНИМАНИЕ: При удалении пользовательского профиля, являющегося базовым для других профилей, вместе с ним будут удалены и все дочерние для него профили!

2.5.5. Настройка режима использования профилей для устройств

Изменять настройки режима использования профилей для устройства могут только пользователи с правами *Управление* в категории *Настройки контроля.*
Для настройки пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выбрать сервер, для которого настраивается профиль.
3) В области *Настройки контроля* нажать кнопку ***Профили***.
4) В открывшейся форме управления профилями устройств (см. рис. 41) выделить профиль в списке.
5) В открывшейся вкладке ***Конфигурации*** (или во вкладке ***Проверки***) нажать в заголовке кнопку ***Использование*** ().
6) В открывшемся окне настройки использования профилей (рис. 52) выбрать для устройств требуемые профили. В окне отображается список устройств, тип которых соответствует выбранному на шаге 3 профилю, в столбце ***Профиль*** каждому устройству соответствует список используемых в комплексе профилей для этого типа устройств (отображается наименование текущего выбранного для устройства профиля).

Примечание – В окне настройки использования профилей для устройств пользователь может свернуть дерево устройств, нажав кнопку ***Свернуть все*** (), найти требуемое устройство, используя поле ***Поиск***, а также выполнить фильтрацию списка устройств по используемому профилю, нажав в заголовке окна кнопку ***Фильтр*** () и выбрав установкой флагов в открывшемся окне фильтрации требуемые значения списков профилей ***Профили***, и типа профилей ***Переопределенный*** (*Да*, *Нет*).

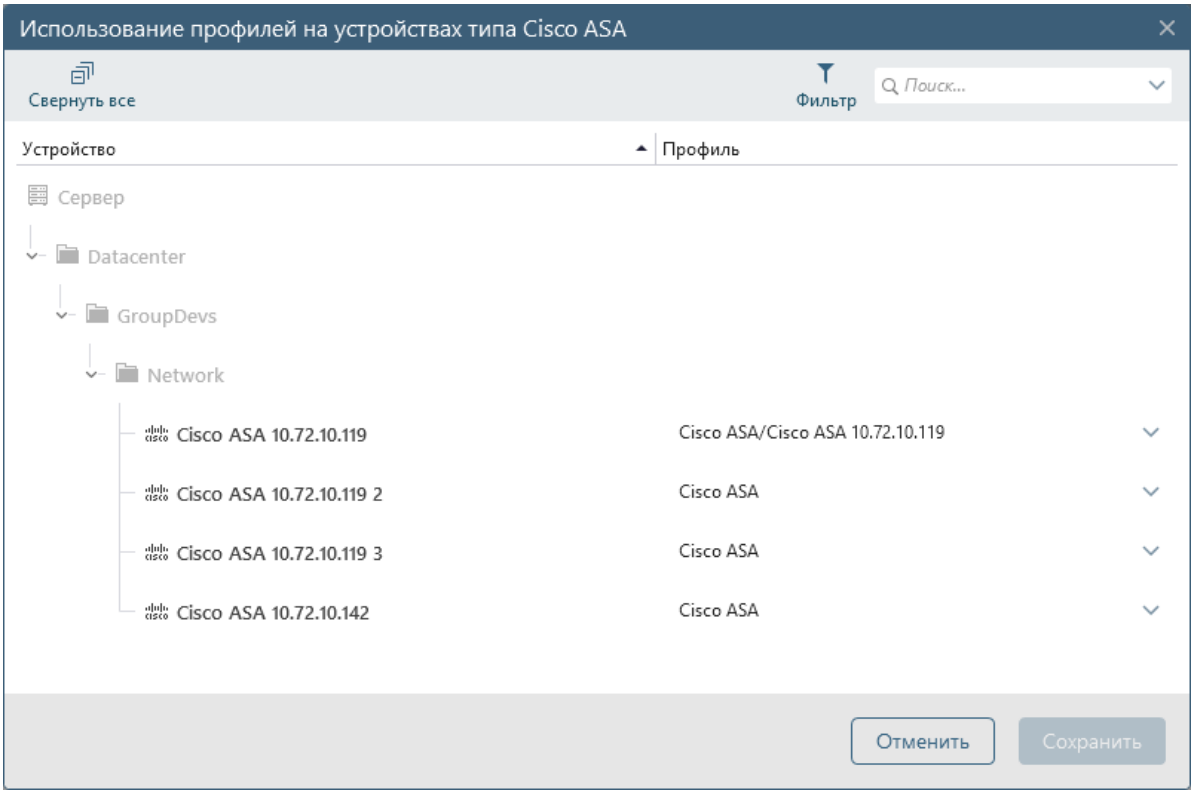


Рисунок 52 – Окно настройки использования профилей для устройств

7) После выбора в окне настройки использования профилей для устройств требуемых профилей нажать кнопку ***Сохранить***. Окно закроется, внесенные изменения будут сохранены.

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.

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*.

Последовательность действий и правила добавления ***Пользовательских*** отчетов и отчетов типа ***Фильтр*** приведены соответственно в пунктах 2.6.1 «Добавление пользовательских отчетов» и 2.6.2 «Добавление отчета типа Фильтр». Добавление отчетов с наименованием уже имеющегося отчета запрещено.

Настройка отчетов на сервере ПК заключается в:

1) Настройке отчетов в имеющихся профилях комплекса:
   - 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:
   - 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. Добавление пользовательских отчетов

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

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выбрать, при необходимости, сервер, для которого изменяется профиль.
3) В области *Настройки контроля* нажать кнопку ***Профили***.
4) В открывшейся форме управления профилями устройств (см. рис. 41) выделить необходимый профиль.
5) В заголовке вкладки ***Конфигурации*** (см. рис. 44) нажать кнопку ***Новый отчет*** (+).

6) В открывшемся окне **Новый отчет** (рис. 53) ввести необходимые параметры, в зависимости от вида добавляемого отчета: имя создаваемого отчета, тип отчета, настройки отчета, настройки тестирования, настройки использования.

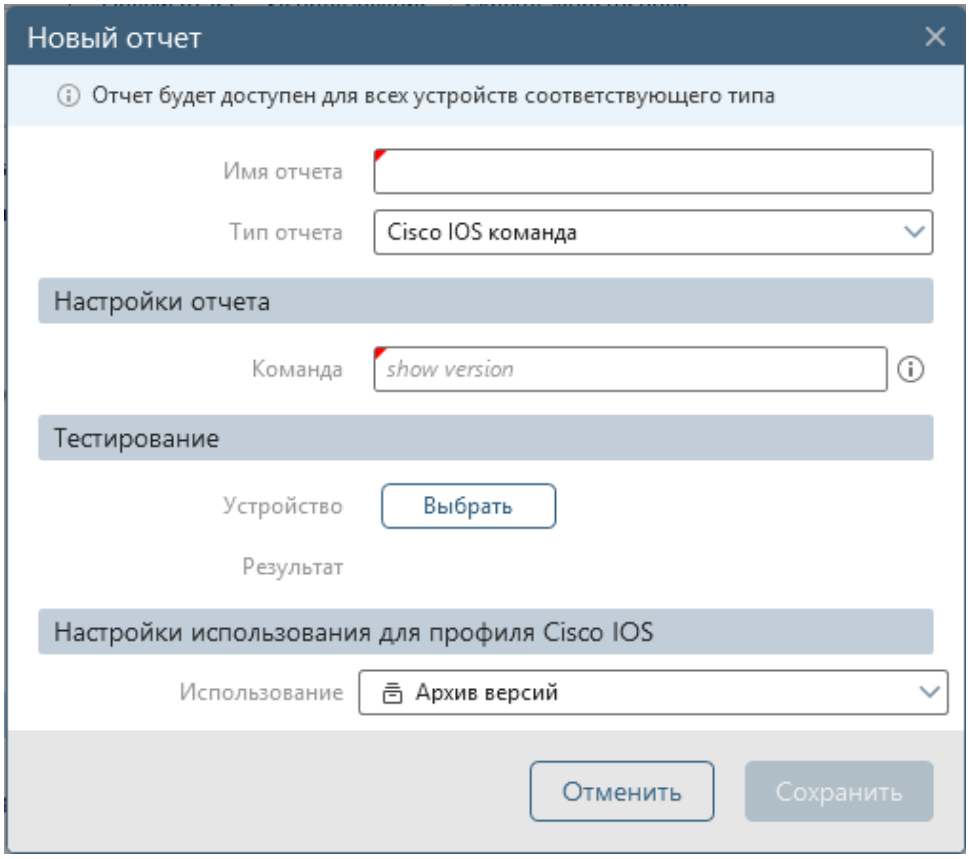


Рисунок 53 – Окно **Новый отчет**

Примечание – Настройка использования по умолчанию *Архив версий* распространяется только на тип устройств, для которого создается пользовательский отчет. Для других типов устройств будет применена настройка *Запрещено*.

7) Нажать кнопку ***Сохранить*.**

При создании пользовательского отчета существует возможность проверки корректности введенных параметров нового отчета. Для этого необходимо нажать кнопку ***Выбрать*** в поле **Устройство** области *Тестирование*, в открывшемся окне указать устройство, с которого будет выполняться загрузка нового отчета, и нажать кнопку ***Выбрать*** – начнется процесс загрузки нового отчета с выбранного устройства.

При создании отчета по контролю целостности (КЦ) для операционных систем Windows пользователь имеет возможность выбрать контролируемые файлы в окне, которое открывается по нажатию кнопки «🗁». Кроме того, пользователю для некоторых типов устройств (ОС, СУБД и др.) в поле **Шаблон** окна доступны для выбора шаблоны со списками файлов, которые необходимо поставить на КЦ (на рис. 54 приведен пример для ОС Windows).

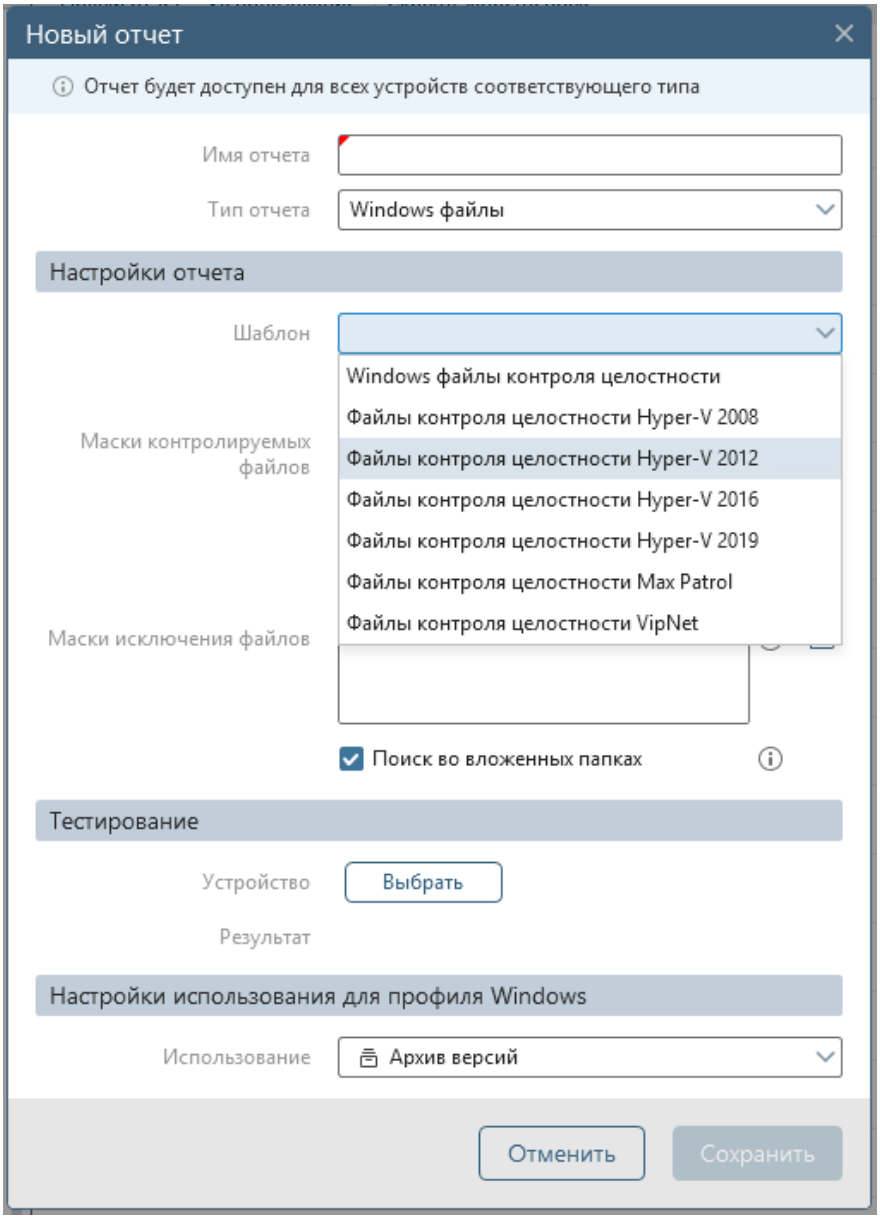


Рисунок 54 – Окно **Новый отчет** с раскрытым списком шаблонов

В Приложении 2 к документу 643.72410666.00082-01 96 01-02 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 3. Работа с устройствами» приведен перечень файлов, рекомендованных разработчиками устройств для постановки на контроль целостности при создании пользовательских отчетов для различных типов устройств и операционных систем (если для отчета выбран тип использования *Контроль изменений*).

2.6.2. Добавление отчета типа Фильтр

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*** ( )

В открывшемся окне **Фильтр содержимого** настроить условия отбора данных выбранного отчета. Для структурированных отчетов в соответствии с пунктом 2.6.2.1 «Настройка условий фильтрации для структурированных отчетов» и для текстовых отчетов – с пунктом 2.6.2.2 «Настройка условий фильтрации для текстовых отчетов» и нажать кнопку ***Применить***.

В консоли откроется форма просмотра отчета в соответствии с указанными настройками фильтрации (рис. 55). 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;
- 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***.

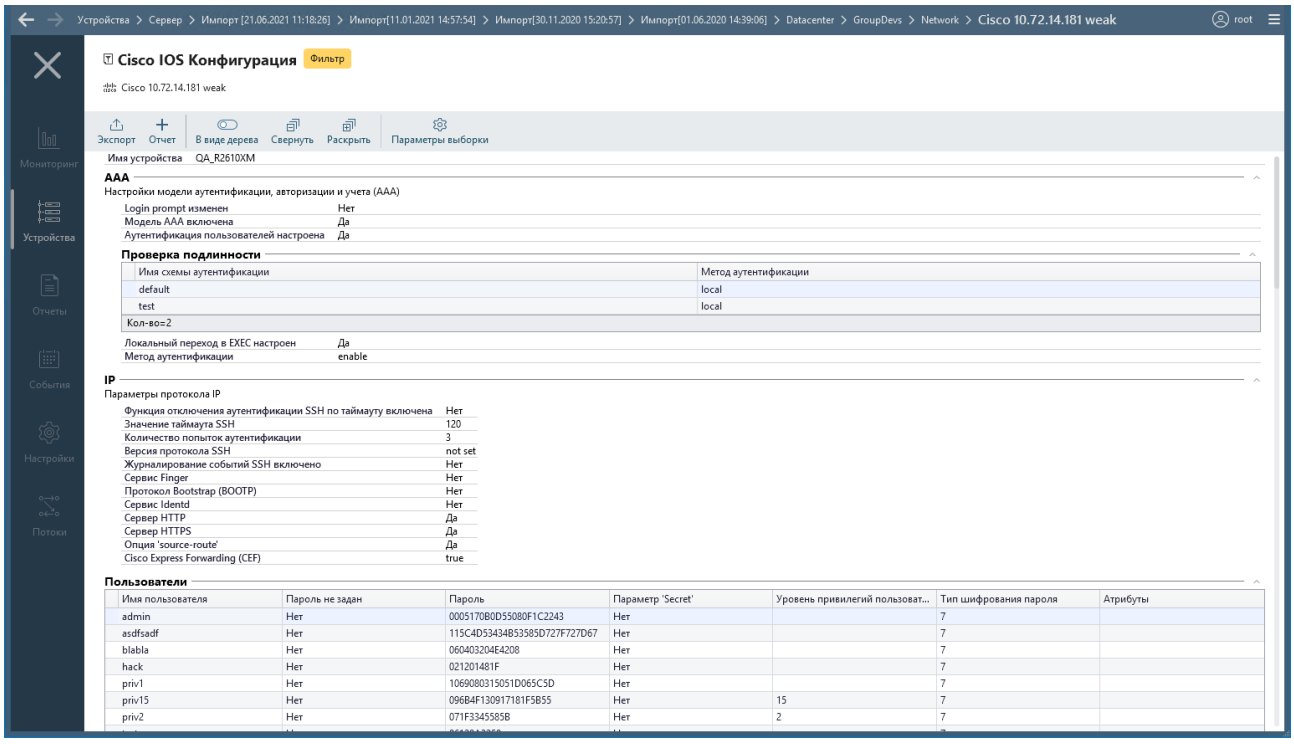


Рисунок 55 – Отображение структурированного отчета с заданными параметрами фильтра

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 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).

Для создания нового отчета типа *Фильтр* на основе заданных условий фильтрации пользователю необходимо выполнить следующие действия:

- нажать в форме просмотра отчета кнопку ***Отчет*** (+);
- в открывшемся окне **Сохранить фильтр** (рис. 56) проконтролировать заданные настройки фильтрации отчета и внести при необходимости изменения, ввести наименование нового типа отчета, выбрать режим его использования (см. таблицу 14) и нажать кнопку ***Сохранить***;
- нажать кнопку ***Закрыть*** (✕) в открывшемся окне с сообщением ***Создан <название отчета>*** (либо окно закроется автоматически через несколько секунд). В списке отчетов устройства (на вкладке ***Отчеты*** раздела **Устройства**) добавится строка нового отчета типа *Фильтр*.

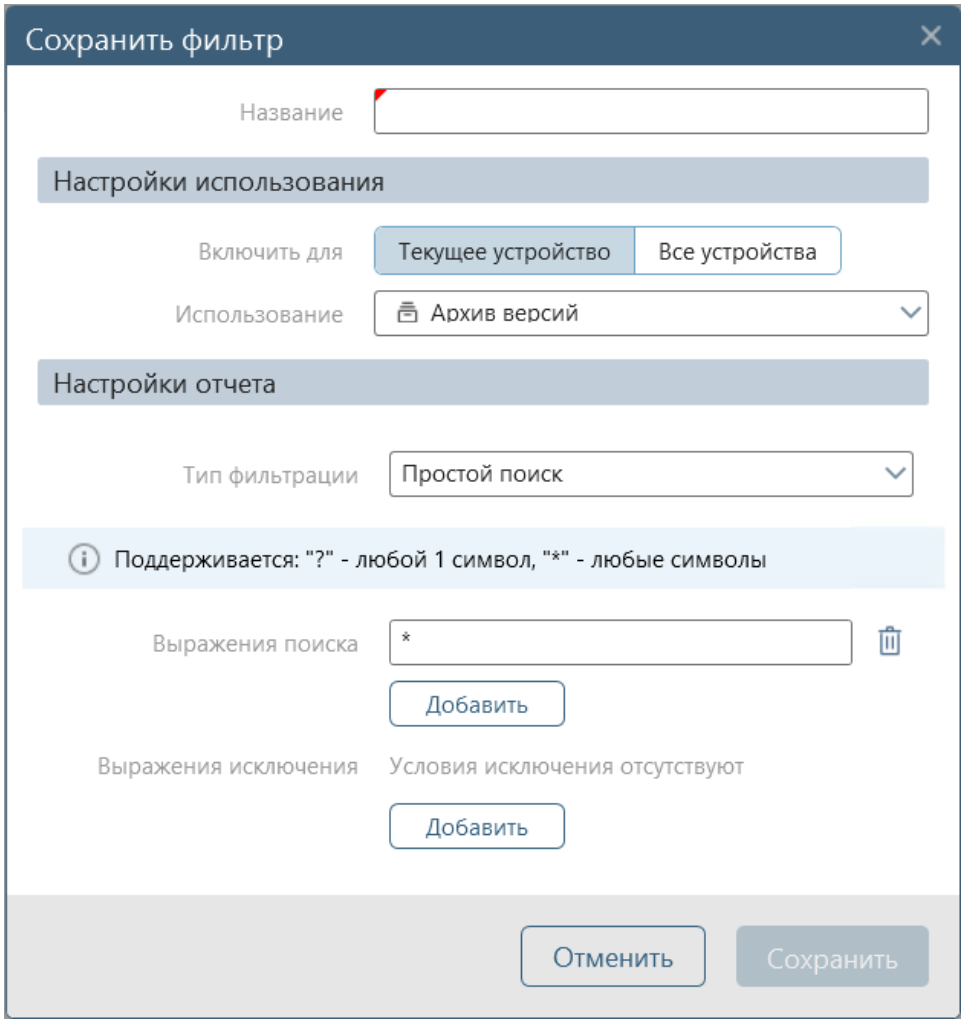


Рисунок 56 – Параметры сохранения нового типа отчета

Таблица 14 – Параметры нового типа отчета

Параметр	Описание/Назначение
Название	Имя нового типа отчета
Включить для	Выбор одного из значений: – *Текущее устройство* – отчет будет доступен для загрузки только с текущего устройства, для остальных устройств этого же типа будет включен режим использования *Запрещено*; – *Все устройства* – отчет будет загружаться со всех устройств того же типа, что и текущее устройство
Использование	Выбор режима использования отчета. Возможные значения: – *Контроль изменений* – при загрузке отчета будет выполняться контроль целостности загружаемых версий и их сравнение с эталоном; – *Архив версий* – в базе данных сервера ПК будут храниться все измененные версии отчета, загруженного с устройства; – *Только последний* – в базе данных сервера ПК будет храниться только последняя измененная версия отчета, загруженного с устройства
Настройки отчета	Содержит поля настройки условий отбора данных отчета. Для структурированных отчетов настройка выполняется в соответствии с пунктом 2.6.2.1 «Настройка условий фильтрации для структурированных отчетов» и для текстовых отчетов – с пунктом 2.6.2.2 «Настройка условий фильтрации для текстовых отчетов»

Созданный новый отчет станет доступен для загрузки с указанных устройств и просмотра после загрузки во вкладках ***Отчеты*** и ***Архив***.
Созданный с помощью условий фильтрации новый отчет будет доступен для последующей настройки.

2.6.2.1. 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. 57) выбрать установкой/отменой установки флагов параметры, которые должны отображаться в отчете. Состав доступных для выбора параметров отчета зависит от его типа.

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

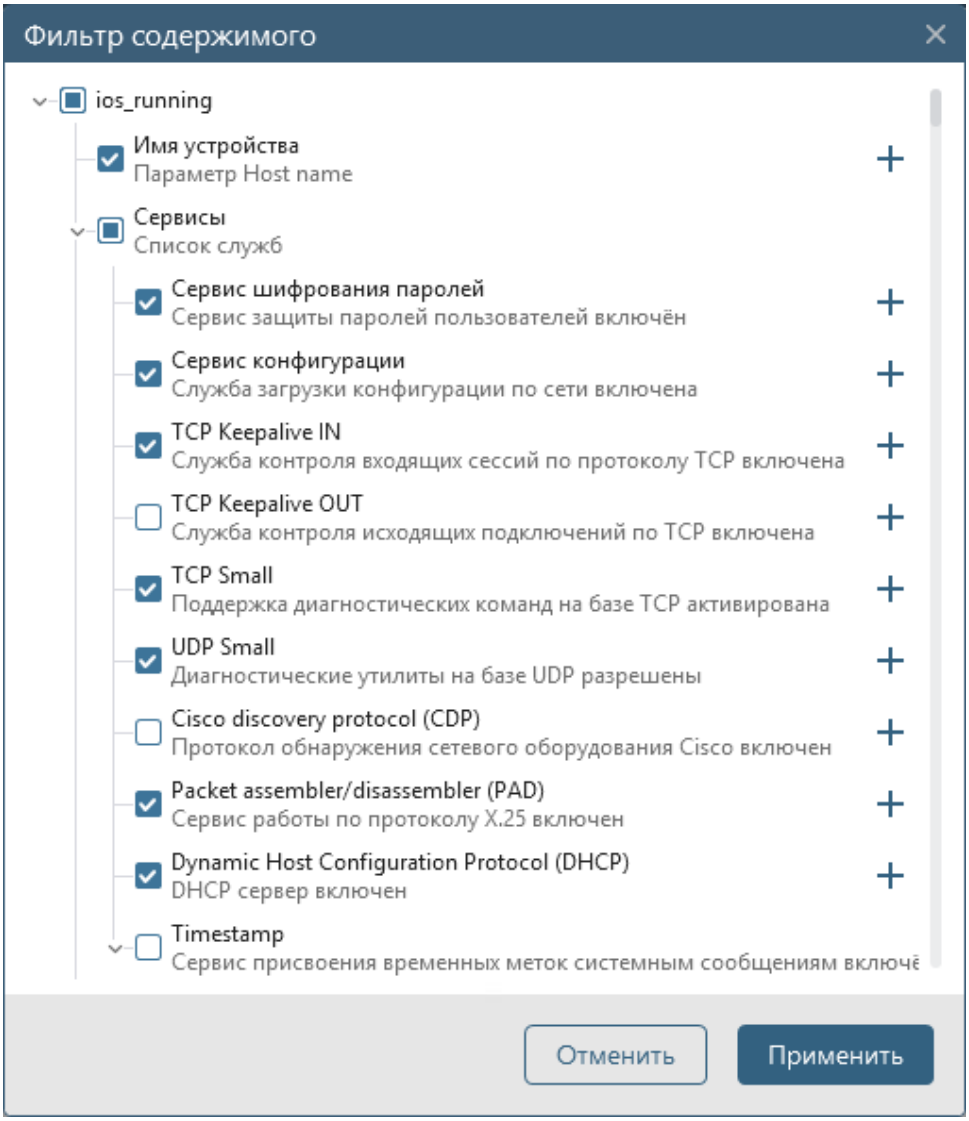


Рисунок 57 – Окно **Фильтр содержимого**

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. 58), ввести в текстовое поле значение для проверки.

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. 59).

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.

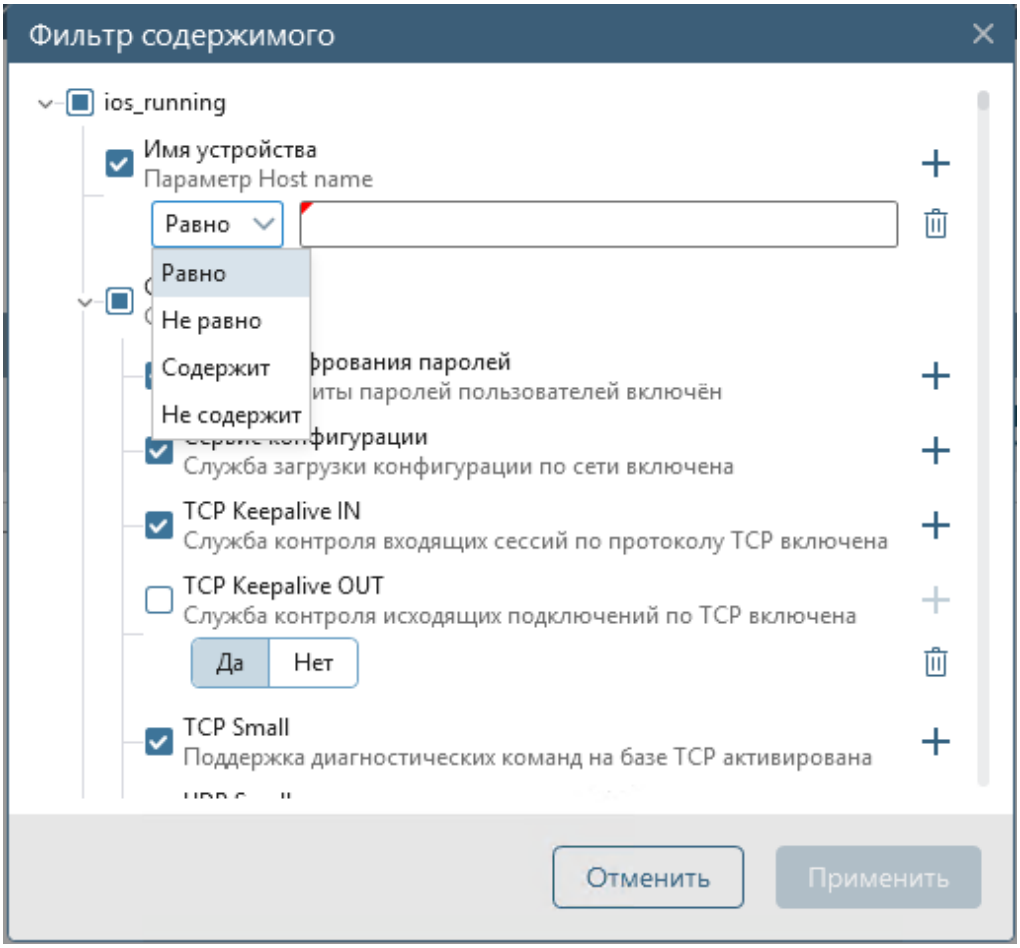


Рисунок 58 – Добавление условий для параметров

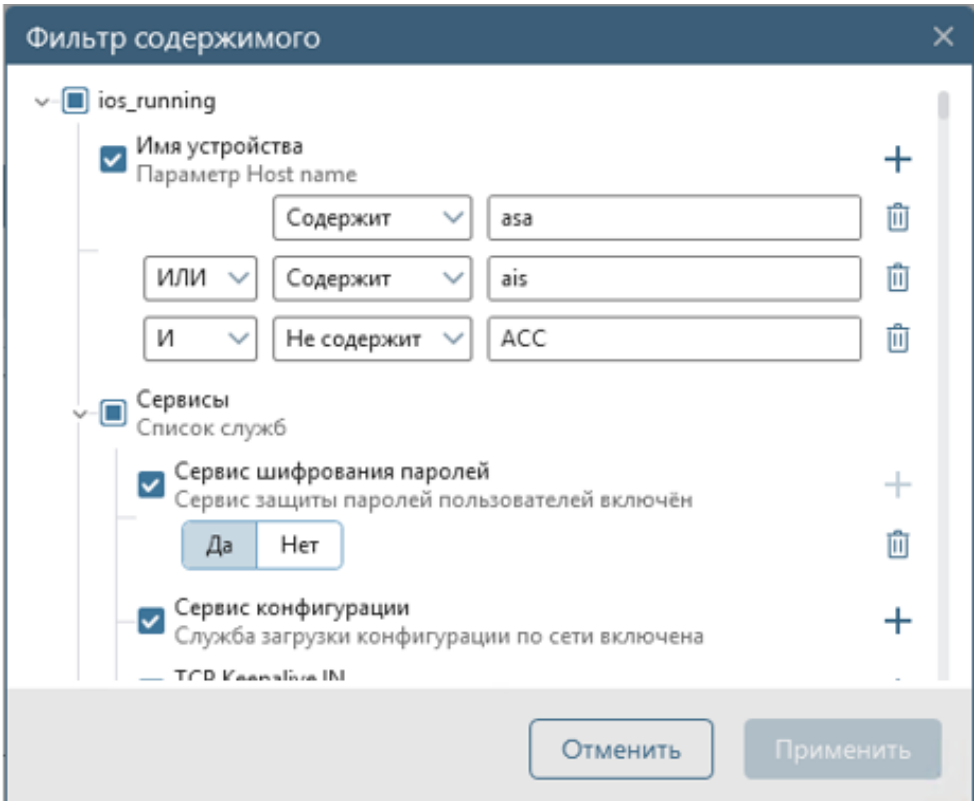


Рисунок 59 – Добавление нескольких условий для текстового параметра

2.6.2.2. Настройка условий фильтрации для текстовых отчетов

Для настройки условий отбора данных для текстовых отчетов пользователю необходимо выполнить следующие действия в окне **Фильтр содержимого** (рис. 60):

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.

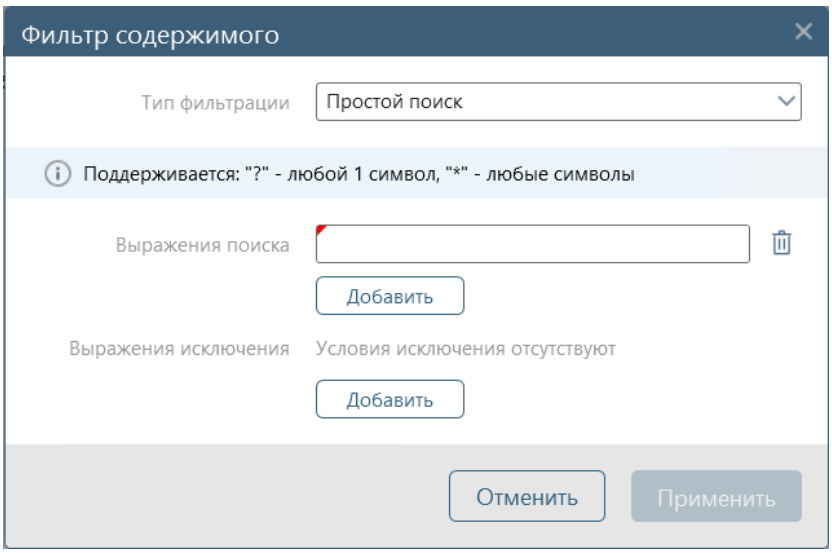
Примечание – Описание регулярных выражений стандарта PCRE, допустимых к применению в ПК «Efros Config Inspector» v.4, приведено в Приложении 1.

2) Ввести необходимые критерии отбора для фильтрации отчета:

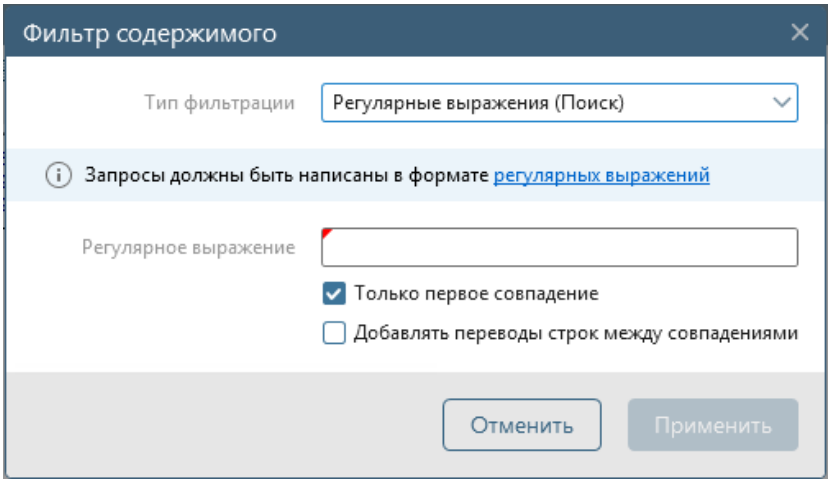
а) при выборе параметра ***Простой поиск*** (рис. 60, а) ввести ключевое значение в поле ***Выражения поиска*** (для ввода нескольких значений – нажимать кнопку ***Добавить*** и вводить новые значения); для исключения строк из отчета, в которых содержатся определенные значения, нажать кнопку ***Добавить*** в области *Выражения исключения* и ввести необходимое значение в открывшееся поле ввода (для ввода нескольких значений – нажимать кнопку ***Добавить*** и вводить новые значения).

б) при выборе параметра ***Регулярные выражения (Поиск)*** (рис. 60, 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.

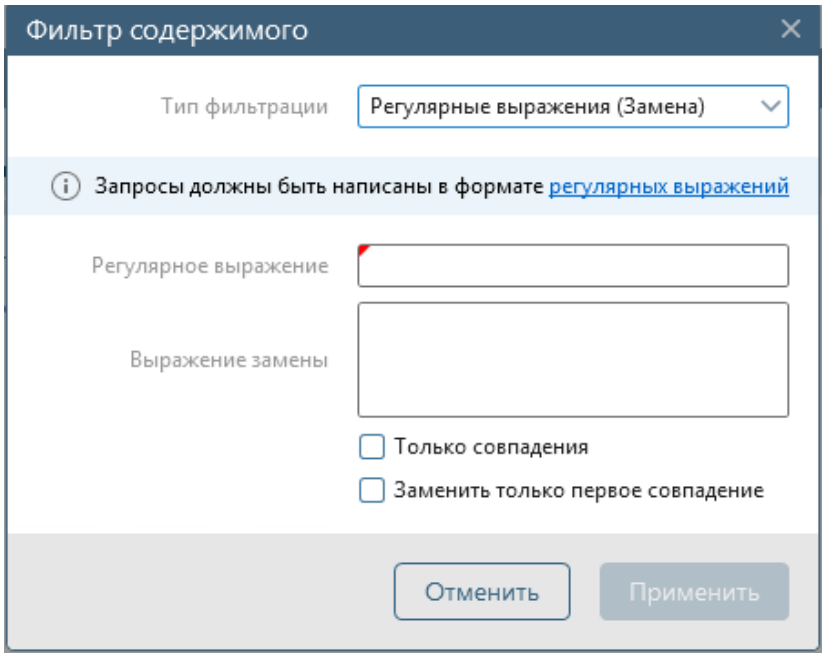
в) при выборе параметра ***Регулярные выражения (Замена)*** (рис. 60, в) ввести в поле ***Регулярное выражение*** шаблон для поиска искомых данных в загружаемом отчете, а в поле ***Выражение замены*** – данные, которыми будут заменены искомые выражения. При необходимости отметить требуемые параметры 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.



а)



б)



в)

Рисунок 60 – Фильтр содержимого текстового отчета

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

2.6.3. Изменение отчетов

На сервере ПК доступны для изменения только пользовательские отчеты и отчеты типа ***Фильтр***.
Правом изменения отчетов обладают только пользователи с правами *Управление* в категории *Настройки контроля.*

ВНИМАНИЕ: Нельзя изменить пользовательский отчет, предназначенный для контроля файлов на устройстве, в параметрах использования которого установлено ***Контроль изменений,*** а последняя загруженная версия отличается от эталона – во вкладке **Статус** устройства есть сообщение о нарушении целостности такого отчета!

Для изменения отчета необходимо выполнить следующие действия в клиентской консоли комплекса:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выбрать сервер, для профиля которого изменяется отчет.
3) В области *Настройки контроля* нажать кнопку ***Профили***.
4) В открывшейся форме управления профилями устройств (см. рис. 41) выделить необходимый профиль.
5) На вкладке ***Конфигурации*** выделить необходимый отчет.
6) В строке выбранного отчета нажать кнопку ***Изменить*** (⚙).
7) В открывшемся окне изменения выбранного отчета (пример см. на рис. 61) изменить необходимые параметры, в зависимости от вида отчета: список контролируемых файлов и имя отчета или команду для выполнения (подробнее см. пункт 2.5.3.1 «Настройка отчетов в профиле»).
8) Выполнить, при необходимости, тестовый запуск отчета, для чего нажать в блоке **Тестирование** кнопку ***Выбрать*** и выбрать в открывшемся окне **Выбор устройств** устройство.
9) Скорректировать, при необходимости, по результатам тестового запуска отчета, параметры отчета.
10) Нажать кнопку ***Сохранить***.

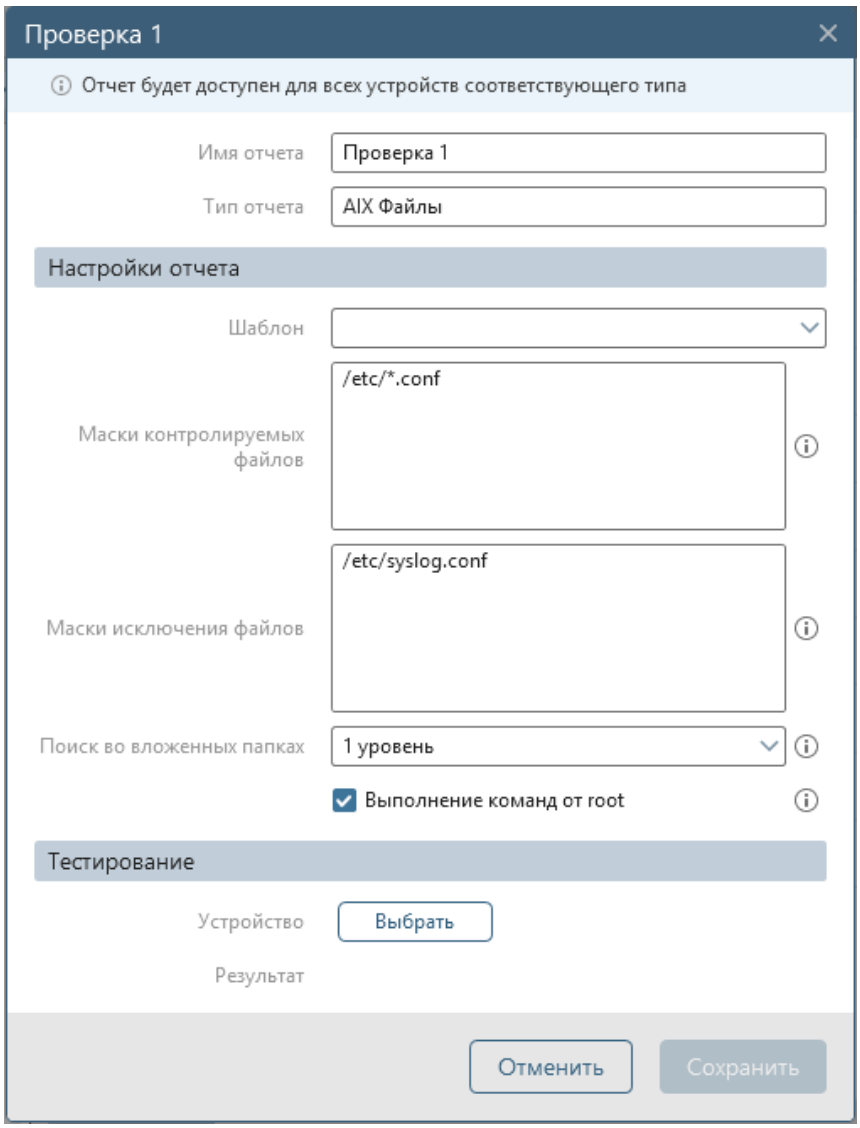


Рисунок 61 – Окно изменения отчета

2.6.4. Клонирование отчетов

На основе пользовательских отчетов, хранящихся на сервере ПК, можно создать (клонировать) новый отчет с теми же параметрами и настройками для профилей комплекса и контролируемых устройств.

Для клонирования отчета необходимо выполнить следующие действия в клиентской консоли комплекса:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выбрать сервер, для профиля которого клонируется отчет.
3) В области *Настройки контроля* нажать кнопку ***Профили***.
4) В открывшейся форме управления профилями устройств (см. рис. 41) выделить необходимый профиль.
5) На вкладке ***Конфигурации*** выделить клонируемый отчет.
6) В контекстном меню отчета выбрать пункт ***Клонировать*** или нажать в его строке кнопку ***Меню*** (⋯) и выбрать в раскрывшемся меню пункт ***Клонировать***.

7) В открывшемся окне клонирования выбранного отчета (рис. 62) изменить имя отчета, настройки отчета. При необходимости, можно внести изменения и в другие параметры клонируемого отчета (правила внесения изменений в отчет см. в пункте 2.5.3.1 «Настройка отчетов в профиле»);

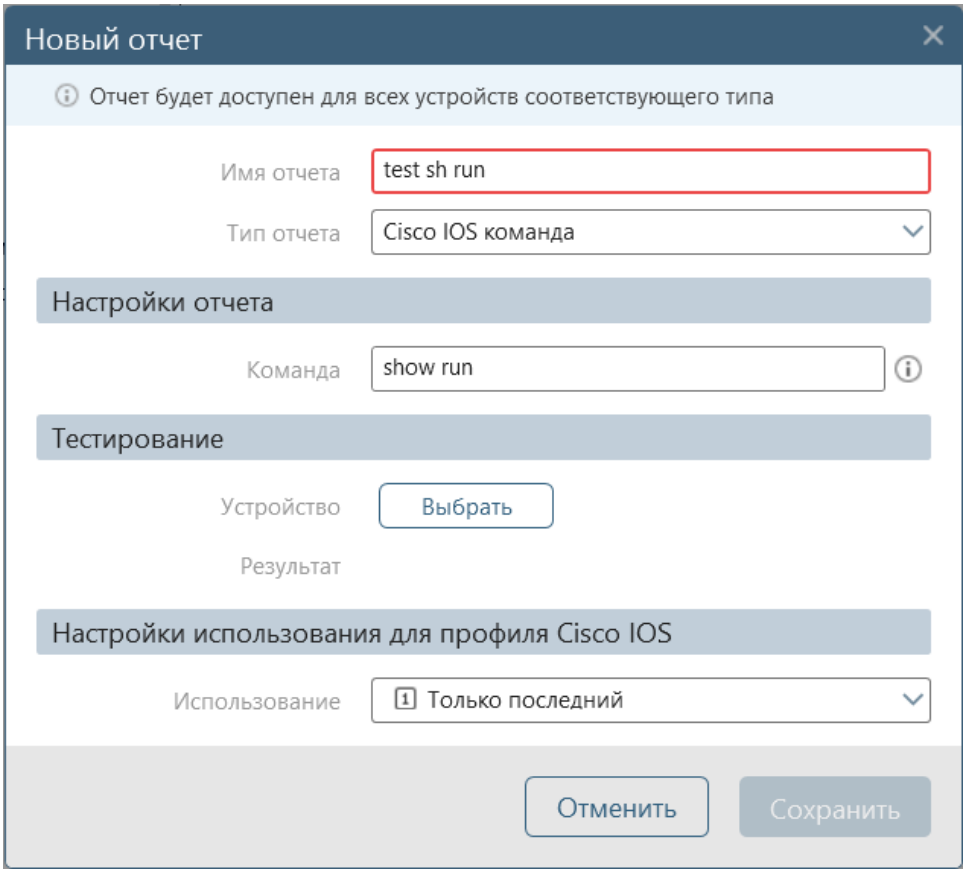


Рисунок 62 – Окно клонирования отчета

8) Выполнить, при необходимости, тестовый запуск отчета, для чего нажать в блоке **Тестирование** кнопку ***Выбрать*** и выбрать в открывшемся окне **Выбор устройств** устройство.

9) Скорректировать, при необходимости, по результатам тестового запуска отчета параметры отчеты.

10) Выбрать необходимый вариант использования отчета.

11) Нажать кнопку ***Сохранить***.

Будет создан пользовательский отчет с заданными настройками. Созданный отчет доступен для изменения в соответствии с п. 2.6.3 «Изменение отчетов».

2.6.5. Удаление отчетов

С сервера ПК можно удалить только пользовательские отчеты или отчеты, созданные на основе фильтра (тип отчета *Фильтр*). Удалить их могут только пользователи комплекса с правами *Управление* в категории *Настройки контроля*. Отчеты типа *Общий* удаляются с сервера автоматически при отключении внешнего модуля.

Нельзя удалить отчет, предназначенный для контроля файлов на устройстве, в параметрах использования которого установлено ***Контроль изменений***, а

последняя загруженная версия отличается от эталона – во вкладке ***Статус*** устройства есть сообщение о нарушении целостности такого отчета.

Для удаления отчета необходимо выполнить следующие действия в клиентской консоли комплекса:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выбрать сервер, для профиля которого удаляется отчет.
3) В области *Настройки контроля* нажать кнопку ***Профили***.
4) В открывшейся форме управления профилями устройств (см. рис. 41) выделить необходимый профиль.
5) На вкладке ***Конфигурации*** нажать в строке удаляемого отчета кнопку ***Меню*** (⋯) и выбрать в раскрывшемся меню пункт ***Удалить***.
6) В открывшемся окне **Удаление** нажать кнопку ***Удалить*** для подтверждения удаления выбранного отчета. Отчет будет удален с сервера ПК.

2.6.6. 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. 63) выделить требуемый отчет, в контекстном меню отчета выбрать пункт ***Настройки отчета*** или нажать в его строке кнопку ***Настройка*** (⚙).

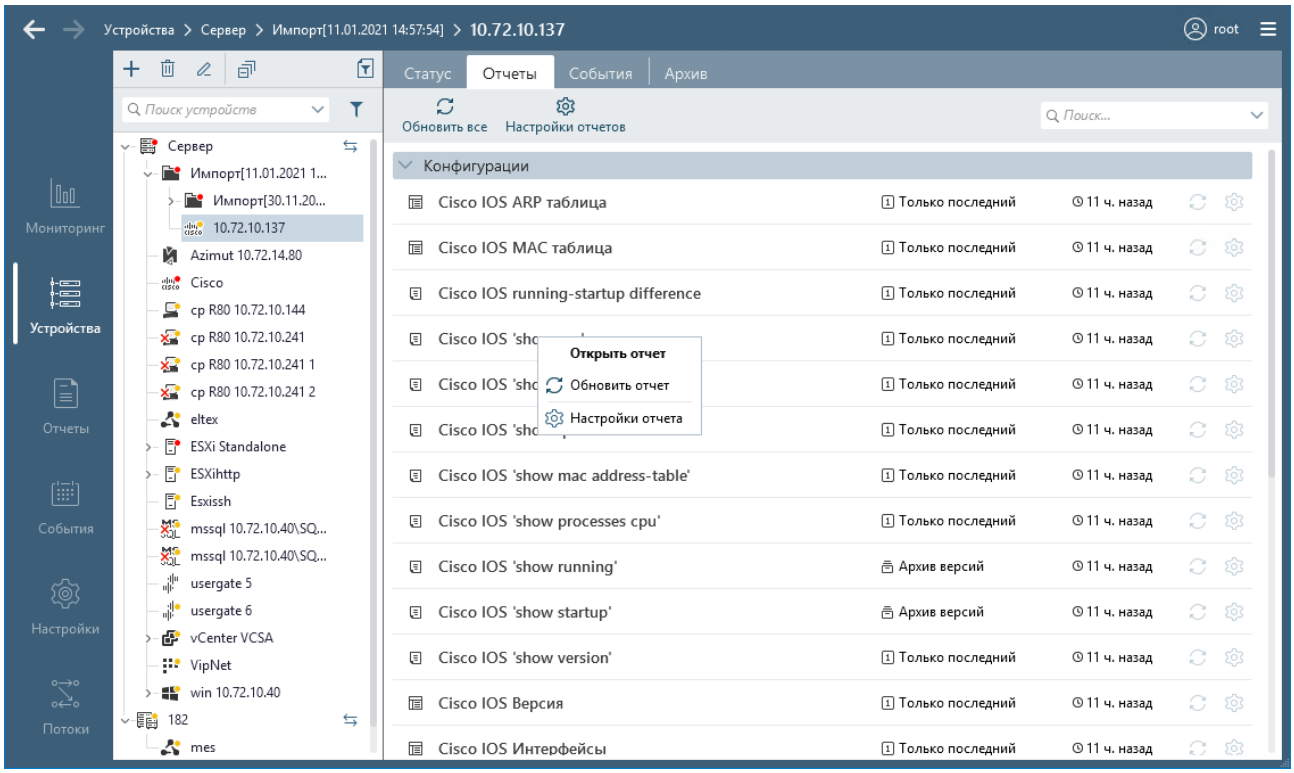


Рисунок 63 – Вкладка **Отчеты** выбранного устройства

4) В открывшемся окне настройки отчета из раскрывающегося списка поля *Использование* выбрать необходимое значение (рис. 64, состав и описание значений полей окна приведено в таблице 15).

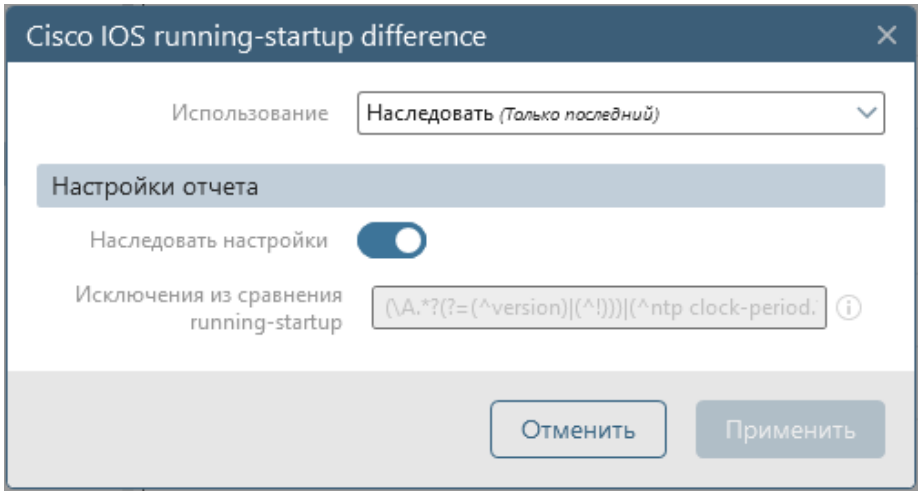


Рисунок 64 – Окно настройки отчета

Таблица 15 – 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	Для настройки дополнительных параметров (например, масок контролируемых файлов, параметров выполнения команд и т.д.).

Настройка	Описание/Назначение
настроек	Поля доступны для редактирования после перевода переключателя в поле ***Наследовать настройки*** в положение *Выключен* ( )

5) Изменить, при необходимости, дополнительные параметры (при их наличии в отчете), предварительно выключив переключатель ***Наследовать настройки*** (см. рис. 64).

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

2.6.7. Настройка одного отчета для нескольких устройств

Для внесения изменений в настройки отчетов для нескольких устройств, подключенных к комплексу, пользователю необходимо выполнить следующие действия:

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

2) Выбрать при необходимости сервер, для профиля которого настраивается отчет.

3) В области *Настройки контроля* нажать кнопку ***Профили***.

4) В открывшейся форме настройки профилей, на вкладке ***Конфигурации*** в контекстном меню настраиваемого отчета выбрать пункт ***Настройки для устройств*** (рис. 65).

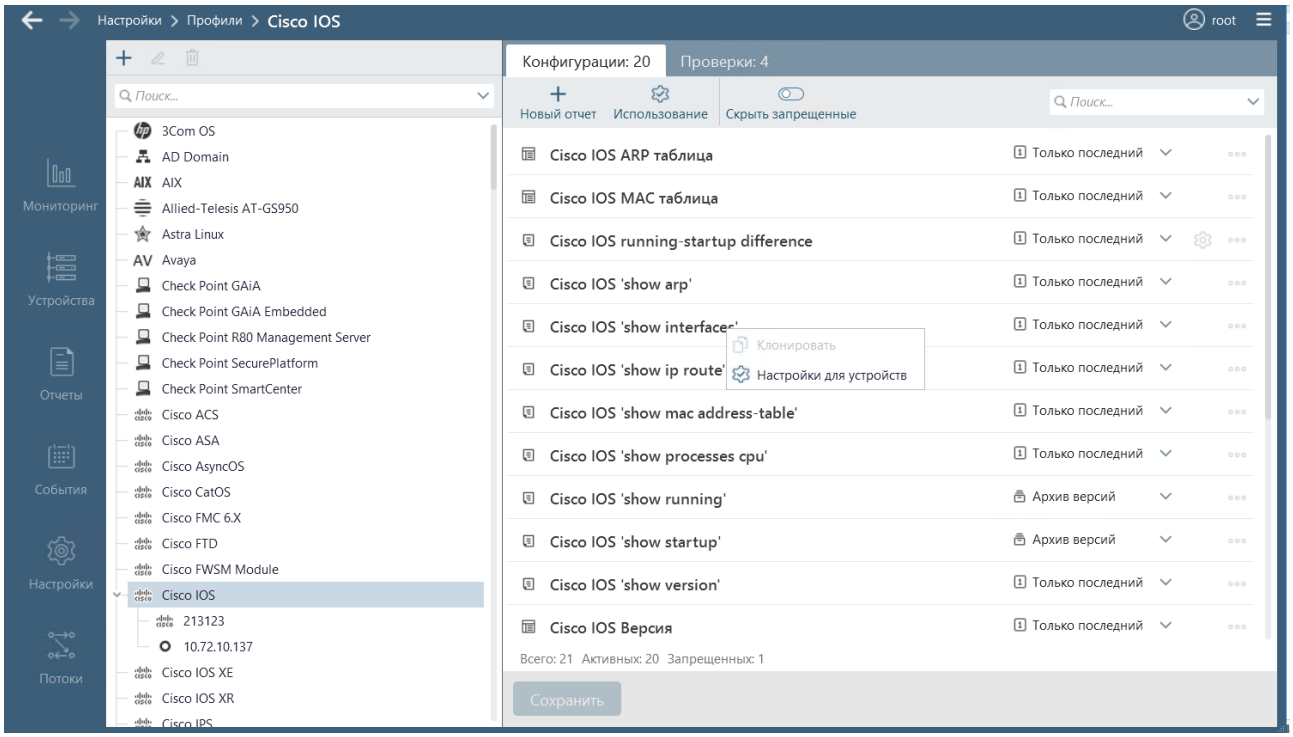


Рисунок 65 – Вкладка ***Конфигурации*** с открытым контекстным меню отчета

5) В открывшемся окне настройки отчета (рис. 66, состав и описание значений полей окна приведено в таблице 16) в строке необходимого устройства

выбрать из раскрывающегося списка поля ***Использование*** требуемое значение варианта использования отчета для устройства.

6) Для изменения дополнительных параметров выбранного отчета (при их наличии для отчета) щелкнуть по кнопке ***Параметры*** (⚙) в окне настройки отчета.

7) В открывшемся окне настройки дополнительных параметров отчета (см. пример на рис. 64, состав и описание значений полей окна приведено в таблице 15) выключить переключатель в поле ***Наследовать настройки***, внести требуемые изменения и нажать кнопку ***Применить*** (подробнее см. п. 2.5.3.1 «Настройка отчетов в профиле»).

8) В окне настройки отчета нажать кнопку ***Сохранить***. Окно настройки отчета для профилей закроется, внесенные изменения будут сохранены.

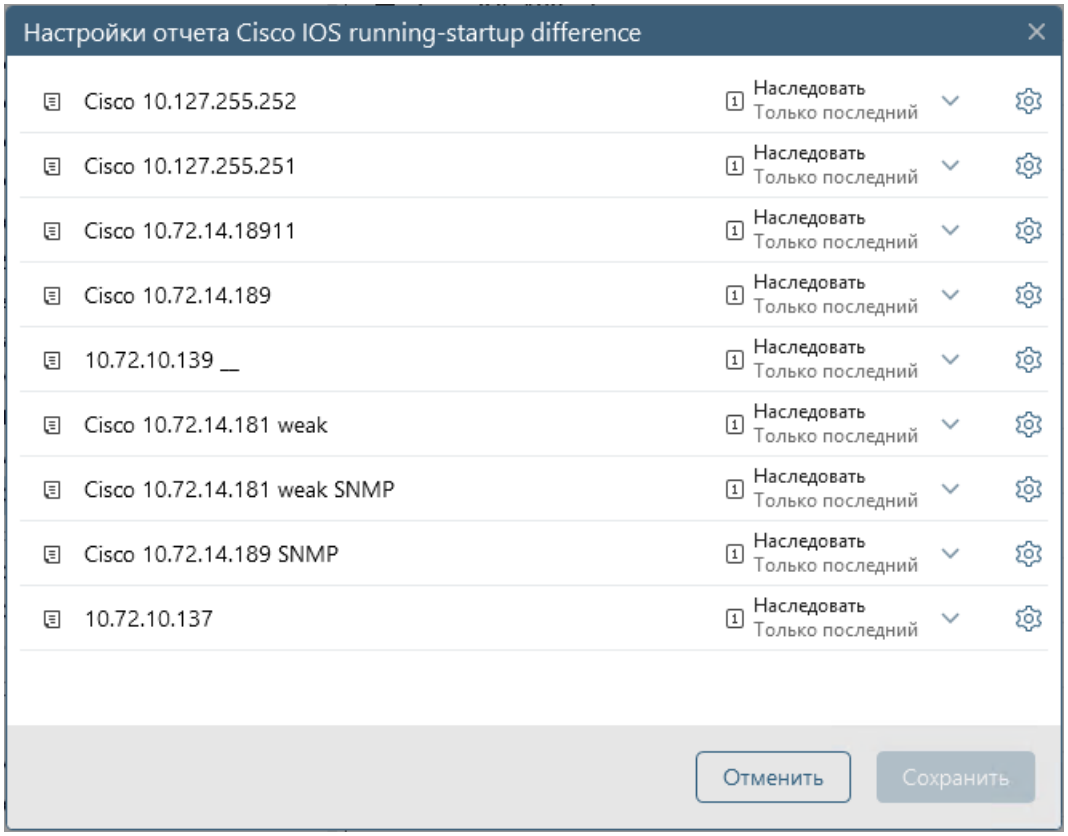


Рисунок 66 – Окно **Настройки отчета**

Таблица 16 – Состав и описание полей окна настройки отчета для группы устройств

Поле	Описание/Назначение
Устройство	Имя устройства
Использование	Выбор режима использования отчета. Возможные значения: – *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;

Поле	Описание/Назначение
	– *Запрещено* – загрузка отчета с устройств запрещена вне зависимости от настроек базового профиля; – *Наследовать (XXXXX)* – применить настройки базового профиля выбранного устройства
Без названия	Содержит кнопку ***Параметры*** (⚙). При нажатии кнопки открывается окно настройки дополнительных параметров выбранного отчета (см. пример на рис. 64)

2.6.8. 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. 63) нажать кнопку ***Настройки отчетов*** (⚙).

4) Откроется окно настройки отчетов выбранного устройства (рис. 67), в котором в поле ***Профиль устройства*** отображается наименование устройства, далее список всех отчетов устройства.

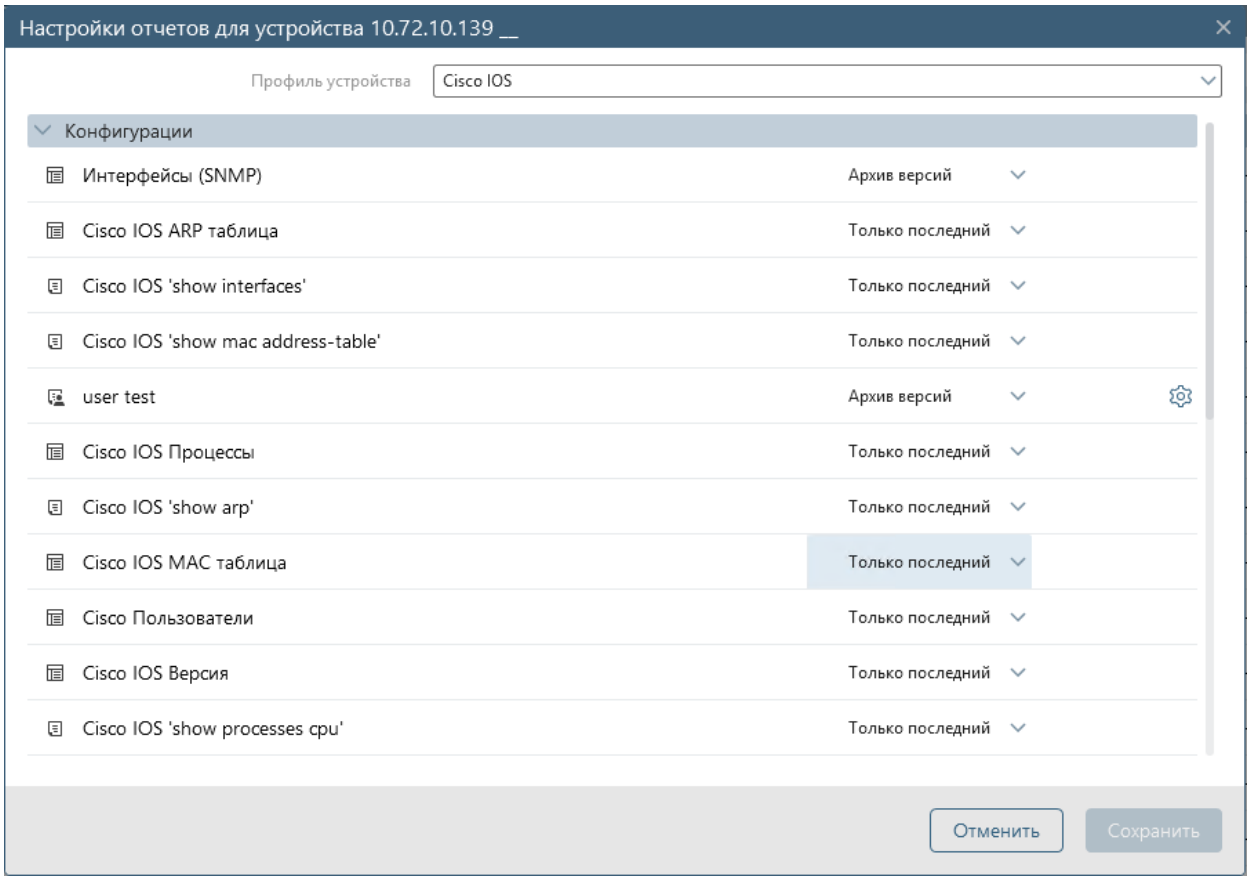


Рисунок 67 – Окно настройки всех отчетов устройства

5) Из раскрывающегося списка поля ***Использование*** выбрать необходимое значение для каждого отчета (состав и описание значений полей окна приведено в таблице 16).

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. 64, состав и описание значений полей окна приведено в таблице 15) 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

2.6.9. 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. 68) 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.

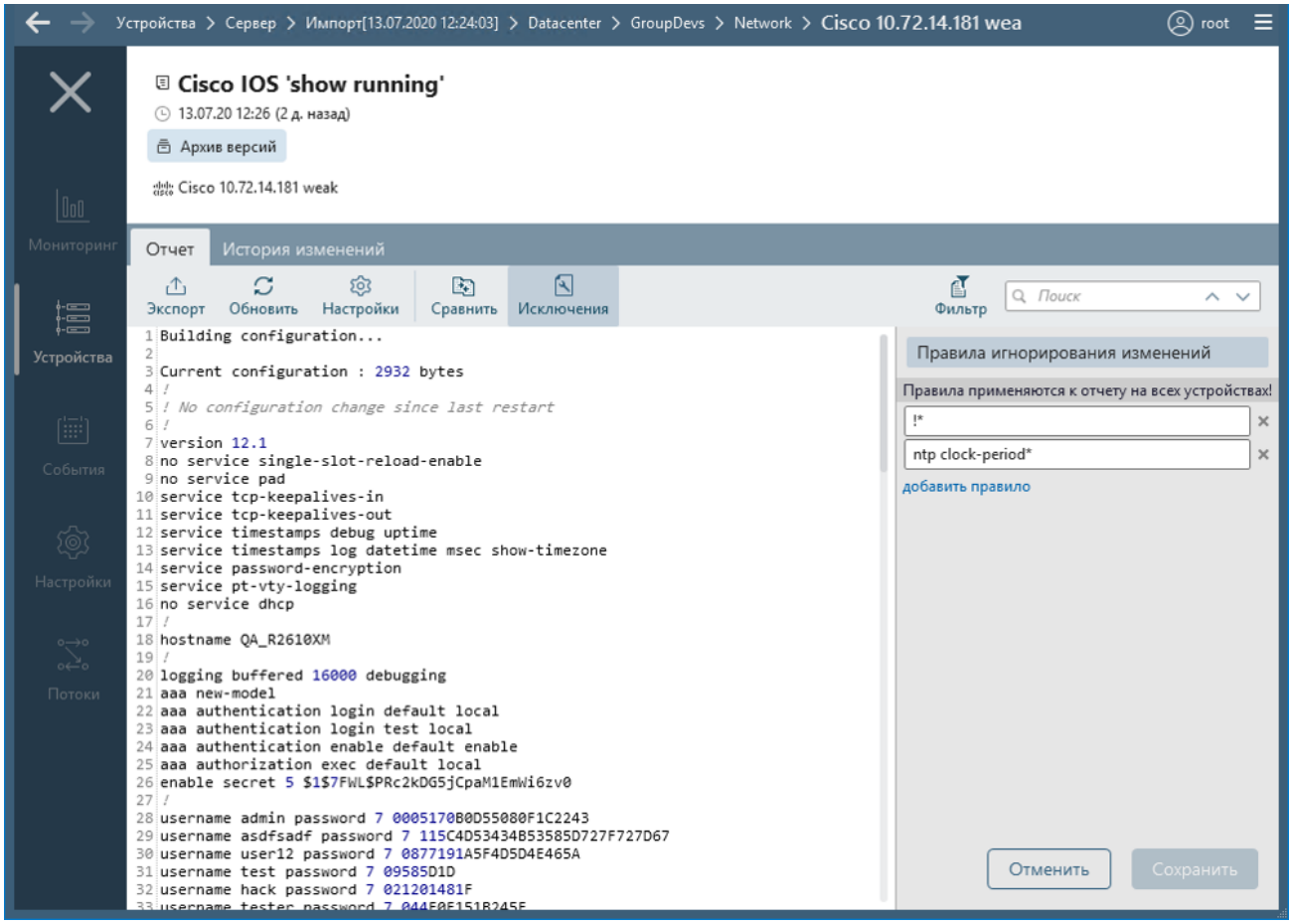


Рисунок 68 – Окно просмотра отчета с открытой областью настройки правил игнорирования изменений в отчетах

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 только пользователи комплекса с правами *Управление* в категории *Настройки контроля*.

Для 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. 69), 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 17).

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

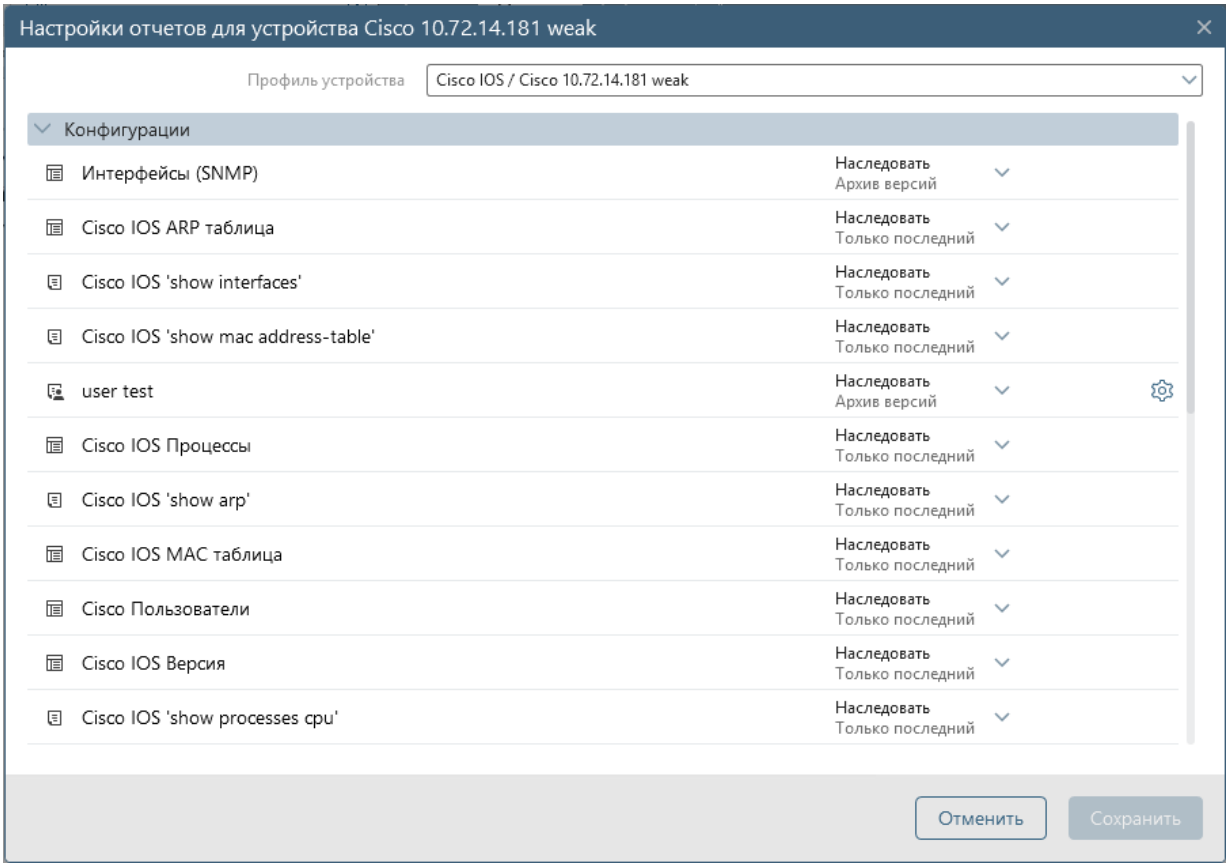


Рисунок 69 – Окно настройки всех доступных для устройства отчетов

Таблица 17 – Состав и описание полей окна настройки отчетов для устройства

Поле	Описание/Назначение
Профиль устройства	Наименование профиля устройства
Конфигурации/Проверки	Наименование отчета

Поле	Описание/Назначение
Использование	Выбор режима использования отчета. Возможные значения: – *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 выбранного устройства. В скобках отображается значение, установленное для отчета 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. 70 состав и описание значений полей окна приведено в таблице 18) 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.

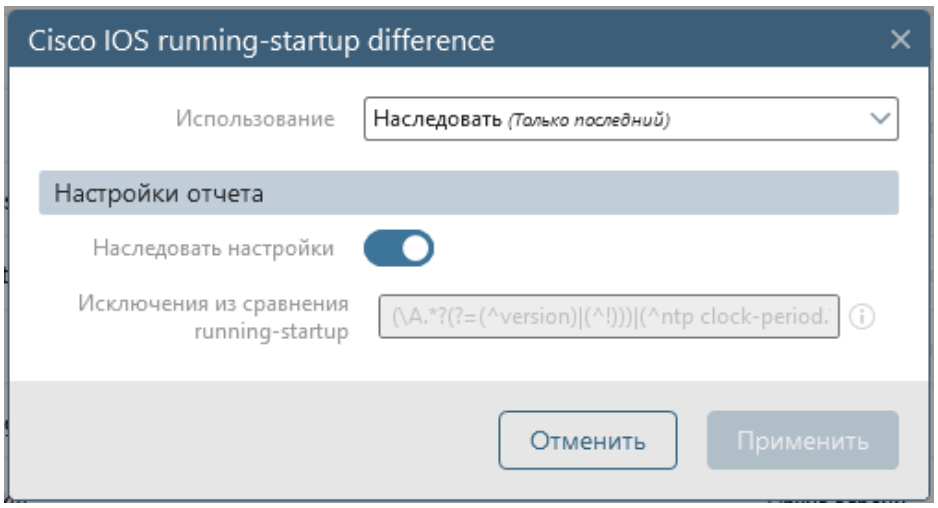


Рисунок 70 – Окно настроек отчета для устройства

Таблица 18 – Состав и описание полей окна настроек отчета для устройства

Поле	Описание/Назначение
Использование	Выбор настройки использования отчета. Возможные значения перечислены в таблице 17
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 параметров выполнения проверок

Изменять параметры выполнения проверок устройств могут только пользователи с правами *Управление* в категории *Настройки контроля*.

Для внесения изменений в настройки проверок для выбранного профиля пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выбрать сервер, для профиля которого настраивается проверка.
3) В области *Настройки контроля* нажать кнопку ***Профили*** для перехода в форму настройки профилей.
4) В открывшейся вкладке ***Профили,*** в поле списка профилей, выбрать профиль и перейти на вкладку ***Проверки*** (рис. 71).

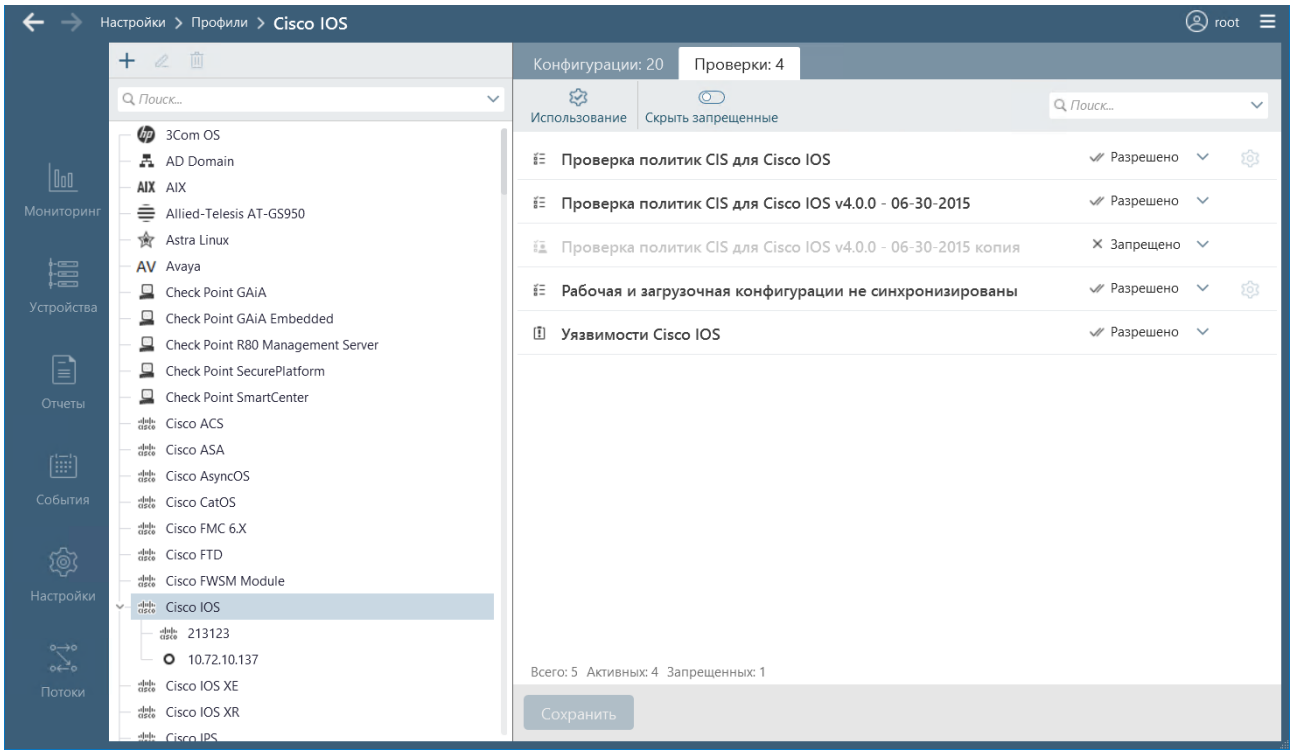


Рисунок 71 – Вкладка ***Проверки***

5) Во вкладке выбрать из перечня значений раскрывающегося списка поля ***Использование*** требуемое значение варианта использования редактируемой проверки для выбранного профиля (состав и описание значений полей окна приведено в таблице 19).

Таблица 19 – Состав и описание полей окна настройки проверок устройства

Поле	Описание/Назначение
Проверки	Наименование проверки
Использование	Выбор режима использования проверки. Возможные значения: – *Разрешено* – разрешить проверку вне зависимости от настроек базового профиля; – *Запрещено* – запретить проверку вне зависимости от настроек базового профиля; – *Наследовать (XXXX)* – применить настройки базового профиля выбранного устройства. В скобках отображается значение, установленное для проверки в базовом профиле
Без названия	Содержит кнопку ***Настройки правил*** ⚙. По нажатию кнопки открывается окно настроек правил соотвествующей проверки

6) Для изменения дополнительных параметров выбранной проверки – нажать в строке проверки кнопку ***Настройки правил*** (⚙).

7) В открывшемся окне дополнительных настроек правил выбранной проверки (рис. 72, состав и описание значений полей окна приведено в таблице 20):

- выключить переключатель в поле ***Наследовать настройки***;
- изменить, при необходимости, режим выполнения для выбранных правил проверки, выбрав в поле ***Выполнение*** таблицы правил требуемое значение;
- изменить, при необходимости, настройки исключений для отдельных правил проверки;
- нажать кнопку ***Применить*** для сохранения внесенных изменений.

8) Нажать кнопку ***Сохранить*** во вкладке ***Проверки***.

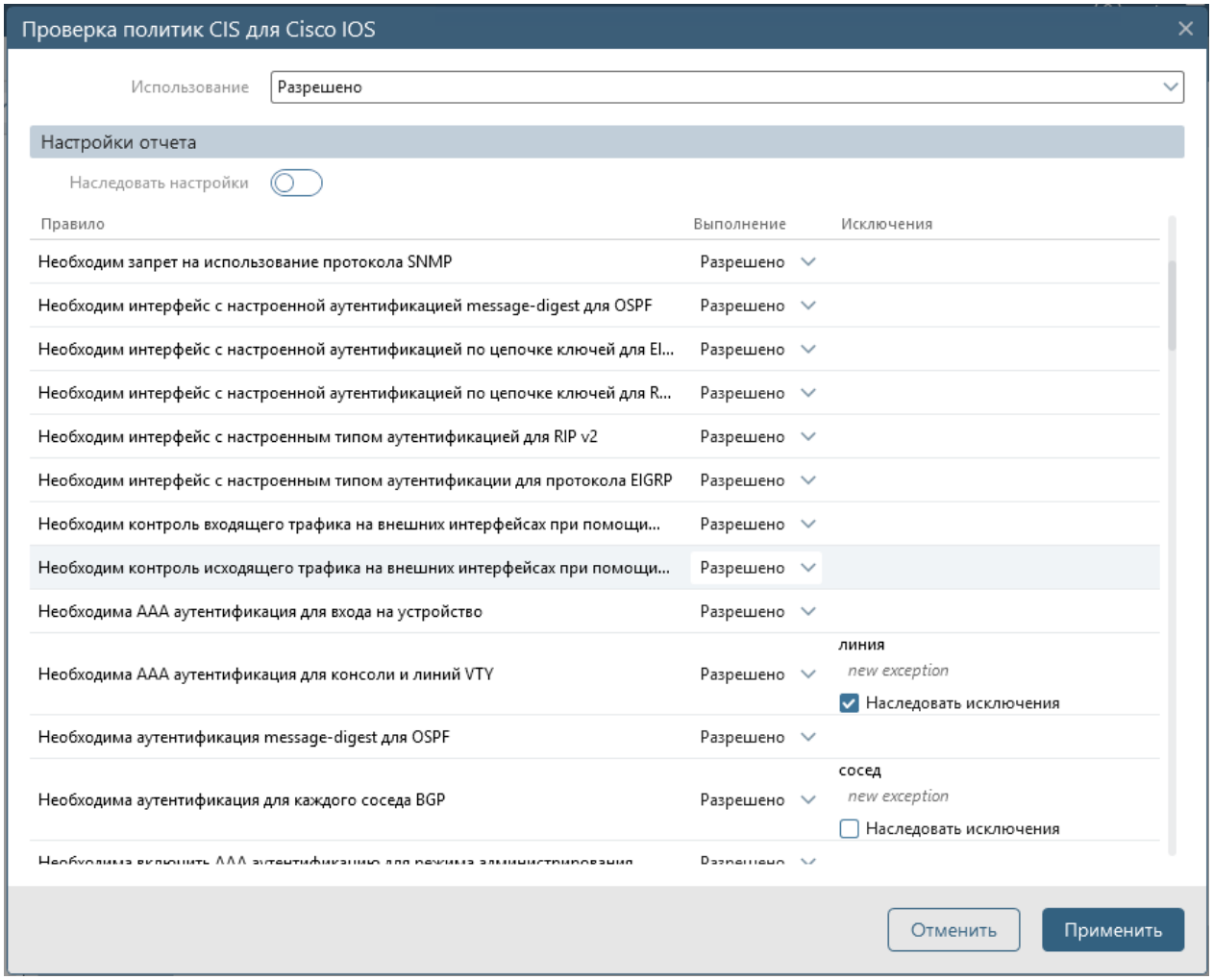


Рисунок 72 – Окно настройки правил проверки политик устройства

Таблица 20 – Состав и описание полей окна настройки правил проверки устройства

Поле	Описание/Назначение
Использование	Выбор режима использования проверки. Возможные значения перечислены в таблице 19
Наследовать настройки	При включенном переключателе () настройки проверки не доступны для внесения изменений, при выключенном () – пользователь имеет возможность внесения изменений в настройки отдельных правил проверки
Правило	Перечень правил проверки
Выполнение	Содержит значения режима выполнения отдельных правил в составе проверки: – *Разрешено* – разрешить выполнение правила; – *Запрещено* – запретить выполнение правила; – *Наследовать (XXXX)* – применить настройки базового профиля выбранного устройства. В скобках отображается значение, установленное для правила в базовом профиле
Исключения	Поле заполняется только для правил, в которых могут быть назначены исключения.

Поле	Описание/Назначение
	При включенном переключателе ***Наследовать настройки*** содержит значения, установленные в родительском профиле и не доступно для редактирования. При выключенном переключателе – содержит список доступных для настройки исключений при выполнении правила. Для ввода нового исключения необходимо ввести необходимое значение в строке ***новое значение*** и нажать клавишу клавиатуры **ENTER**

2.7.3. Настройка режима использования обработчиков событий для устройств

Изменять настройки режима использования обработчиков событий для устройства могут только пользователи с правами *Управление* в категории *Настройки контроля*. Настройка использования триггеров может быть выполнена как в списке триггеров вкладки ***Обработчики событий*** (см. п. 2.4.4 «Настройка использования триггеров») для всех устройств (групп) сервера ПК, так и в списке устройств раздела **Устройства** для каждого устройства (группы) отдельно.

Для внесения изменений в настройки 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. 73) перейти на вкладку ***Обработчик событий*** (рис. 74).
5) В строке настраиваемого обработчика событий выбрать из перечня значений раскрывающегося списка поля *Использование* требуемое значение варианта использования триггера для выбранного устройства (см. рис. 74, состав и описание значений полей окна приведено в таблице 21).
6) Нажать кнопку ***Сохранить***. Окно свойств устройства закроется, внесенные изменения будут сохранены.

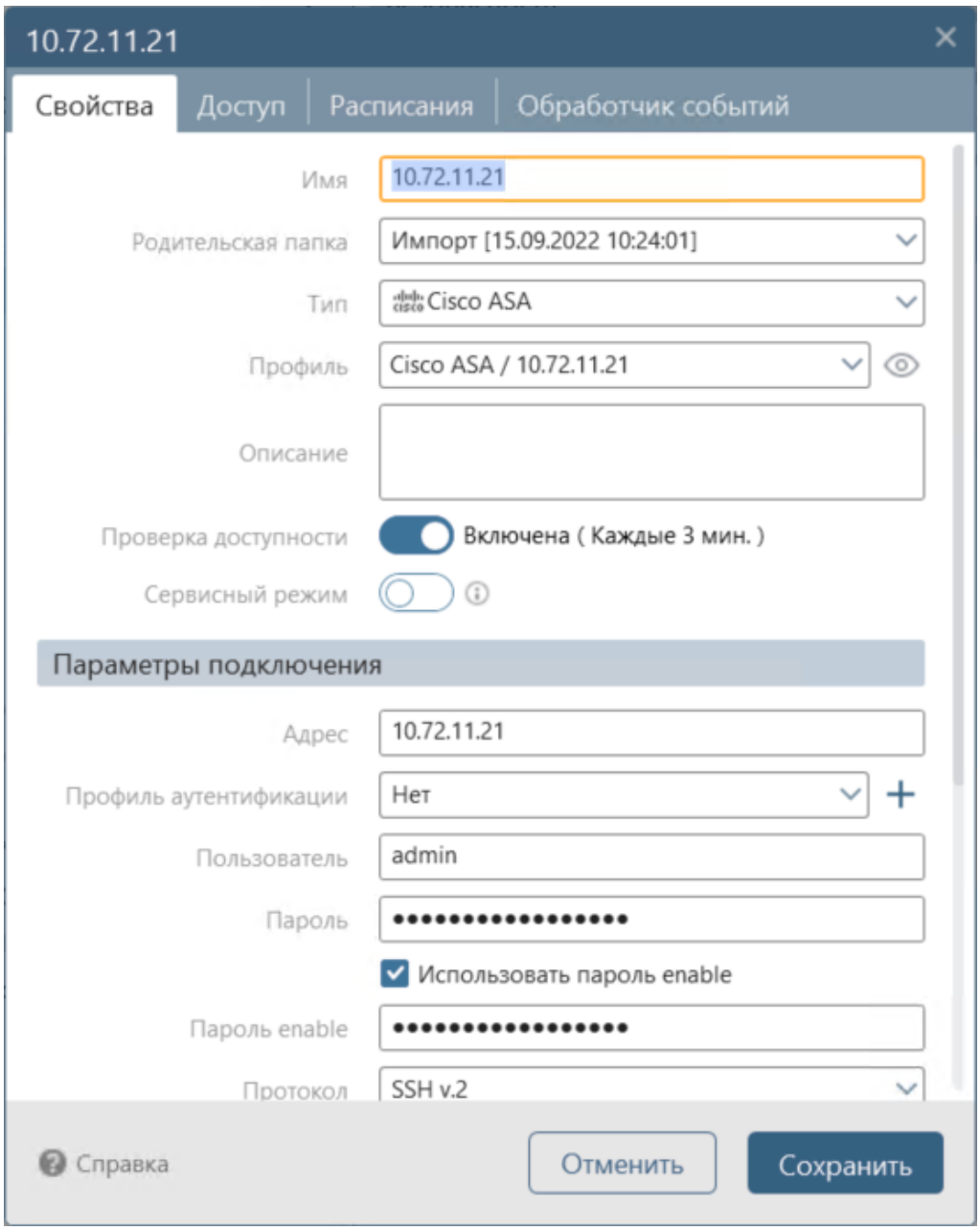


Рисунок 73 – Окно свойств устройства

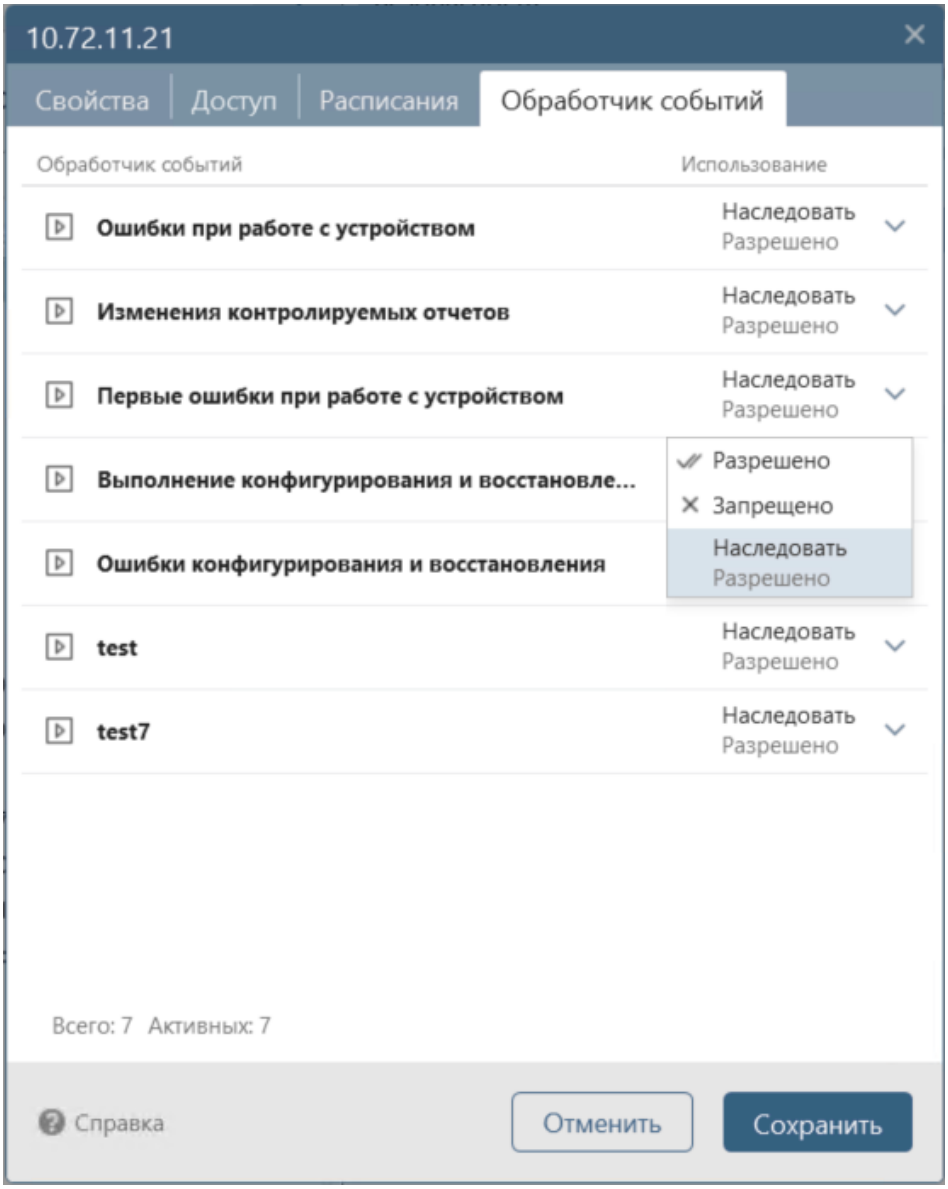


Рисунок 74 – Вкладка ***Обработчик событий***

Таблица 21 – 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 базового профиля; – *Запрещено* – запретить выполнение триггера вне зависимости от настроек базового профиля; – *Наследовать (XXXX)* – применить настройки базового профиля, используемого устройством. В скобках отображается значение, установленное для триггера в базовом профиле

2.7.4. Настройка режима использования расписаний для устройств

Изменять настройки режима использования расписаний загрузки отчетов и проверок устройств могут только пользователи с правами *Управление* в категории *Настройки контроля*.

Настройка использования расписаний может быть выполнена как в списке расписаний формы *Расписания* (см. п. 2.9.5 «Настройка использования расписаний») для всех устройств (групп) сервера ПК, так и в списке устройств раздела ***Устройства*** для каждого устройства (группы) отдельно.

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. 75).

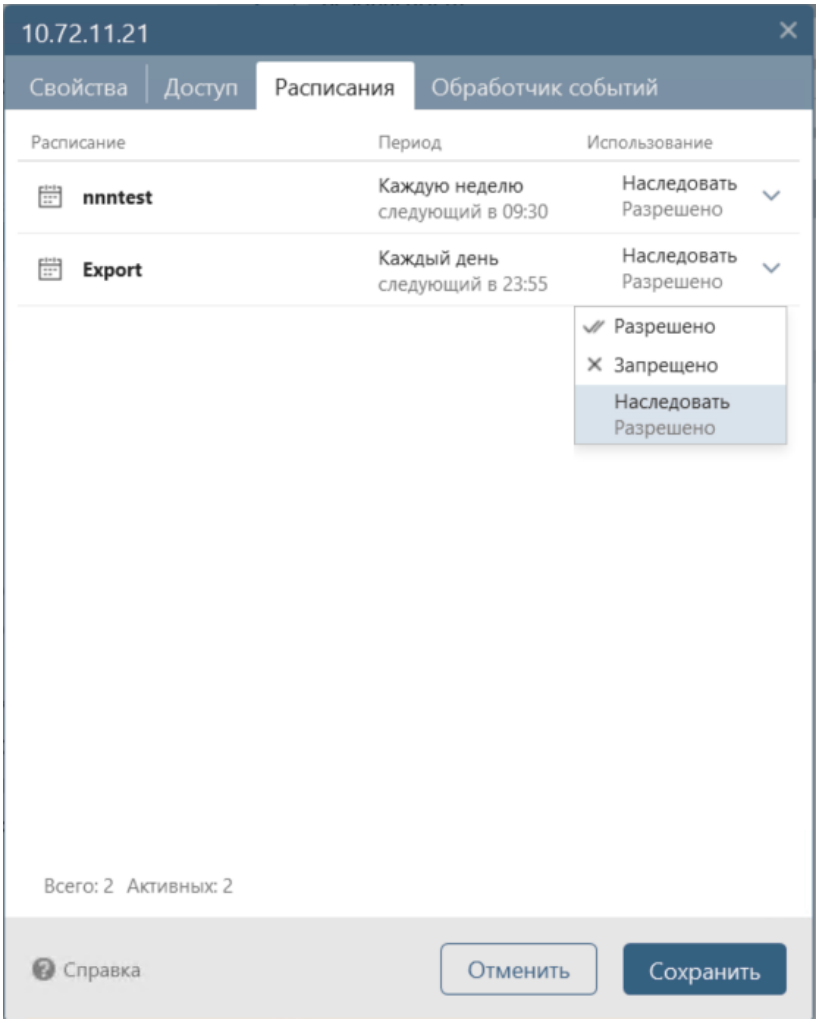


Рисунок 75 – Вкладка ***Расписания***

5) Выбрать необходимое расписание и из перечня значений раскрывающегося списка поля ***Использование*** установить требуемое значение варианта использования расписания для выбранного устройства (см. рис. 75, состав и описание значений полей окна приведено в таблице запуска расписания можно настроить в окне **Свойства** расписания, открываемого в форме настроек расписаний в разделе **Настройки** при нажатии кнопки ***Свойства*** для выбранного расписания (см. п. 2.9 «Настройка расписаний»).

6) Таблица 22).

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

Периодичность запуска расписания можно настроить в окне **Свойства** расписания, открываемого в форме настроек расписаний в разделе **Настройки** при нажатии кнопки ***Свойства*** для выбранного расписания (см. п. 2.9 «Настройка расписаний»).

Таблица 22 – 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. Настройка проверок безопасности

В ПК «Efros Config Inspector» v.4 реализована возможность формирования пользовательских стандартов проверок безопасности, на основании базы проверок CIS, существующих пользовательских проверок (включая проверки с помощью регулярных выражений[3]), а также путем копирования и последующего редактирования проверок. Для стандартов реализован механизм редактирования исключений, что позволяет создавать новые пользовательские стандарты в комбинации с существующими стандартами, или с использованием пользовательских настроек. Реализована данная опция в клиентской консоли, раздел **Настройки,** вкладка ***Проверки безопасности***.

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

Добавлять на сервер ПК, удалять с сервера ПК и изменять параметры проверок устройств могут только пользователи с правами *Управление* в категории *Настройки контроля*.

2.8.1. Просмотр списка проверок безопасности

Для просмотра списка проверок безопасности необходимо перейти в раздел **Настройки**, для чего в консоли нажать соответствующую кнопку на панели выбора раздела, выбрать сервер, список проверок безопасности которого просматривается (нажать кнопку ***Сервер*** и выбрать в открывшемся окне **Выбор сервера** строку требуемого сервера), и в панели ***Настройки контроля*** нажать ссылку ***Проверки безопасности***. Откроется форма управления проверками безопасности типов устройств, настройки стандартов, требований и исключений (рис. 76).

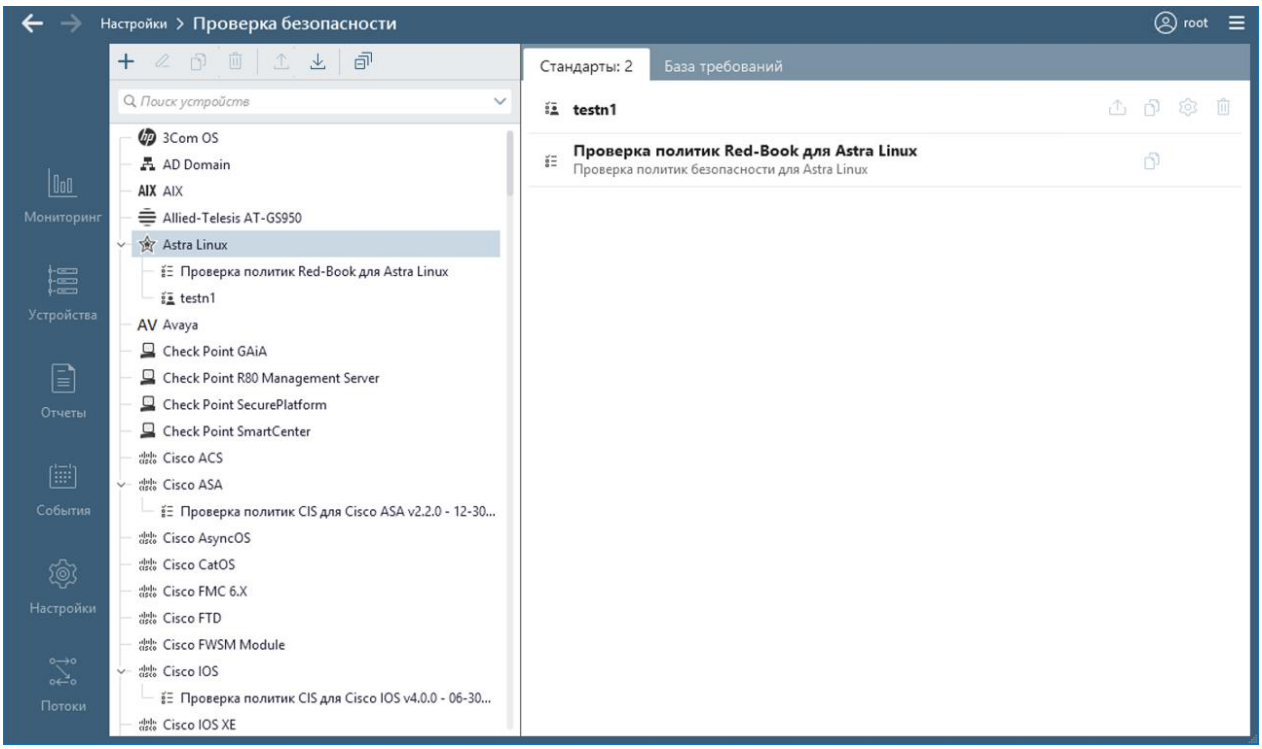


Рисунок 76 – Форма управления проверками безопасности типов устройств

Список стандартов формируется динамически при подключении к комплексу внешних модулей для работы с контролируемыми устройствами и сгруппирован по типам устройств (предустановленные стандарты). Также у пользователя с правами *Управление* в категории *Настройки контроля* есть возможность добавить в комплекс свои, пользовательские стандарты и требования (только при использовании *Premium* лицензии комплекса).

Подробное описание структуры автоматически добавленных в комплекс стандартов проверок и список входящих в эти стандарты требований приведены в файле справки *Описание модулей.zip* (*Описание модулей.chm*), расположенном на дистрибутивном диске программного комплекса.

Рабочая область формы управления проверками безопасности типов устройств разделена на:

- панель списка стандартов;

– панель настройки стандартов.

2.8.1.1. Панель списка стандартов

Панель списка стандартов содержит:

– кнопку ***Добавить стандарт*** (+) – активна всегда. Позволяет перейти к окну создания нового пользовательского стандарта (см. п. 2.8.2 «Добавление проверок безопасности»);
– кнопку ***Клонировать*** () – активна только при выборе стандарта. Служит для создания нового пользовательского стандарта на основе выбранного в списке стандарта (см. п. 2.8.2 «Добавление проверок безопасности»);
– кнопку ***Свойства*** () – активна только при выборе созданного пользователем стандарта. Служит для изменения имени и описания стандарта. (см. п. 2.8.3 «Изменение имени и описания пользовательского стандарта»);
– кнопку ***Удалить*** () – активна только при выборе созданного пользователем стандарта. Служит для удаления стандарта (см. п. 2.8.4 «Удаление пользовательского стандарта»);
– кнопку ***Экспорт*** () – активна только при выборе созданного пользователем стандарта. Предназначена для экспорта стандарта в файл формата XML;
– кнопку ***Импорт*** () – активна всегда. Предназначена для импорта стандарта из файла формата XML;
– кнопку ***Свернуть все*** () – активна всегда. Предназначена для сворачивания дерева стандартов до первого уровня – наименования типа устройств;
– поле поиска – для ввода символов из названия искомого устройства или стандарта;
– древовидный список стандартов, сгруппированный по типам устройств.

2.8.1.2. Панель настройки стандартов для типов устройств

Если в панели списка стандартов выделен **тип устройства**, то в рабочей области отображаются две вкладки (см. рис. 76):

1) Вкладка ***Стандарты*** содержит перечень стандартов проверок безопасности, для выделенного типа устройств.

Строка каждого стандарта проверок безопасности содержит кнопки для выполнения действий с выбранным стандартом (назначение кнопок приведено в таблице 23). Кнопки ***Экспорт***, ***Изменить*** и ***Удалить*** доступны только для пользовательских стандартов.

Таблица 23 – Перечень и назначение элементов управления вкладки ***Стандарты***

Кнопка	Внешний вид	Назначение
Экспорт		Предназначена для экспорта стандарта в файл формата XML

Кнопка	Внешний вид	Назначение
Клонировать		Предназначена для создания копии выбранного стандарта проверок безопасности для выбранного типа устройств. Открывает окно клонирования стандарта, включая все содержащиеся в нем требования, для создания на его основе пользовательского стандарта. После нажатия кнопки **Сохранить** в окне клонирования стандарта, в панели списка стандартов будет создана копия стандарта проверки безопасности для выбранного типа устройств
Изменить		Предназначена для изменения имени и описания стандарта проверки безопасности
Удалить		Открывает окно подтверждения удаления, выделенного в текущий момент времени в списке стандарта. После нажатия в окне кнопки «Да», удаляется выделенный стандарт

2) Вкладка ***База требований*** содержит перечень требований (разделены по категориям) применимых к данному типу устройства (рис. 77).

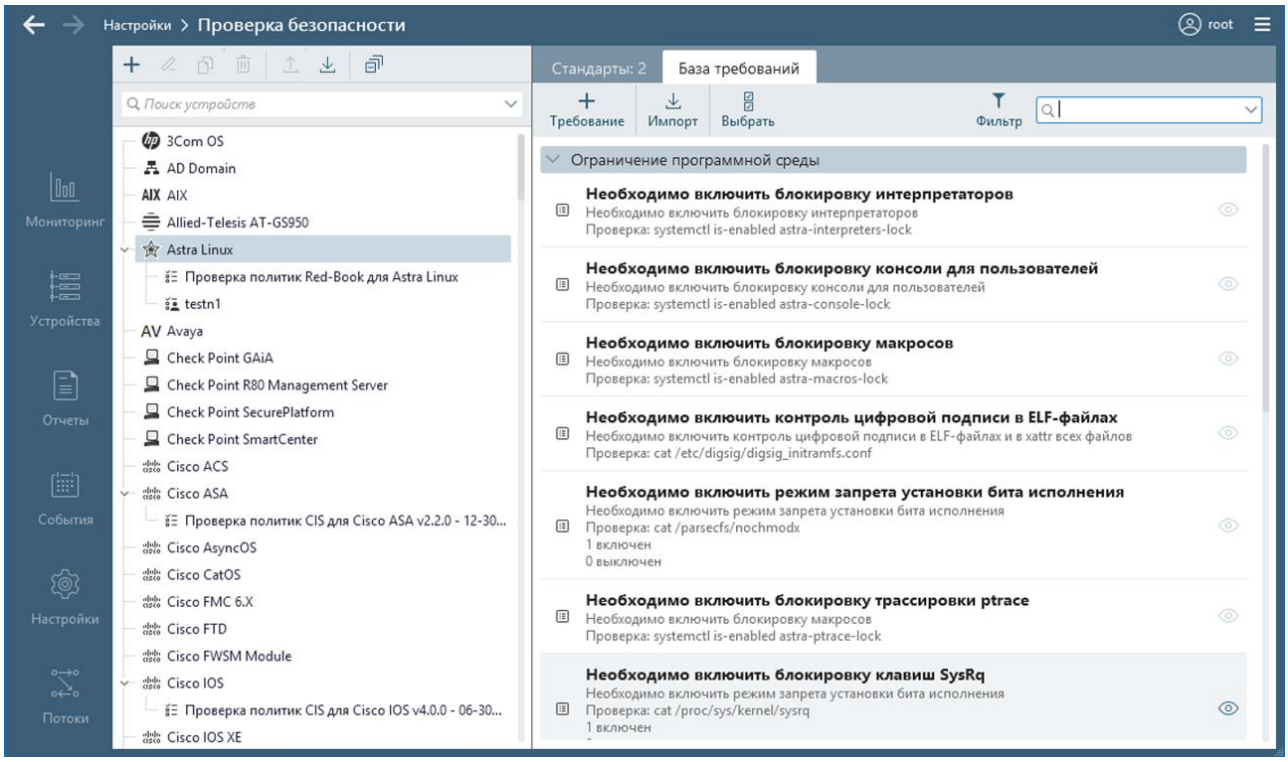


Рисунок 77 – Вкладка ***База требований***

Заголовок вкладки содержит поле поиска для ввода символов из названия искомого требования и кнопки:

- ***Требование*** (+) – открывает окно **Новое требование** для формирования нового требования (см. п. 2.8.2.1 «Создание и добавление требований проверок»);
- ***Импорт*** (⬇) – для импорта требований пользовательского стандарта из файла формата XML (см. п. 2.8.2.3 «Экспорт и импорт стандартов и требований проверок»);

– ***Выбрать*** – для открытия формы выбора требований для их экспорта или удаления (см. п. 2.8.2.3 «Экспорт и импорт стандартов и требований проверок» и 2.8.2.4 «Удаление требований из пользовательского стандарта»);
– ***Фильтр*** – для раскрытия окна настройки фильтрации списка требований по типу (пользовательское, встроенное) и категории требования.

По нажатию в строке требования стандарта кнопки ***Просмотр*** (см. рис. 77) открывается окно для просмотра настроек выбранного требования (например, рис. 78).

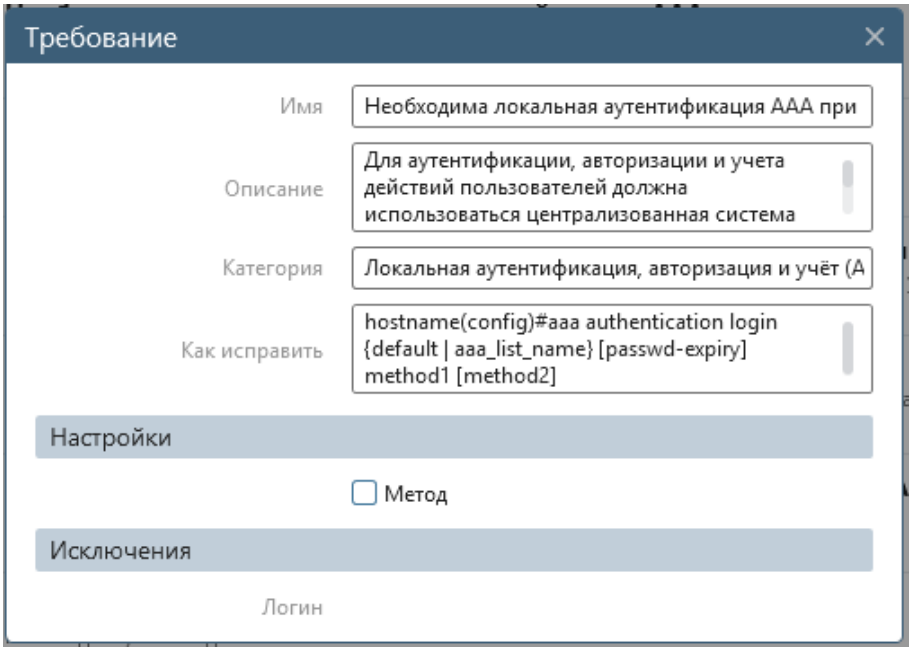


Рисунок 78 – Окно просмотра настроек требования

2.8.1.3. Панель настройки стандартов для стандартов проверок безопасности

Если в панели списка стандартов выделен ***предустановленный стандарт*** проверок безопасности, то в рабочей области отображается панель требований, разделенных на категории (рис. 79), в заголовке рабочей области отображается поле поиска для ввода символов из названия искомого требования и кнопки:

– ***Профили*** – для раскрытия окна **Профили** – окна настройки использования стандарта проверки для всех устройств, к которым он может быть применен;
– ***Фильтр*** – для раскрытия окна настройки фильтрации списка требований по типу (пользовательское, встроенное) и категории требования.

Примечание – При отсутствии для стандарта проверки безопасности требований, кнопка ***Профили*** неактивна, настройка использования стандарта проверки безопасности не доступна.

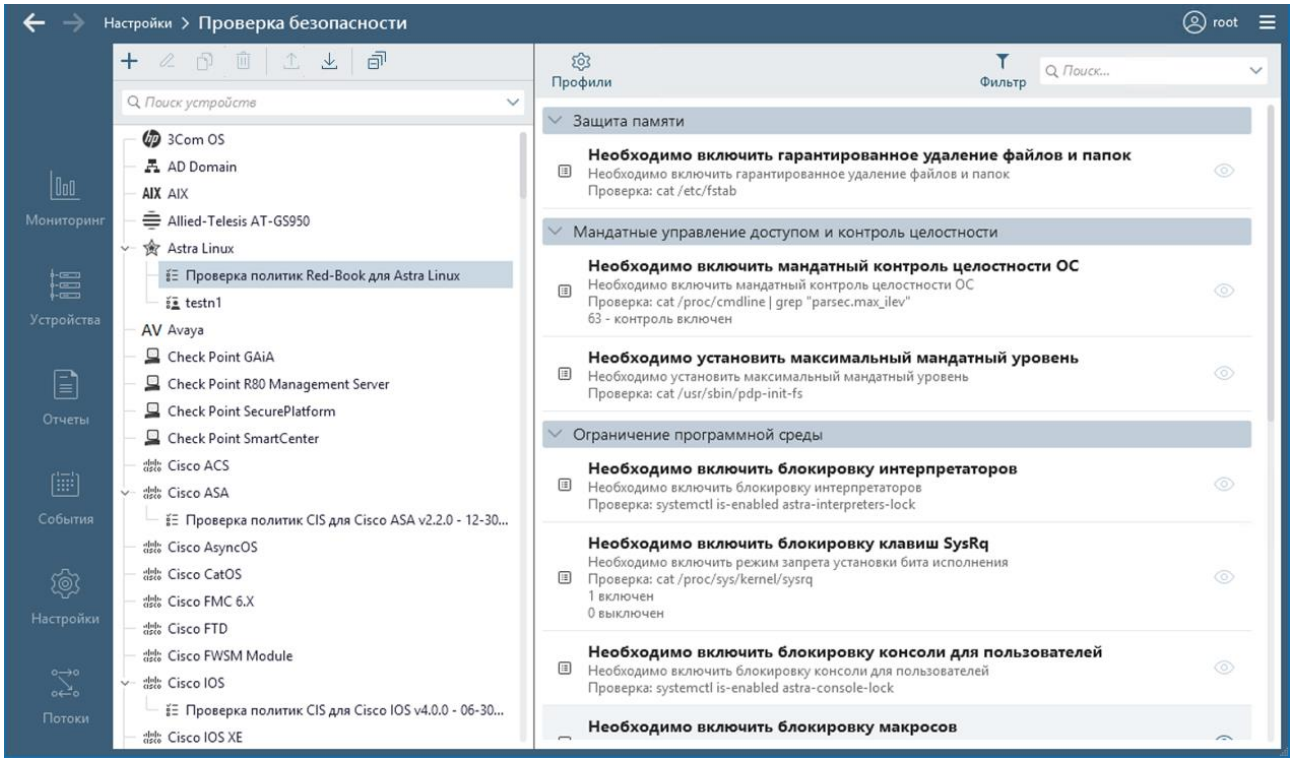


Рисунок 79 – Форма просмотра настроек требования выбранного стандарта (для предустановленного стандарта)

По нажатию в строке требования стандарта кнопки ***Просмотр*** (👁) (см. рис. 79) открывается окно для просмотра настроек выбранного требования (например, см. рис. 78).

Если в панели списка стандартов выделен ***пользовательский стандарт***, то в заголовке дополнительно отображаются кнопки:

- ***Требование*** (➕▾) – для добавления требования (только для пользовательских стандартов). Для создания нового требования в выпадающем меню кнопки необходимо выбрать пункт ***Новое требование***, для выбора требования из базы требований, применимых для данного вида устройств или требований, ранее созданных пользователем, выбрать пункт ***Выбрать*** (подробнее см. п. 2.8.2.1 «Создание и добавление требований проверок»);
- ***Выбрать*** (☑) – для перехода в окно выбора/удаления требований при редактировании стандартов. Выбор/удаление требований применимо только для пользовательских стандартов.

В строке пользовательского требования доступны кнопки:

- ***Изменить*** (⚙) – для перехода в окно редактирования параметров требования;
- ***Меню*** (⋯) – по нажатию кнопки открывается контекстное меню требования с пунктами:
  а) ***Клонировать*** – при выборе пункта меню открывается окно создания требования с параметрами выбранного требования;
  б) ***Удалить*** – для удаления требования.

2.8.2. Добавление проверок безопасности

Для добавления на сервер ПК новой (пользовательской) проверки необходимо выполнить следующие действия:

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

2) Выбрать сервер, для которого добавляется проверка безопасности.

3) В области *Настройки контроля* нажать кнопку ***Проверки безопасности***.

4) В открывшейся форме управления проверками безопасности устройств (см. рис. 76), настройки правил и исключений выделить нужный тип устройства в списке и нажать в панели списка стандартов кнопку ***Добавить новый стандарт*** ().

5) В открывшемся окне **Создание стандарта безопасности** (рис. 80, состав и описание полей окна приведены в таблице 24) заполнить необходимые поля и нажать кнопку ***Сохранить***.

6) Произойдет возврат в форму управления проверками устройств, настройки правил и исключений, а в списке стандартов указанного типа устройств появится созданный пользовательский стандарт.

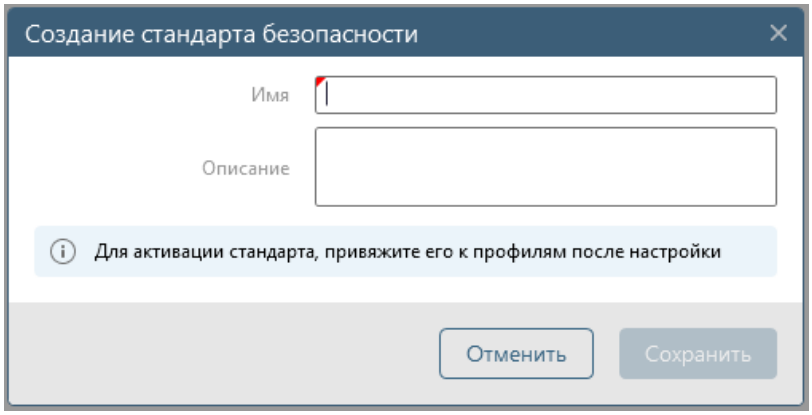


Рисунок 80 – Окно создания пользовательского стандарта безопасности

Таблица 24 – Состав и описание полей окна создания пользовательского стандарта безопасности

Поле	Описание/Назначение
Имя	Наименование создаваемого стандарта безопасности. Имя должно быть уникальным, т.е. не повторять имена уже существующих на сервере ПК стандартов безопасности данного типа. Поле обязательно к заполнению
Описание	Текстовое поле, в которое можно ввести понятное описание создаваемой проверки

Созданный стандарт проверки безопасности не содержит требований. Необходимо добавить требования в созданный стандарт (см. пункт 2.8.2.1 «Создание и добавление требований проверок») и, при необходимости, изменить параметры режима его использования на контролируемых на сервере ПК устройствах (см. пункт 2.8.5 «Настройка использования стандартов проверок безопасности»).

Создание пользовательского стандарта возможно с использованием других инструментов формы управления проверками безопасности типов устройств, настройки требований и исключений:

1) При нажатии кнопки ***Импорт*** () в панели списка стандартов откроется стандартное окно ОС для выбора файла (формата XML), содержащего импортируемые настройки и проверки пользовательского стандарта.

2) При нажатии кнопки ***Клонировать*** () в панели списка стандартов или во вкладке ***Стандарты*** формы управления проверками безопасности типов устройств (см. рис. 76) откроется окно создания копии выбранного соответственно в панели списка стандартов или во вкладке ***Стандарты*** стандарта безопасности (рис. 81). В окне необходимо внести изменения в имя и описание создаваемого стандарта и нажать кнопку ***Сохранить***.

Примечание – Имя стандарта должно быть обязательно изменено (не допускается наличие дубликатов стандартов проверок безопасности).

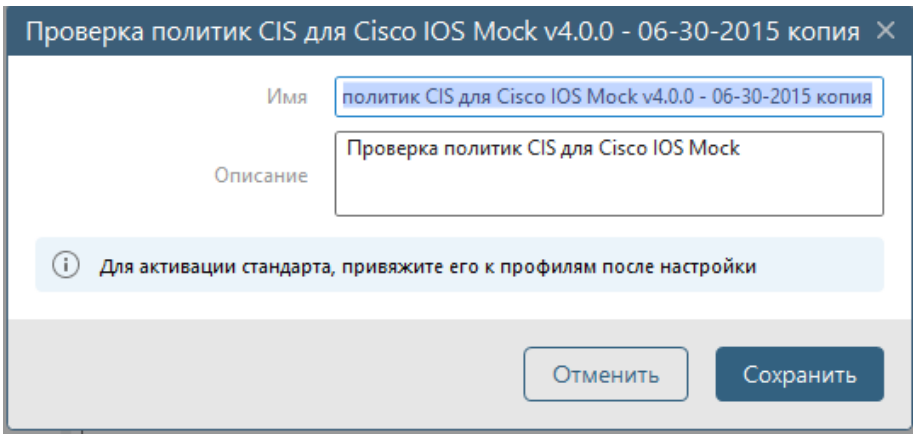


Рисунок 81 – Окно копирования стандарта проверок безопасности

Созданный путем клонирования стандарта пользовательский стандарт проверок безопасности будет содержать все требования исходного стандарта. После копирования можно отредактировать параметры созданного стандарта с использованием инструментов вкладки ***Стандарты*** (изменение имени и описания стандарта) и области настройки требований (изменение имени, описания, категории, добавление исключений для требований, входящих в созданный пользовательский стандарт).

Для активации созданного стандарта необходимо после добавления требований и их редактирования выполнить настройку использования пользовательского стандарта. Для этого необходимо:

1) В панели списка стандартов, выделить добавленный стандарт.

2) В заголовке открывшейся формы настройки пользовательского стандарта нажать кнопку ***Профили*** () .

3) В открывшемся окне настройки проверок выполнить настройку использования стандарта проверки для всех устройств, к которым он может быть применен. Для этого в области *Использование* в выпадающем списке выбрать значение ***Разрешено***.

2.8.2.1. Создание и добавление требований проверок

Правила проверок формируются требованиями, содержащимися в стандартах проверок безопасности. Добавление требований в стандарты возможно путем:

- создания новых пользовательских требований;
- копирования имеющихся в пользовательском стандарте требований (с их последующим редактированием);
- использования базы требований применимых для выбранного типа устройств;
- использования требований в существующих стандартах проверок безопасности для выбранного типа устройств.

Для создания нового пользовательского требования необходимо:

1) В форме управления проверками безопасности типов устройств, настройки правил и исключений, в панели списка стандартов выделить тип устройств, для которых создается пользовательский стандарт.
2) Перейти на вкладку ***База требований***.
3) Нажать в заголовке вкладки кнопку ***Требование*** (+). Откроется окно **Новое требование** (рис. 82).

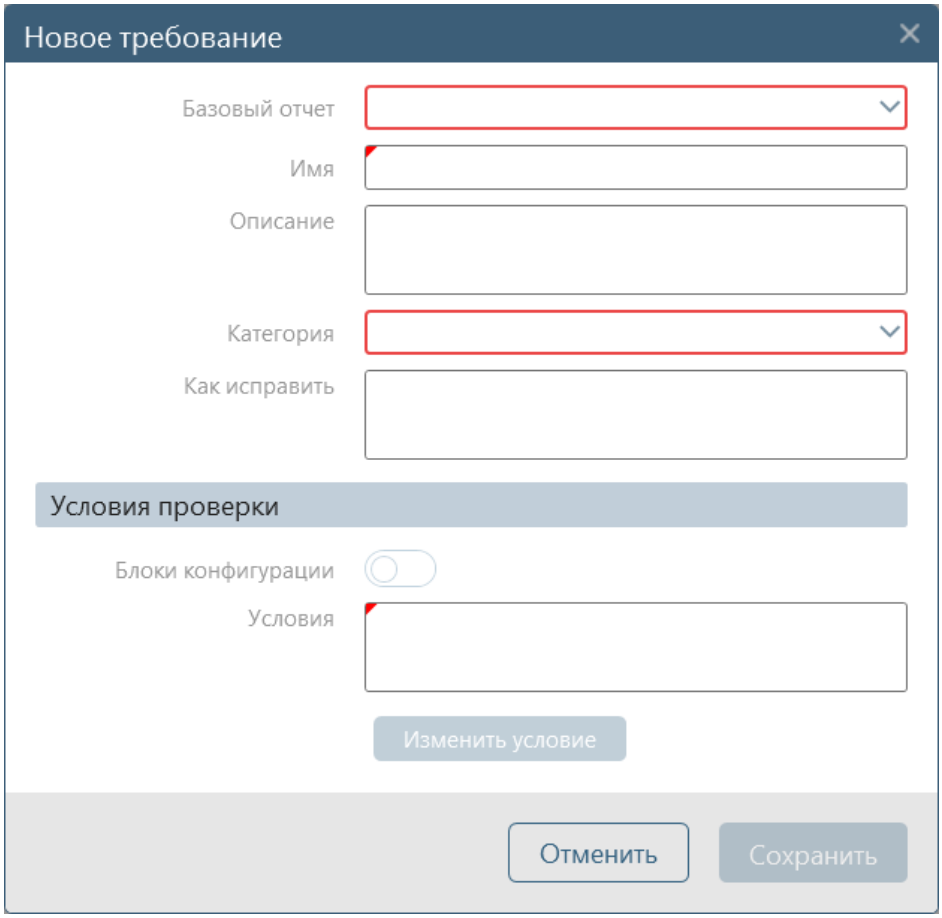


Рисунок 82 – Окно **Новое требование**

4) В открывшемся окне:

– в поле ***Базовый отчет*** выбрать из выпадающего списка наименование отчета, который будет использоваться при проверке параметров устройства. Поле обязательно к заполнению;
– в поле ***Имя*** ввести название создаваемого правила;
– при необходимости, в поле ***Описание*** ввести описание создаваемого требования;
– в поле ***Категория*** выбрать из выпадающего списка категорию требования. Пользователь может также сформулировать и ввести свою категорию. Поле обязательно к заполнению;
– заполнить, при необходимости, поле ***Как исправить***;
– в области ***Условия проверки*** добавить условия проверки, для чего:

а) нажать кнопку ***Изменить условие***. Откроется *окно* ***Редактор условий*** (рис. 83);

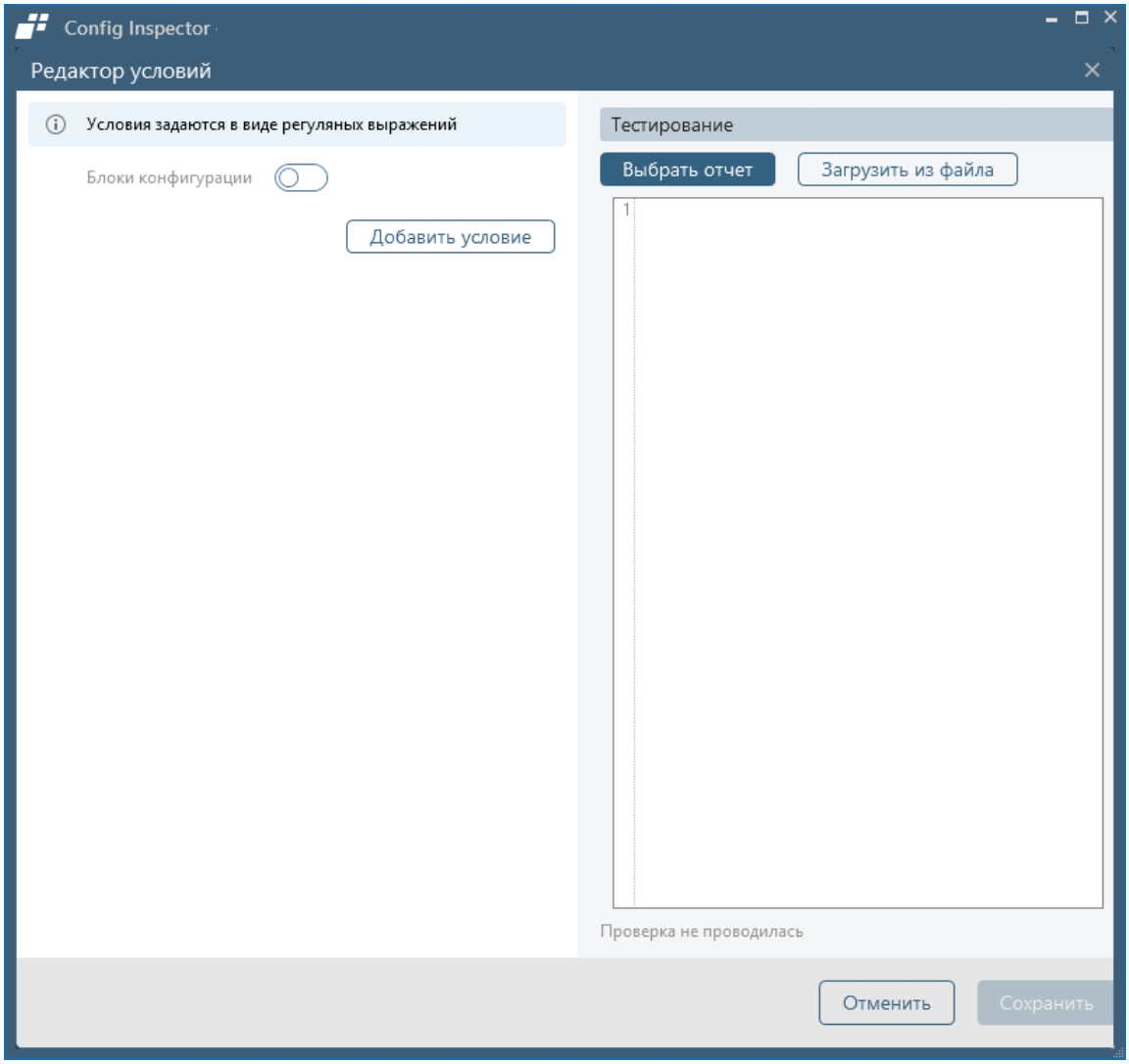


Рисунок 83 – Окно **Редактор условий**

б) отметить параметр ***Блоки конфигурации*** и ввести в открывшиеся поля ввода значения начала и окончания блока (рис. 84), выбрать

необходимое значение выполнения заданных условий: ***На любом блоке*** или ***На всех блоках***;

в) нажать кнопку ***Добавить условие,*** в отобразившихся полях (см. рис. 84) выбрать тип условия: ***Содержит*** или ***Не содержит*** базовый отчет редактируемой проверки значение и ввести это значение условия выполнения правила;

г) при необходимости, нажав кнопку ***Добавить условие,*** добавить еще условия выполнения правила проверки, повторив действия предыдущего пункта. При добавлении новых условий появляется возможность задания дополнительного параметра условия выполнения проверки: ***И*** – проверка будет пройдена, если выполнены все указанные условия, ***ИЛИ*** – проверка будет пройдена, если выполнено любое из указанных условий. Заданные условия можно объединить, разъединить, для чего установить флаги в строках изменяемых условий и в открывшейся панели меню (см. рис. 84) выбрать требуемое действие, также условия можно клонировать и удалить, для чего установить флаг в строке изменяемого условия и в открывшейся панели меню (см. рис. 84) выбрать требуемое действие.

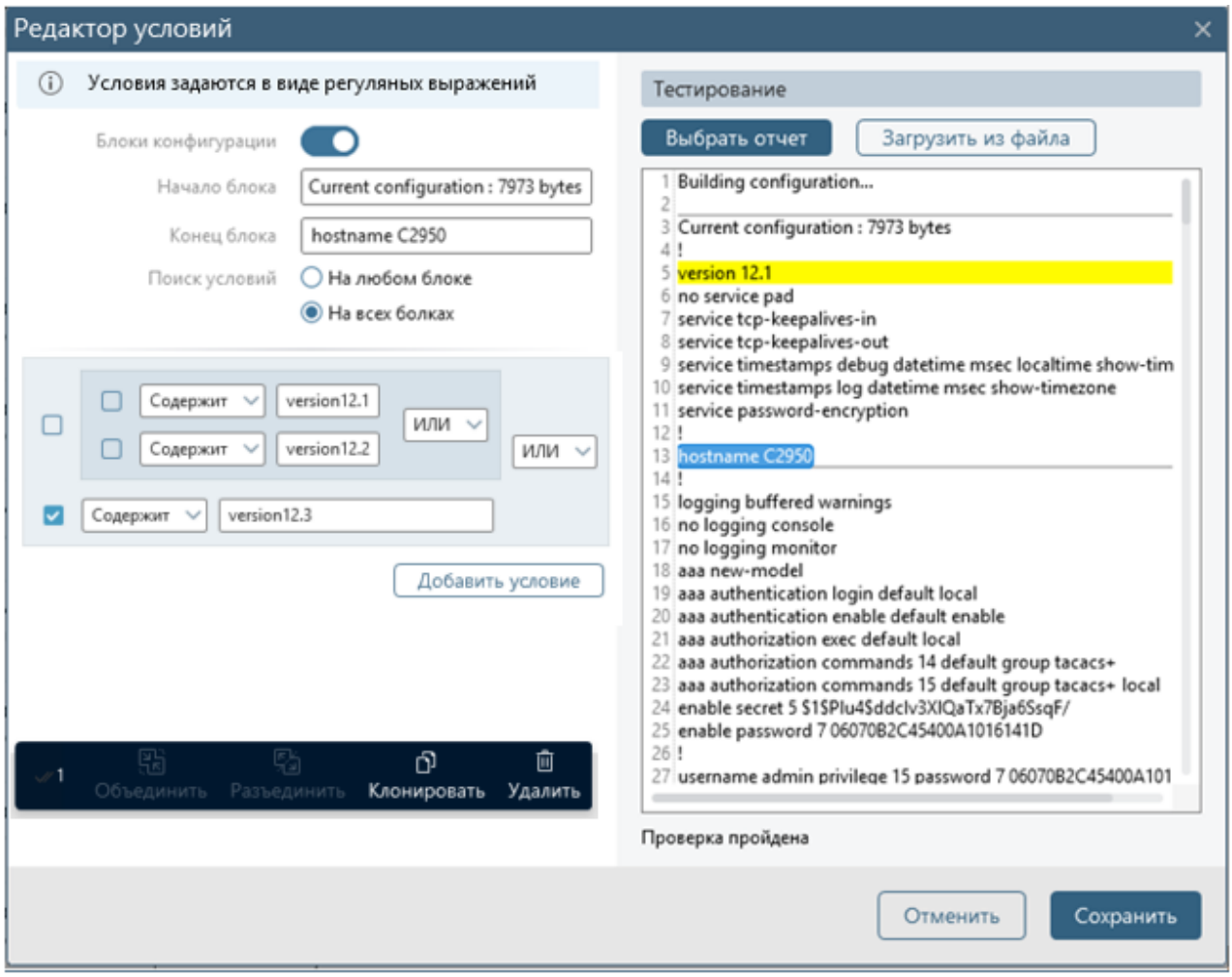


Рисунок 84 – Окно **Редактор условий** с результатами проверки выполнения

Примечание – Для проверки выполнения сформированного требования при его создании (редактировании) необходимо в окне **Редактор условий** загрузить в область ***Тестирование*** содержимое базового отчета проверки (с использованием кнопок ***Выбрать отчет*** или ***Загрузить из файла***) – в области *Тестирование* будет отображаться результат выполнения проверки (см. рис. 84).

- скорректировать, при необходимости заданные условия;
- нажать в окне **Редактор условий** кнопку ***Сохранить***;
- нажать в окне **Новое требование** кнопку ***Сохранить***.

Произойдет возврат в форму управления проверками безопасности типов устройств. На вкладке ***База требований*** появится новый шаблон требования.

При нажатии в окне **Новое требование** кнопки ***Отменить*** произойдет возврат на вкладку ***База требований*** в форму управления проверками устройств без добавления нового требования.

Для добавления требований в пользовательский стандарт с использованием базы требований или требований в существующих стандартах, применимых для выбранного типа устройств, или копированием необходимо выполнить следующие действия:

1) В панели списка стандартов выделить добавленный пользовательский стандарт проверки безопасности. В области настройки требований стандартов отобразятся содержащиеся в стандарте требования (рис. 85). Для пользовательских стандартов возможно редактирование состава требований стандарта и содержания требований (по кнопке ***Изменить*** ( ) в строке каждого требования).

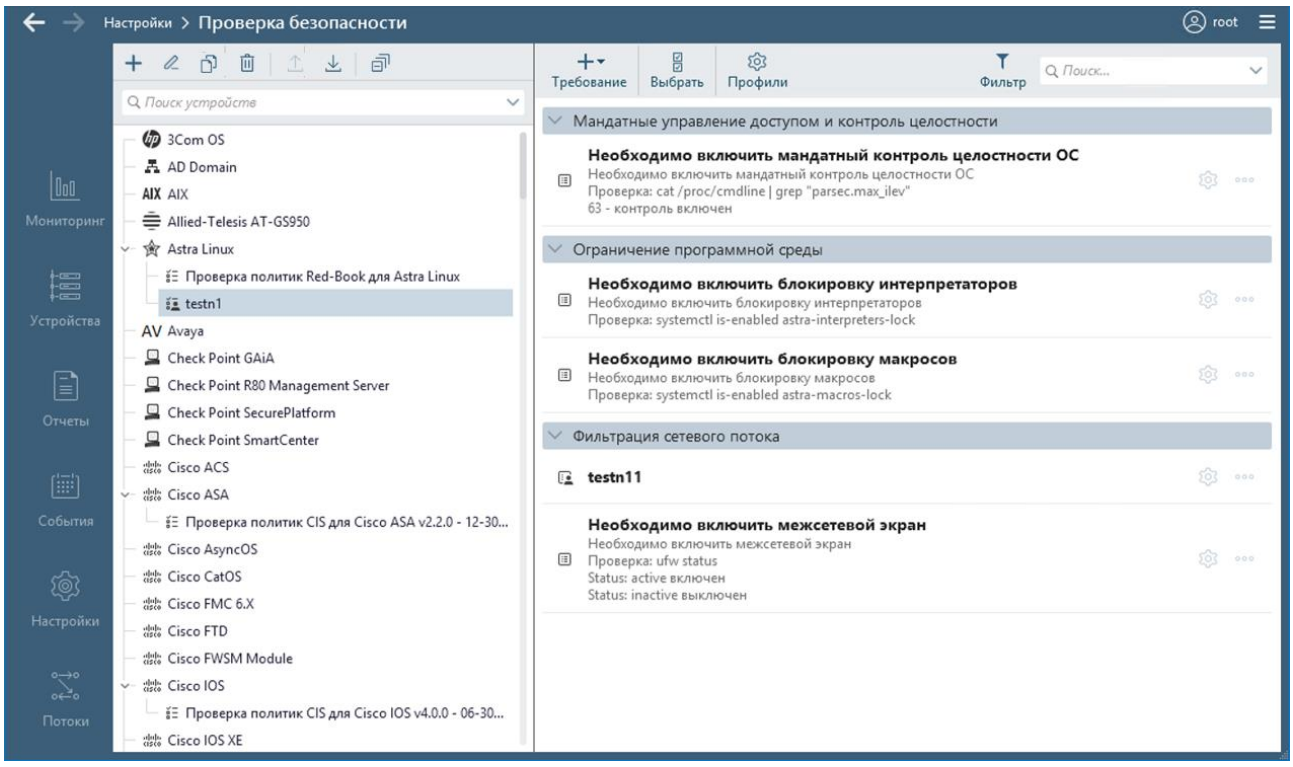


Рисунок 85 – Область настройки требований стандартов со списком требований пользовательского стандарта

2) Для добавления требований в создаваемый пользовательский стандарт, в области настройки параметров проверки нажать кнопку ***Требование*** (+▾) (см. рис. 85) и в раскрывшемся списке выбрать значение ***Выбрать*** или ***Создать новое***. Далее:

- для создания нового требования (выбрано значение ***Создать новое***) – выполнить действия по созданию нового требования в соответствии с п. 2.8.2.1 «Создание и добавление требований проверок»;
- для выбора требования из базы существующих требований (выбрано значение ***Выбрать***) в открывшемся окне **Требования** (рис. 86) выполнить следующие действия:
  а) в поле источника формирования требований выбрать значение ***База требований*** или ранее существующие для этого типа устройств стандарты проверок безопасности. В окне отобразится перечень требований, применимых к типу устройств, для которого создаётся стандарт, в соответствии с выбранным источником требований. Требования разделены на группы по их назначению;
  б) установить флаги в строках требований, включаемых в создаваемый стандарт проверки безопасности;
  в) нажать кнопку **Добавить**;
  г) произойдет возврат в форму управления проверками безопасности типов устройств. В области настройки требований стандартов отобразятся добавленные требования;
  д) для сохранения в пользовательском стандарте сделанных изменений нажать кнопку **Применить** в форме настройки пользовательского стандарта.

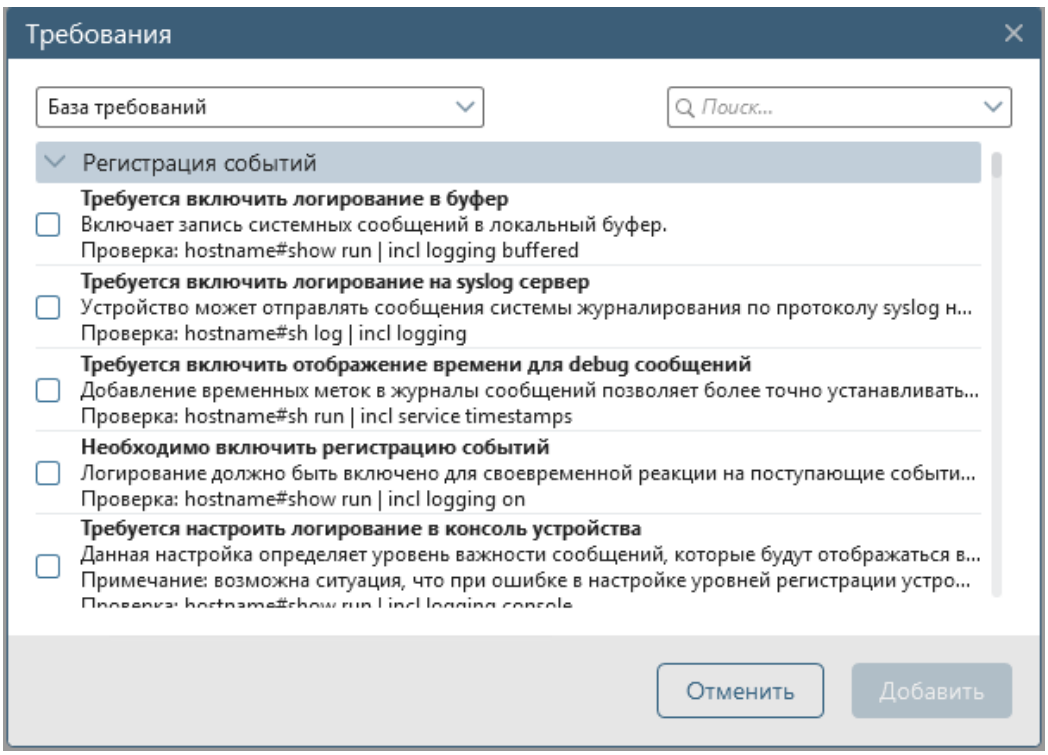


Рисунок 86 – Окно **Требования**

3) Для добавления требований в пользовательский стандарт путем копирования имеющегося требования – нажать в строке копируемого требования кнопку ***Меню*** (), нажать в раскрывшемся меню кнопку ***Клонировать*** (). Откроется окно **Новое требование**, поля которого будут заполнены данными исходного требования. Изменить название требования в поле ***Имя***, внести требуемые изменения в параметры требования и нажать кнопку ***Сохранить***. Для сохранения в пользовательском стандарте сделанных изменений нажать кнопку ***Применить*** в форме настройки пользовательского стандарта.

После добавления в пользовательский стандарт требований их можно отредактировать с использованием инструментов области настройки требований стандартов (см. п. 2.8.2.2 «Редактирование стандартов проверок»).

2.8.2.2. Редактирование стандартов проверок

Редактировать возможно только пользовательские стандарты. Редактирование предустановленных стандартов безопасности, загружаемых вместе с внешними модулями для типов устройств, невозможно.

Для редактирования пользовательских стандартов проверки безопасности необходимо выполнить следующий действия:

1) В панели списка стандартов выделить необходимый тип устройств.
2) В открывшейся вкладке ***Стандарты*** нажать в строке изменяемого стандарта кнопку ***Изменить*** () или дважды щелкнуть левой клавишей «мыши».
3) В открывшемся окне настройки стандарта (см. рис. 80) внести необходимые изменения в имя и описание стандарта и нажать кнопку ***Сохранить***.
4) Произойдет возврат в форму управления проверками безопасности типов устройств.

Для редактирования требований, добавленных в пользовательский стандарт, необходимо:

1) В панели списка стандартов выделить необходимый стандарт.
2) Выполнить настройку состава требований в выбранном стандарте, для чего:

– для удаления требования из стандарта – нажать в строке требования кнопку ***Меню*** () и выбрать в раскрывшемся меню пункт ***Удалить***. В результате откроется окно **Удаление**, в котором для подтверждения удаления нажать кнопку ***Удалить***. После нажатия кнопки ***Удалить*** выбранное требование будет удалено из стандарта проверки;
– для удаления нескольких требований – нажать в заголовке формы кнопку ***Выбрать*** ().Откроется форма для выбора и удаления группы требований (рис. 87). Выбрать установкой флагов удаляемые требования (для удаления всех требований – нажать в заголовке формы кнопку ***Выбрать все*** ()). Кнопка ***Удалить*** () в заголовке формы станет активной. Нажать кнопку ***Удалить*** (), откроется окно подтверждения удаления, в котором будут перечислены все удаляемые

требования. После подтверждения удаления выбранные требования будут удалены из стандарта проверки. Нажать кнопку ***Закрыть*** в форме выбора и удаления требований (см. рис. 87). Произойдет возврат в форму настроек требований стандартов проверки.

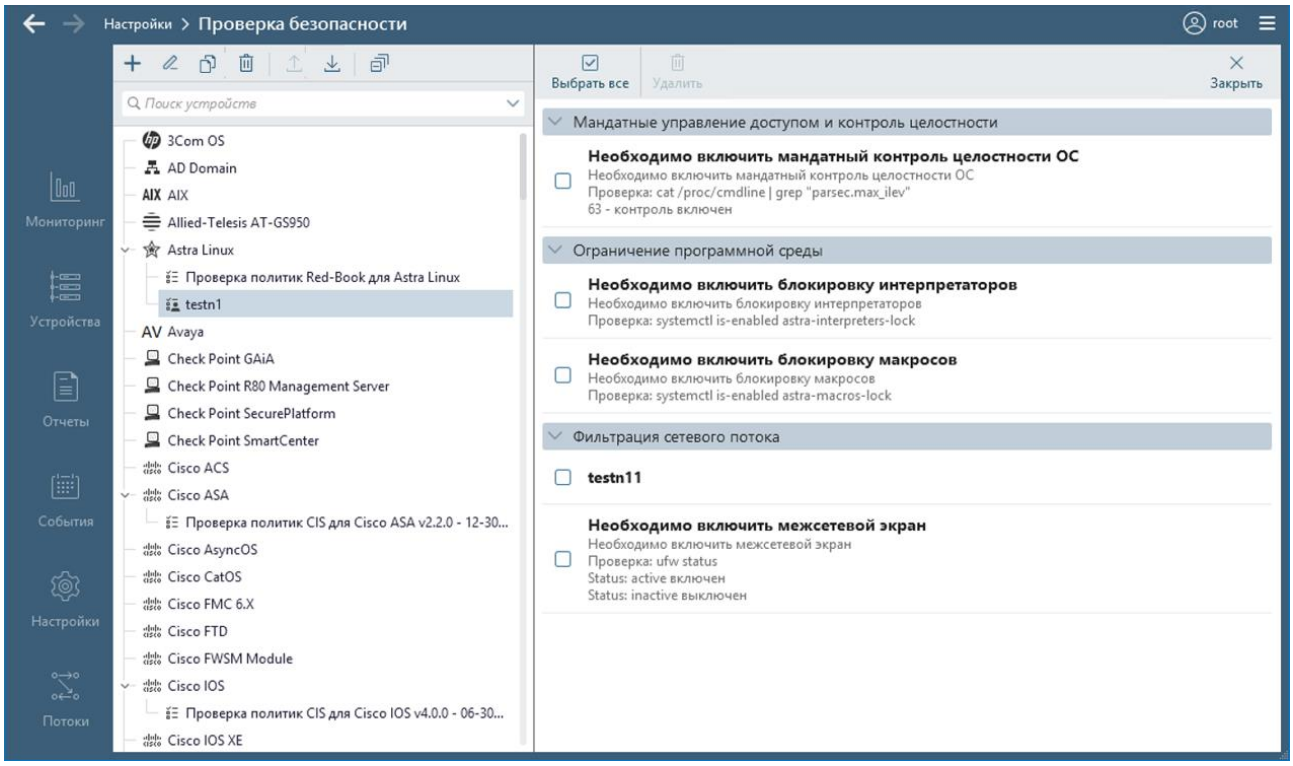
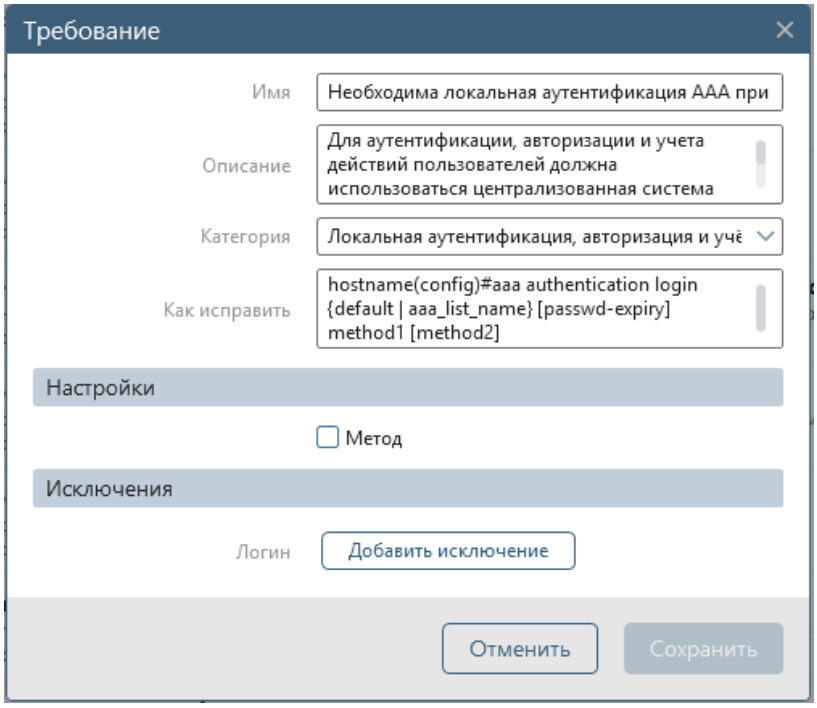
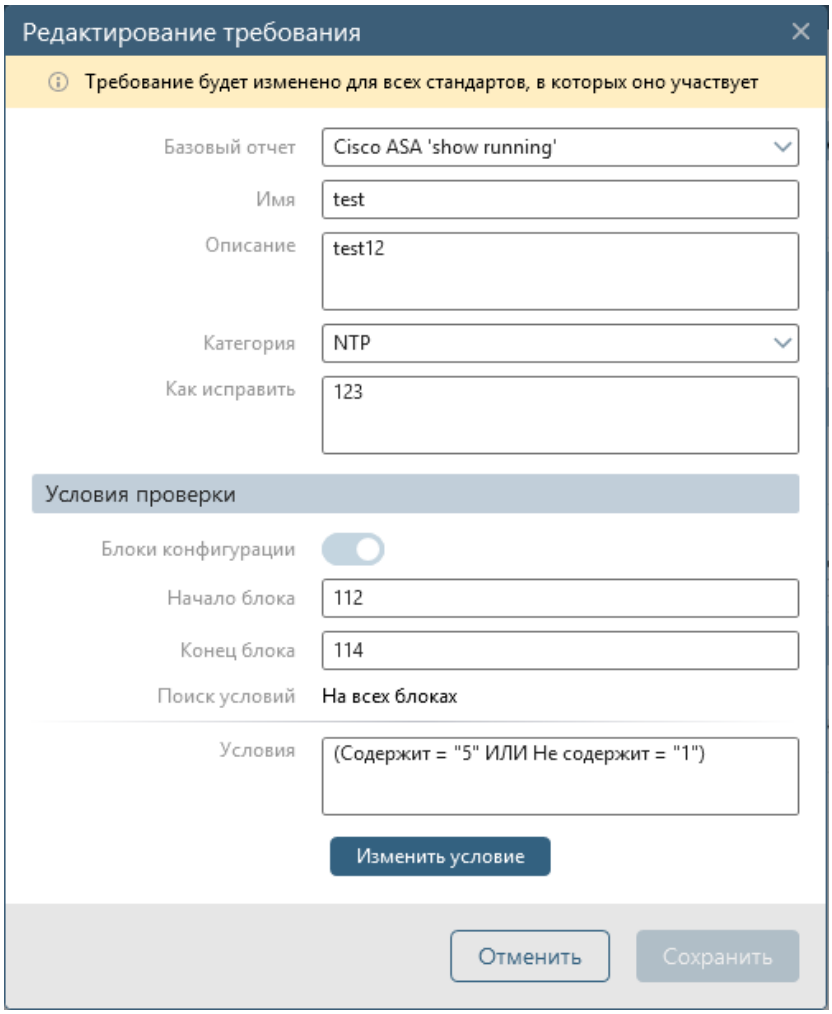


Рисунок 87 – Форма выбора и удаления требований

3) В форме настроек требований стандартов проверки для редактирования требования и добавления исключения – нажать кнопку ***Изменить*** () или дважды щелкнуть левой клавишей «мыши» в строке редактируемого требования. В результате откроется окно **Требование** (для требований, созданных на основе встроенных требований – рис. 88, а, для пользовательских требований – рис. 88, б) с настройками выбранного требования. Перечень настроек для каждого требования индивидуален.



а)



б)

Рисунок 88 – Окно **Требование**

2.8.2.3. Экспорт и импорт стандартов и требований проверок

Для экспорта пользовательского стандарта проверки в файл необходимо выполнить следующие действия:

1) В панели списка стандартов выделить необходимый пользовательский стандарт.

2) Нажать кнопку ***Экспорт*** ( ) в панели кнопок списка стандартов.

3) В открывшемся стандартном окне ОС Windows **Сохранить как** указать имя и каталог размещения файла, в котором будут сохранены настройки выбранных правил проверки, и нажать кнопку ***Сохранить***. Параметры отмеченных требований проверки (имя, статус, условия и пр.) будут сохранены в файле формата *.xml с заданным именем в указанном каталоге.

Возможен экспорт пользовательского стандарта проверки безопасности также путем выбора команды ***Экспорт*** в контекстном меню выбранного для экспорта пользовательского стандарта либо путем выбора кнопки ***Экспорт*** в строке экспортируемого стандарта (см. пример на рис. 89) в области настройки параметров пользовательского стандарта. Для этого в форме управления проверками безопасности для типов устройств, настройки требований и исключений предварительно необходимо выделить тип устройств для которого применим экспортируемый стандарт проверки безопасности.

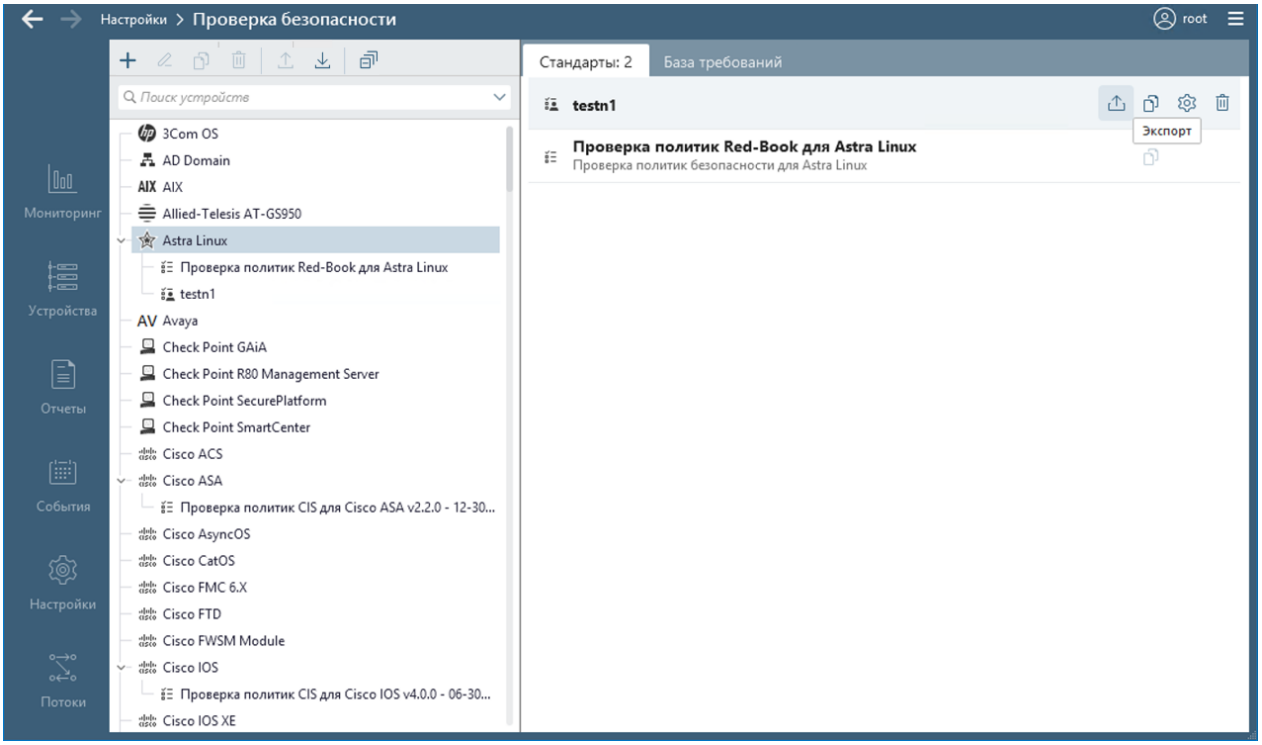


Рисунок 89 – Пример выбора стандарта проверки для экспорта

Для экспорта пользовательских требований проверки в файл необходимо выполнить следующие действия:

1) В панели списка стандартов выделить тип устройств.

2) В области настройки параметров пользовательского стандарта выбрать вкладку ***База требований.*** Нажать в заголовке вкладки кнопку ***Выбрать*** ( ).

3) Выбрать установкой флагов в появившемся списке пользовательских требований необходимые для экспорта, или нажать в заголовке вкладки кнопку ***Выбрать все*** (☑) для выбора всех требований.

4) Нажать в заголовке вкладки кнопку ***Экспорт*** (⬆).

5) В открывшемся стандартном окне ОС Windows **Сохранить как** указать имя и каталог размещения файла, в котором будут сохранены настройки выбранных правил проверки, и нажать кнопку ***Сохранить***.

Для импорта требований, сохраненных в файле, необходимо выполнить следующие действия:

1) В панели списка стандартов выделить необходимый тип устройств.

2) В области настройки параметров стандартов выбрать вкладку ***База требований*** и нажать в заголовке вкладки кнопку ***Импорт*** (⬇).

3) В открывшемся стандартном окне ОС Windows **Открыть** указать файл xml-формата, содержащий настройки импортируемого правила, и нажать кнопку ***Открыть***. В области настройки параметров появятся новые требования проверки для стандартов проверки безопасности, применимые к выбранному типу устройств.

В дальнейшем импортированные требования можно отредактировать (подробнее см. п. 2.8.2.2 «Редактирование стандартов проверок»).

Для импорта пользовательского стандарта проверки, сохраненного в файле, необходимо выполнить следующие действия:

1) В панели списка стандартов выделить необходимый тип устройств.

2) В меню панели списка стандартов нажать кнопку ***Импорт*** (⬇).

3) В открывшемся стандартном окне ОС Windows **Открыть** указать файл xml-формата, содержащий настройки импортируемого правила, и нажать кнопку ***Открыть***. В панели списка стандартов, в перечне стандартов для редактируемого типа устройств, появится новый стандарт проверки для выбранного типа устройств.

В дальнейшем импортированный стандарт можно отредактировать (подробнее см. п. 2.8.2.2 «Редактирование стандартов проверок»).

Примечание – При наличии в списке дубликата требования или стандарта проверки откроется окно подтверждения импорта с сообщением о перезаписи требования/стандарта. Импорт будет выполнен в таком случае только после подтверждения действия пользователем.

2.8.2.4. Удаление требований из пользовательского стандарта

Для удаления существующих требований из пользовательского стандарта необходимо выполнить следующие действия:

1) В панели списка стандартов выделить необходимый пользовательский стандарт.

2) В строке удаляемого требования нажать кнопку ***Меню*** (⋯) и выбрать в раскрывшемся меню пункт ***Удалить***.

Примечание – Для удаления группы требований – нажать в заголовке вкладки кнопку ***Выбрать*** (☑). В открывшемся окне выбора требований отметить установкой флагов

удаляемые требования (или нажать в заголовке окна кнопку меню ***Выбрать все*** ( )) и нажать в заголовке окна кнопку ***Удалить*** ( ).

3) Подтвердить операцию удаления правила из пользовательской проверки, нажав кнопку ***Удалить*** в открывшемся окне **Удаление.**

4) Произойдет возврат в форму управления проверками безопасности для типов устройств, требование будет отсутствовать в списке.

2.8.3. Изменение имени и описания пользовательского стандарта

На сервере ПК можно изменять только пользовательские стандарты проверок безопасности.

Для изменения параметров пользовательской проверки необходимо выполнить следующие действия в клиентской консоли:

1) Перейти в раздел **Настройки**.

2) Выбрать сервер, для которого изменяется проверка безопасности.

3) В области *Настройки контроля* нажать кнопку ***Проверки безопасности***.

4) В панели списка стандартов выделить необходимый стандарт и нажать в панели кнопок списка кнопку ***Свойства*** ( ) или выбрать пункт ***Изменить*** в контекстном меню выбранной проверки.

5) В открывшемся окне свойств проверки (рис. 90) изменить необходимые параметры и нажать кнопку ***Сохранить***.

6) Произойдет возврат в форму управления проверками устройств, настройки правил и исключений, в которой отобразятся внесенные в проверку изменения.

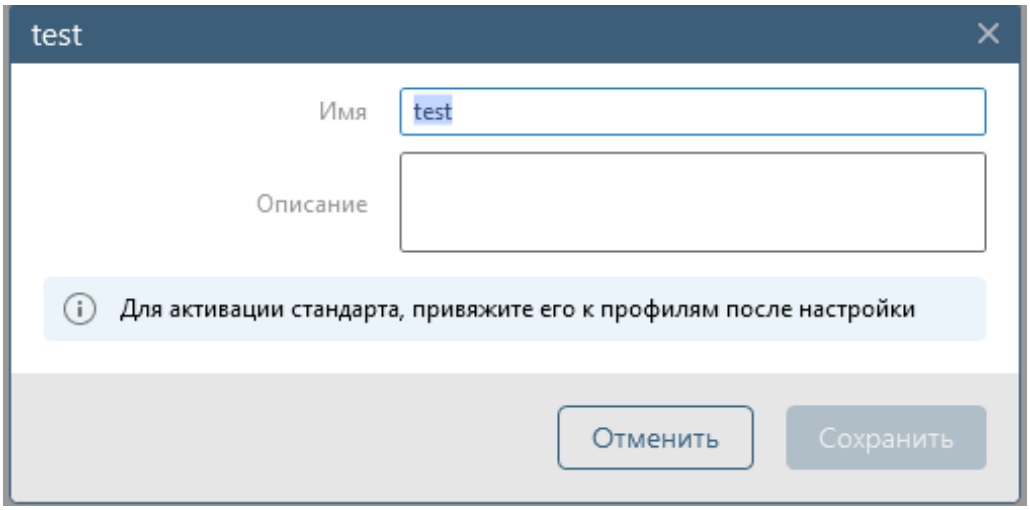


Рисунок 90 – Окно изменения параметров пользовательского стандарта

2.8.4. Удаление пользовательского стандарта

С сервера ПК можно удалять только пользовательские стандарты.

Для удаления пользовательского стандарта необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**.

2) Выбрать сервер, для которого удаляется проверка безопасности.

3) В области *Настройки контроля* нажать кнопку ***Проверка безопасности***.

4) В открывшейся форме управления проверками безопасности для типов устройств, настройки требований и исключений выделить необходимый стандарт и нажать кнопку ***Удалить*** () в панели кнопок списка стандартов или выбрать пункт ***Удалить*** в контекстном меню удаляемого стандарта.

5) Подтвердить операцию удаления проверки с сервера ПК нажав кнопку ***Удалить*** в открывшемся окне **Удаление.**

6) Произойдет возврат в форму управления проверками безопасности для типов устройств.

2.8.5. Настройка использования стандартов проверок безопасности

Настройка использования стандартов проверок безопасности может быть выполнена как в форме управления проверками безопасности для всех устройств сервера ПК, так и в списке профилей формы ***Профили*** (см. п. 2.8.6 «Настройка проверок для профилей»).

Для настройки использования стандарта проверок безопасности пользователю необходимо выполнить следующие действия:

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

2) Выбрать сервер, для которого настраивается проверка безопасности.

3) В области *Настройки контроля* нажать кнопку ***Проверки безопасности***.

4) В панели списка стандартов открывшейся формы управления проверками безопасности выделить необходимый стандарт.

5) В заголовке панели настройки стандартов нажать кнопку ***Профили*** () .

6) В открывшемся окне настройки проверок (рис. 91) выполнить настройку использования стандарта проверки для всех устройств, к которым он может быть применен. Для этого:

– в области ***Использование*** в выпадающем списке выбрать требуемое значение для соответствующих типов устройств и отдельных устройств. Возможные значения для типов устройств:
  а) *Разрешено* – разрешить проверку вне зависимости от настроек базового профиля;
  б) *Запрещено* – запретить проверку вне зависимости от настроек базового профиля.

  Возможные значения для устройств:
  а) *Разрешено* – разрешить проверку вне зависимости от настроек для типа устройств;
  б) *Запрещено* – запретить проверку вне зависимости от настроек для типа устройств;

в) *Наследовать (XXXXX)* – применить настройку, заданную для типа устройств. В скобках отображается значение, установленное для типа устройств: *Разрешено* или *Запрещено.*

– нажать кнопку ***Сохранить***. Окно настройки использования стандарта проверок закроется, внесенные изменения будут применены

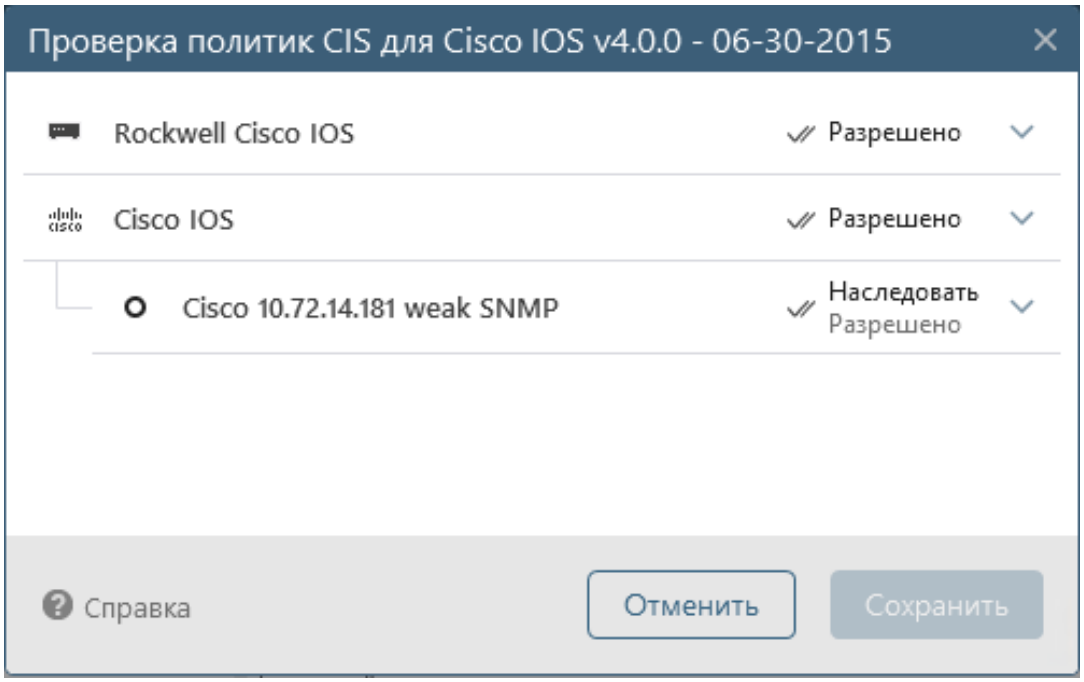


Рисунок 91 – Окно настройки использования стандарта проверок.

2.8.6. Настройка проверок для профилей

Для внесения изменений в настройки режима использования проверок устройств для базовых профилей (профилей автоматически добавленных на сервер ПК при подключении к нему внешних модулей) пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**.
2) Выбрать сервер, для которого настраивается проверка профиля.
3) В области *Настройки контроля* нажать кнопку ***Профили***.
4) В списке профилей формы ***Профили*** выделить необходимый профиль.
5) В рабочей области формы перейти на вкладку ***Проверки*** (рис. 92, состав и описание значений полей вкладки приведено в таблице 25).
6) В строке изменяемой проверки нажать кнопку ***Настройки правил*** (⚙).

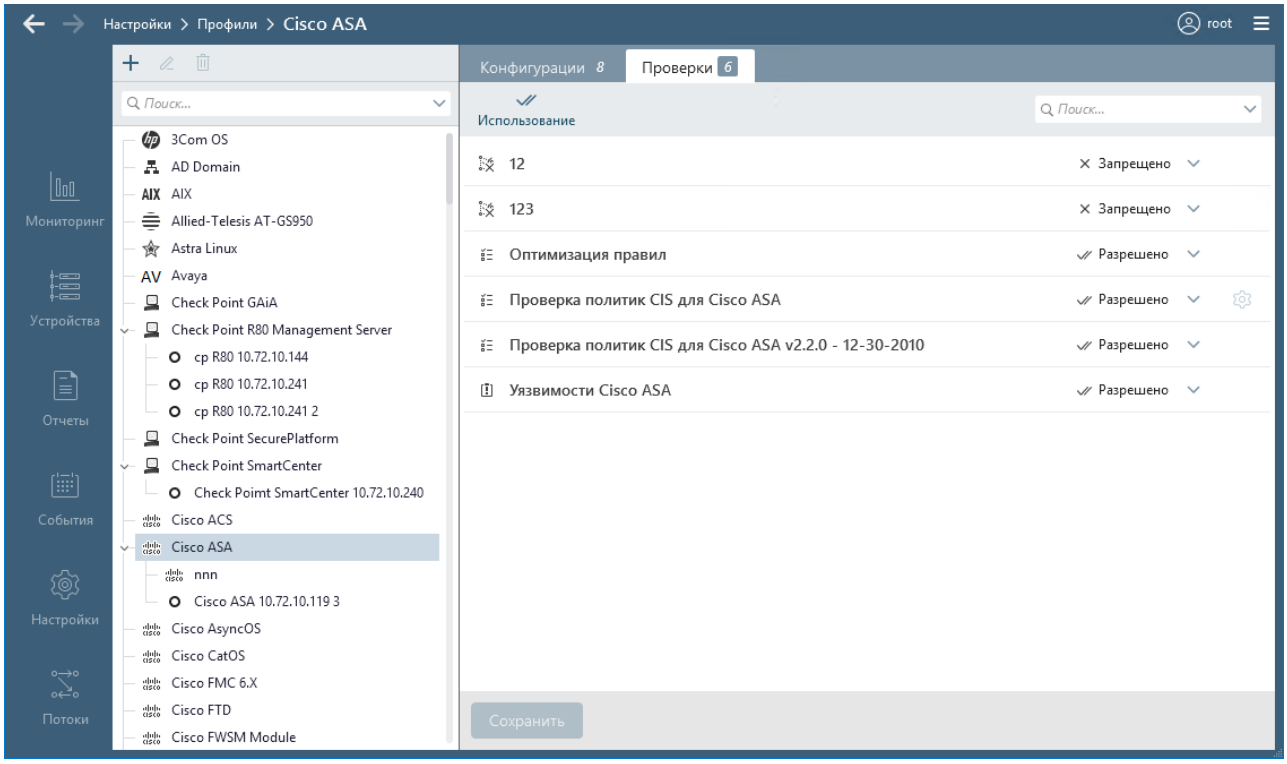


Рисунок 92 – Вкладка ***Проверки***

Таблица 25 – Состав и описание элементов окна настройки проверки устройств

Поле	Описание/Назначение
Проверки	Наименование проверки на сервере ПК
Использование	Выбор режима использования проверки. Возможные значения: – *Разрешено* – разрешить проверку вне зависимости от настроек базового профиля; – *Запрещено* – запретить проверку вне зависимости от настроек базового профиля.
Без названия	Содержит кнопку ***Настройки правил*** ⚙. Щелчок по кнопке открывает окно настроек правил соотвествующей проверки.

7) В открывшемся окне настройки правил выбранной проверки (рис. 93, состав и описание значений полей вкладки приведено в таблице 26):

- раскрыть список поля ***Использование*** для профиля требуемого типа устройства и установить необходимый вариант использования проверки устройств выбранного типа;
- изменить, при необходимости, режим выполнения для выбранных правил проверки, выбрав в поле ***Выполнение*** таблицы правил требуемое значение;
- изменить, при необходимости, настройки исключений для отдельных правил проверки;
- нажать кнопку ***Применить*** для сохранения внесенных изменений.

8) Нажать кнопку ***Сохранить*** в окне изменения проверки для сохранения внесенных изменений.

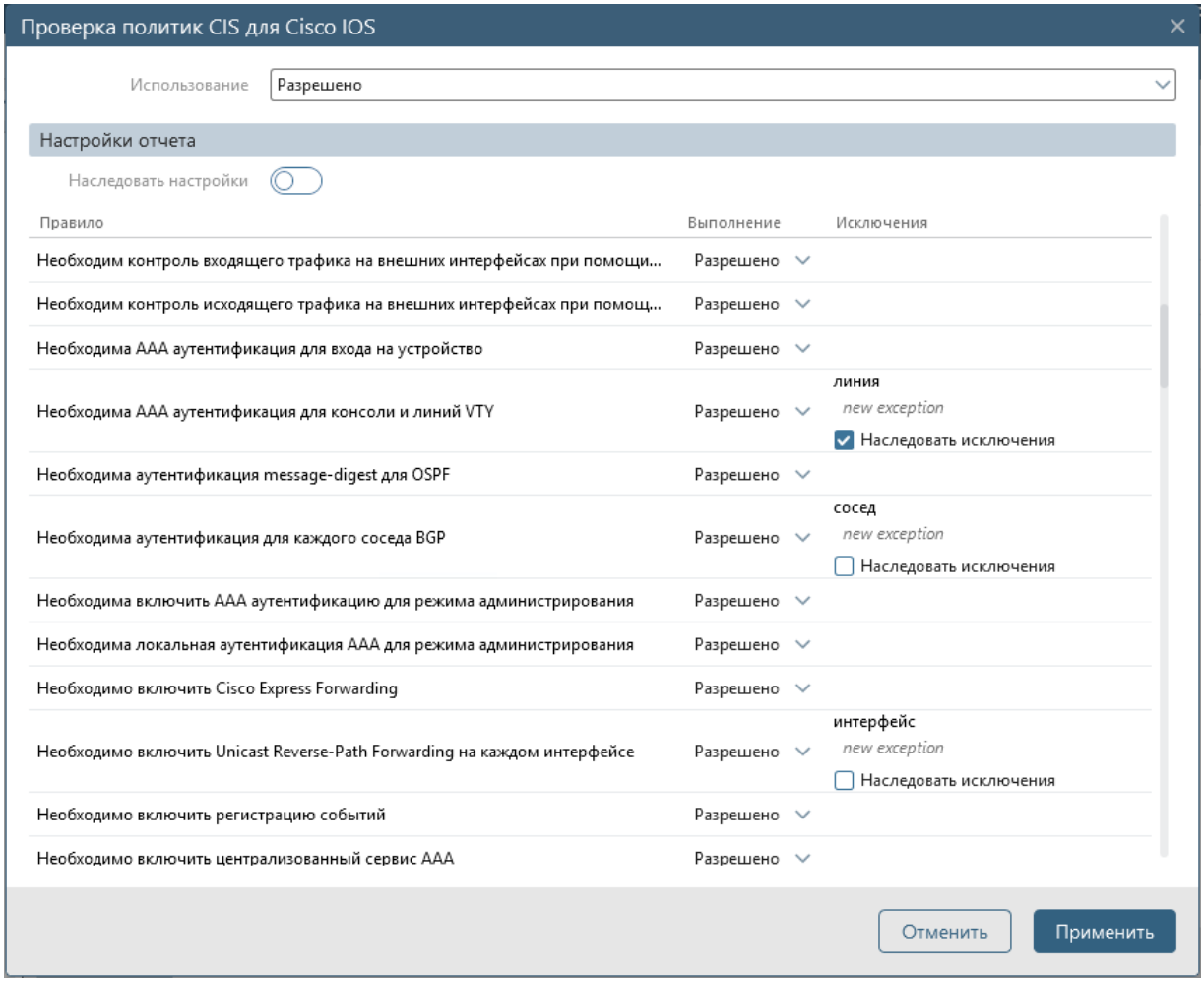


Рисунок 93 – Окно настройки правил проверки устройства

Таблица 26 – Состав и описание полей окна настройки правил выбранной проверки

Поле	Описание/Назначение
Использование	Выбор режима использования проверки. Возможные значения перечислены в таблице 25
Наследовать настройки	При включенном переключателе (●) настройки проверки не доступны для внесения изменений, при выключенном (○) – пользователь имеет возможность внесения изменений в настройки отдельных правил проверки
Правило	Перечень правил проверки
Выполнение	Содержит значения режима выполнения отдельных правил в составе проверки: – *Разрешено* – разрешить выполнение правила; – *Запрещено* – запретить выполнение правила
Исключения	Поле отображается и заполняется только для правил, в которых могут быть назначены исключения. При включенном переключателе ***Наследовать исключения*** содержит значения, установленные в родительском профиле и не доступно для редактирования. При выключенном переключателе – содержит список доступных для

Поле	Описание/Назначение
	настройки исключений при выполнении правила. Для ввода нового исключения необходимо ввести необходимое значение в строке ***новое значение*** и нажать клавишу клавиатуры **ENTER**

Действия по настройке проверок для остальных профилей комплекса совпадают с действиями по настройке проверок устройства для базовых профилей, описанными выше. Исключение составляет возможность наследования настроек использования и уровня критичности проверки из базового профиля – дополнительный параметр ***Наследовать (XXX)*** (где XXXX – настройка базового профиля *Разрешено* или *Запрещено*) раскрывающихся списках полей ***Использование*** и ***Выполнение.***

2.9. Настройка расписаний

2.9.1. Просмотр списка расписаний

Для просмотра списка расписаний необходимо:

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

2) Выбрать сервер, список расписаний которого просматривается, для чего нажать кнопку ***Сервер*** и выбрать в открывшемся окне **Выбор сервера** строку требуемого сервера.

3) Нажать в панели ***Настройки контроля*** ссылку ***Расписания***. Откроется форма настройки расписаний загрузки отчетов с устройств или экспорта отчетов и/или списка устройств в XML-файлы (список устройств или структурированные отчеты) или CFG-файлы (при экспорте текстовых отчетов) и обновления базы известных угроз и уязвимостей для установленных модулей (рис. 94).

Форма настройки расписаний содержит:

- кнопку ***Расписание*** (+) – для перехода в форму добавления расписания (см. п. 2.9.2 «Добавление расписания»);
- кнопку ***Фильтр*** (▼) – для перехода в окно фильтрации расписаний по их активности (выбор выполняется установкой флагов одном или обоих полях: *Активные*, *Отключенные*) и сброса настройки фильтра;
- поле поиска расписаний по их названию;
- список имеющихся расписаний (сразу после инсталляции серверной части и клиентской консоли комплекса в форме отображается расписание обновления базы уязвимостей, по умолчанию состояние ***Отключено***).

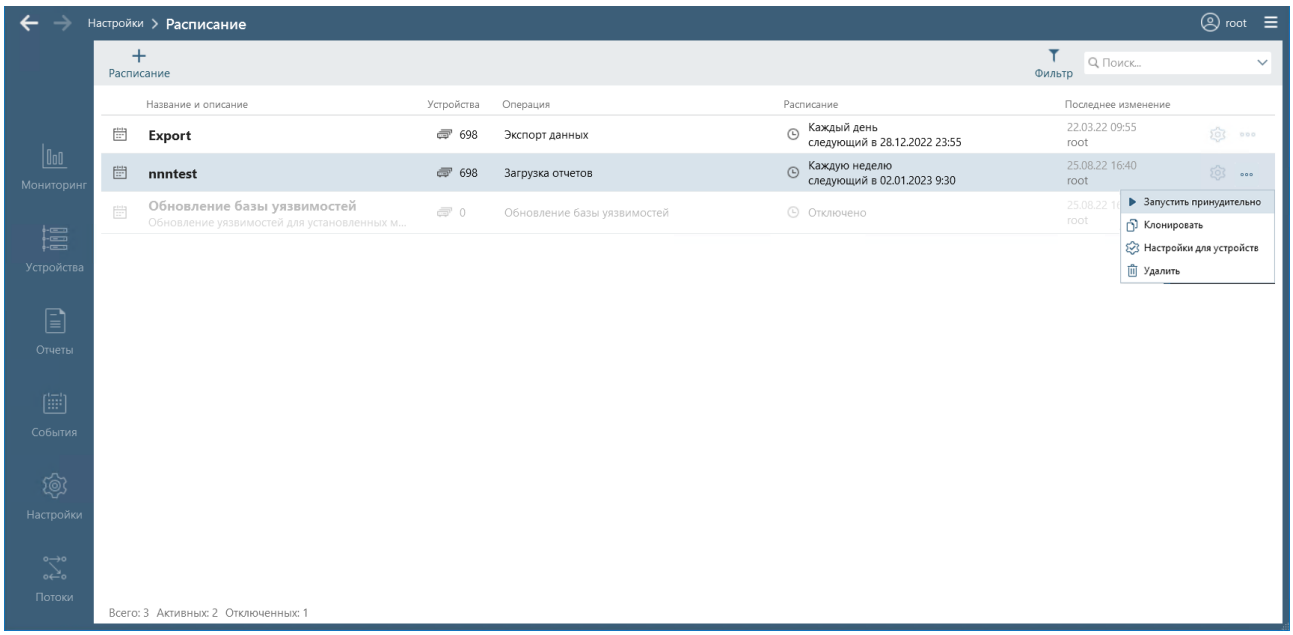


Рисунок 94 – Форма настройки расписаний

В нижней части формы приведены данные об общем количестве расписаний, количестве активных и отключенных на текущий момент времени расписаний.

Для каждого расписания в форме настройки расписаний загрузки отчетов с устройств отображаются данные:

- название и описание;
- количество устройств, для которых расписание применяется;
- выполняемое по расписанию действие (загрузка отчетов, обновление базы уязвимостей экспорт, экспорт устройств в csv или экспорт настроек
- периодичность выполнения расписания или, если расписание неактивно (редактируется только в окне настройки параметров расписания), текст ***Отключено***;
- дата и время внесения последнего изменения и логин внесшего изменение пользователя;
- кнопка ***Изменить*** () – для перехода в окно редактирования параметров расписания;
- кнопка ***Меню*** ( ) – по нажатию кнопки открывается контекстное меню расписания (см. рис. 94) с пунктами:
  а) ***Запустить принудительно*** – для принудительного запуска расписания вручную без отсрочки запуска;
  б) ***Клонировать*** – для клонирования расписания;
  в) ***Удалить*** – для удаления расписания;
  г) ***Настройки для устройств*** – для настройки списка устройств, для которых расписание применяется.

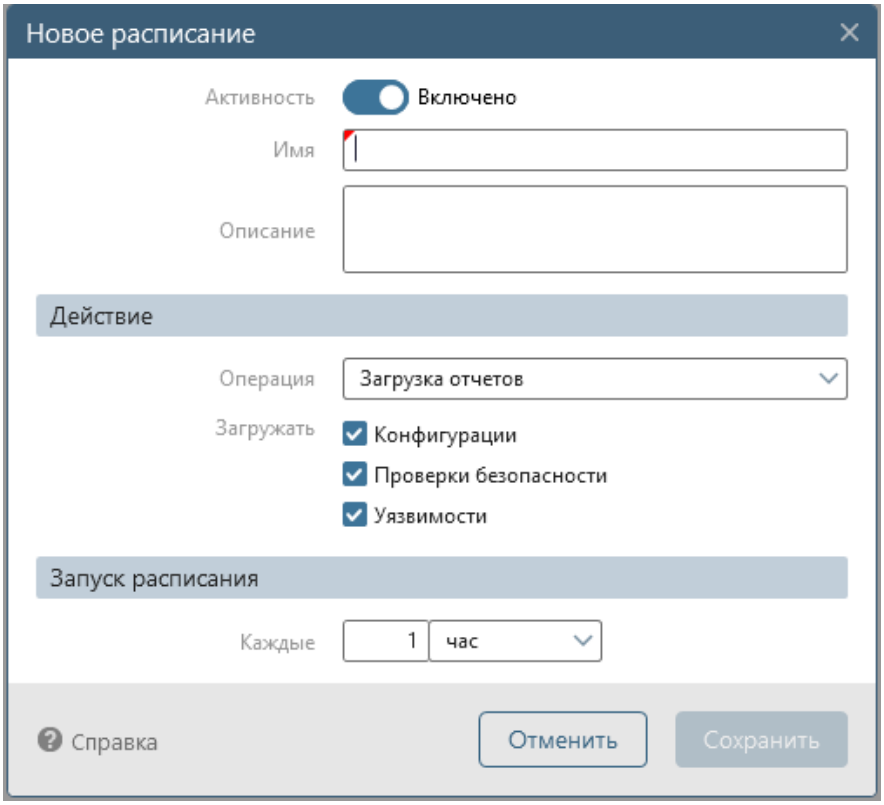
Примечание – При двойном щелчке на цифре в графе ***Устройства*** и при выборе пункта меню ***Настройки*** для устройств открывается окно просмотра и настройки использования расписания (подробнее см. п. 2.9.5 «Настройка использования расписаний»).

2.9.2. Добавление расписания

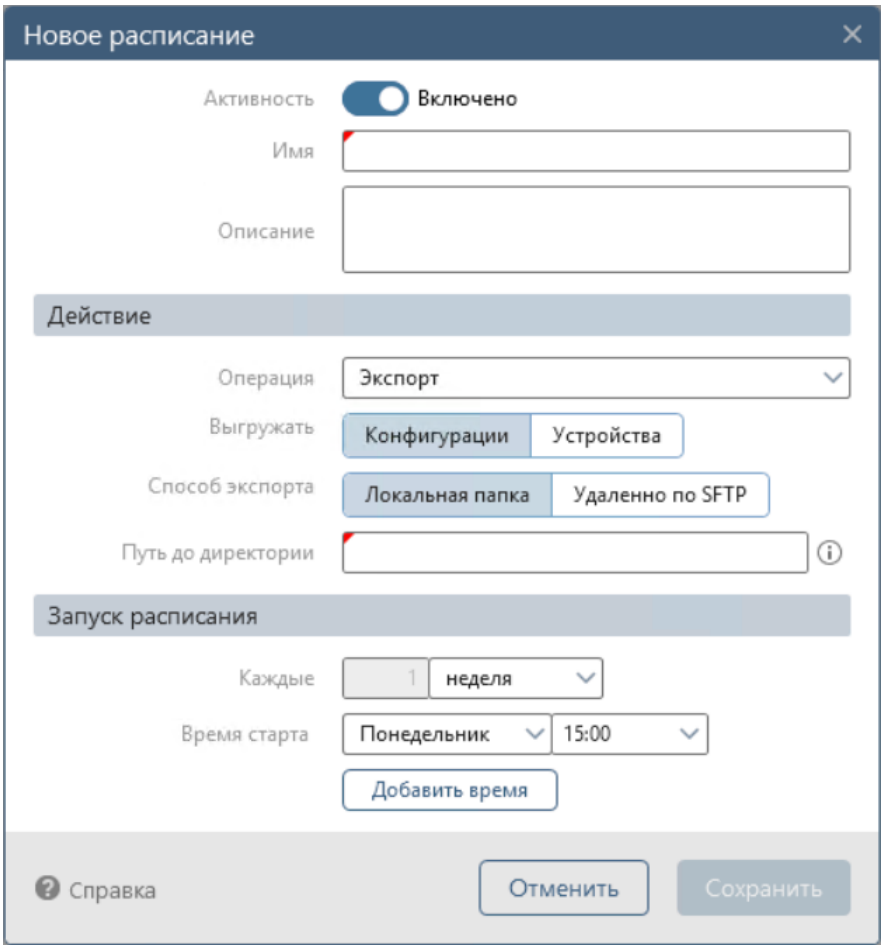
Добавлять на сервер ПК расписания загрузки отчетов (экспорта отчетов и/или устройств в файл) могут только пользователи с правами *Управление* в категории *Настройки контроля*.

Для добавления расписания пользователю необходимо выполнить следующие действия:

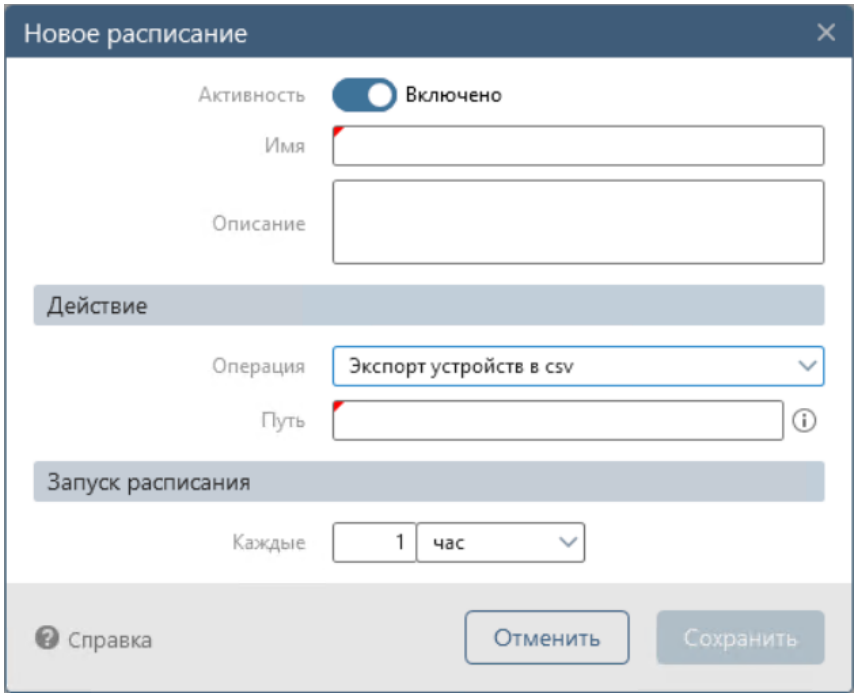
1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выбрать сервер, для которого добавляется расписание.
3) В области *Настройки контроля* нажать кнопку ***Расписания***.
4) В заголовке открывшейся формы настройки расписаний (см. рис. 94) нажать кнопку ***Расписание*** (+).
5) В открывшемся окне создания расписания (рис. 95, состав и описание значений полей окна приведено в таблице 27):
   - ввести наименование создаваемого расписания в поле ***Имя***;
   - при необходимости, ввести краткое описание создаваемого расписания в соответствующее поле;
   - для включения расписания установить переключатель в поле ***Активность*** в положение ***Включено*** ();
   - задать периодичность выполнения расписания, установив необходимые значения в полях ***Периодичность*** и ***Ежедневно/Каждые*** области *Запуск расписания*;
   - выбрать выполняемое по расписанию действие: **Загрузка отчетов** (см. рис. 95, а), **Экспорт** (см. рис. 95, б), **Экспорт устройств в csv** (см. рис. **Ошибка! Источник ссылки не найден.**, в) или **Экспорт настроек** (см. рис. 95, г);
   - указать для выбранного действия требуемые параметры в соответствии с таблицей 27;
   - нажать кнопку ***Сохранить***. Окно создания расписания закроется и произойдет возврат во вкладку настройки расписаний, в которой отобразится строка с данными добавленного расписания.


Новое расписание
Активность
Включено
Имя
Описание
Действие
Операция
Загрузка отчетов
Загружать
Конфигурации
Проверки безопасности
Уязвимости
Запуск расписания
Каждые
1
час
Справка
Отменить
Сохранить

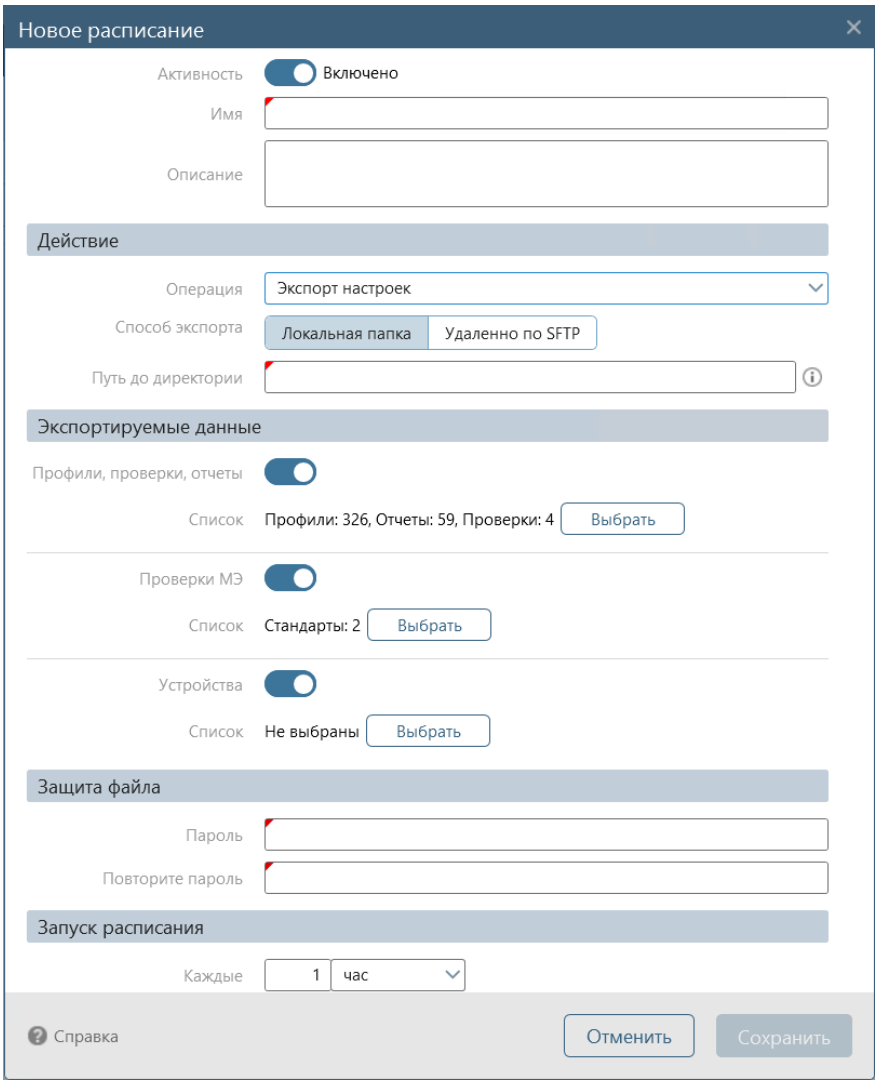
а)


Новое расписание
Активность
Включено
Имя
Описание
Действие
Операция
Экспорт
Выгружать
Конфигурации
Устройства
Способ экспорта
Локальная папка
Удаленно по SFTP
Путь до директории
Запуск расписания
Каждые
1
неделя
Время старта
Понедельник
15:00
Добавить время
Справка
Отменить
Сохранить

б)



в)



г)

Рисунок 95 – Окно добавления/редактирования расписания

Таблица 27 – Состав и описание полей окна создания/редактирования расписания

Поле	Описание/Назначение
Активность	Переключатель. При установленном переключателе расписание включено (), при снятом – выключено ()
Имя	Имя создаваемого (редактируемого) расписания. Поле обязательно к заполнению
Описание	Произвольное описание назначения расписания
Блок полей *Действие* Предназначен для выбора типа выполняемого по расписанию действия и объектов для загрузки или экспорта данных	
Операция	Выбор типа выполняемого по расписанию действия: ***Загрузка отчетов, Экспорт, Экспорт устройств в csv, Экспорт настроек***
Поля для операции ***Загрузка отчетов***	
Загружать	Для операции ***Загрузка отчетов*** установкой флагов могут быть выбраны объекты *Конфигурации*, *Проверки безопасности* и *Уязвимости*
Поля для операции ***Экспорт***	
Выгружать	Для операции ***Экспорт*** могут быть выбраны объекты выгрузки – *Конфигурации* или *Устройства*
Способ экспорта	Для операции ***Экспорт*** могут быть выбраны способы экспорта – *Локальная папка* или *Удаленно по SFTP*
Путь до директории	Для экспорта в: – локальную папку должен быть указан полный путь к каталогу, в который будет осуществляться выгрузка данных; – удаленно по SFTP должен быть указан путь до директории на удаленном сервере SFTP, а также адрес и порт сервера SFTP и данные пользователя для подключения (к полям предъявляются стандартные требования, для поля Пользователь поддерживается использование символов «\» или «@» для указания доменного имени). Для способа экспорта *Удаленно по SFTP* пользователь может проверить подключение к серверу SFTP с заданными параметрами, нажав кнопку ***Проверить подключение***
Поля для операции ***Экспорт устройств в csv***	
Путь	В поле должен быть указан путь к директории на сервере ПК для выгрузки данных. По умолчанию данные записываются в файл *SIEMdevices.scv*. При наличии файла на сервере ПК, он перезаписывается
Поля для операции ***Экспорт настроек***	
Способ экспорта и *Путь до директории*	Поля заполняется аналогично операции ***Экспорт настроек***

Поле	Описание/Назначение
Группа полей *Экспортируемые данные*	Содержит переключатели для выбора экспортируемых по расписанию данных (описание см. ниже): – *Профили, проверки, отчеты;* – *Проверки МЭ;* – *Устройства.* По умолчанию выгружаются все данные, все переключатели включены
Переключатель *Профили, проверки, отчеты*	При включенном переключателе (положение) при экспорте выполняется выгрузка параметров профилей и отчетов, выбранных в поле *Список* (см. ниже). При выключенном переключателе (положение) поле *Список* в окне не отображается, выгрузка профилей и отчетов не выполняется. Поле *Список* содержит данные о количестве выбранных для выгрузки параметров профилей, проверок и отчетов и кнопку Выбрать, по нажатию которой открывается окно выбора настроек сервера ПК для выгрузки (рис. 96). По умолчанию выбраны все профили устройств, проверки и пользовательские отчеты, имеющиеся на сервере ПК в текущий момент. Примечание – В окне выбора профилей, проверок и отчетов доступен поиск, а также фильтрация списка по типу настройки: *Профиль*, *Отчет*, *Проверка*, и по признаку *Выбрано* (*Да*, *Нет*) Окно фильтрации открывается по кнопке ***Фильтр*** ( ). После установки флага в поле ***Да*** признака *Выбрано*, в списке отображаются только выбранные профили, проверки и отчеты. Отмена фильтрации выполняется по нажатию в окне фильтрации ссылки ***Сбросить фильтр***
Переключатель *Проверки МЭ*	При включенном переключателе (положение) при экспорте выполняется выгрузка параметров стандартов проверок МЭ, выбранных в поле *Список* (см. ниже). При выключенном переключателе (положение) поле *Список* в окне не отображается, выгрузка стандартов проверок МЭ не выполняется. Поле *Список* содержит данные о количестве выбранных для выгрузки параметров стандартов проверок МЭ и кнопку *Выбрать*, по нажатию которой открывается окно выбора стандартов проверок МЭ сервера ПК (рис. 97). Окно содержит плоский список стандартов безопасности МЭ (пиктограмма «») и стандартов зонного анализа (пиктограмма «»), имеющихся на сервере ПК в текущий момент. По умолчанию для выгрузки выбраны все стандарты проверок МЭ в списке. Примечание – В окне выбора стандартов проверок МЭ доступен только поиск стандартов, возможность фильтрации списка отсутствует
Переключатель	При включенном переключателе (положение) при экспорте

Поле	Описание/Назначение
Устройства	выполняется выгрузка списка устройств, выбранных в поле *Список* (см. ниже) (взаимосвязь с выбранными для выгрузки профилями и отчетами отсутствует). При выключенном переключателе (положение) поле *Список* в окне не отображается, список устройств не выгружается. Поле *Список* содержит данные о количестве выбранных для выгрузки устройств и кнопку ***Выбрать***, по нажатию которой открывается окно **Выбор устройств**. По умолчанию в списке выбраны все устройства. Примечание – В окне выбора устройств доступен поиск устройств, а также фильтрация списка по признаку *Выбрано* и типам устройств
Группа полей *Защита файла*	Содержит поля для ввода пароля и его подтверждения для шифрования файла с выгружаемыми данными
Блок полей ***Запуск расписания*** Предназначен для настройки временных параметров запуска расписания	
Каждые	Поле для выбора временного интервала – количество и тип: *минута*, *час*, *день*, *неделя.* Если выбрана периодичность: – *минута* или *час*, то в поле устанавливается интервал времени между запусками операции загрузки отчетов/выгрузки данных соответственно в минутах или часах*;* – *день*, то в дополнительных полях (см. ниже) устанавливаются ежедневные значения времени запуска операции в формате: *ЧЧ:ММ*; – *неделя*, то в дополнительных полях (см. ниже) устанавливаются дни недели и время запуска операции в формате: *ЧЧ:ММ*
Время старта	Для интервала *день* позволяет выбрать времени запуска операции, для интервала *неделя* – дни недели и время запуска операции. По нажатию кнопки ***Добавить время*** добавляются дополнительные поля *Время старта* (с нумерацией) для добавления требуемых временных параметров запуска расписания. Каждому добавленному полю соответствует кнопка ***Удалить*** () для отмены запуска расписания в соответствующий период

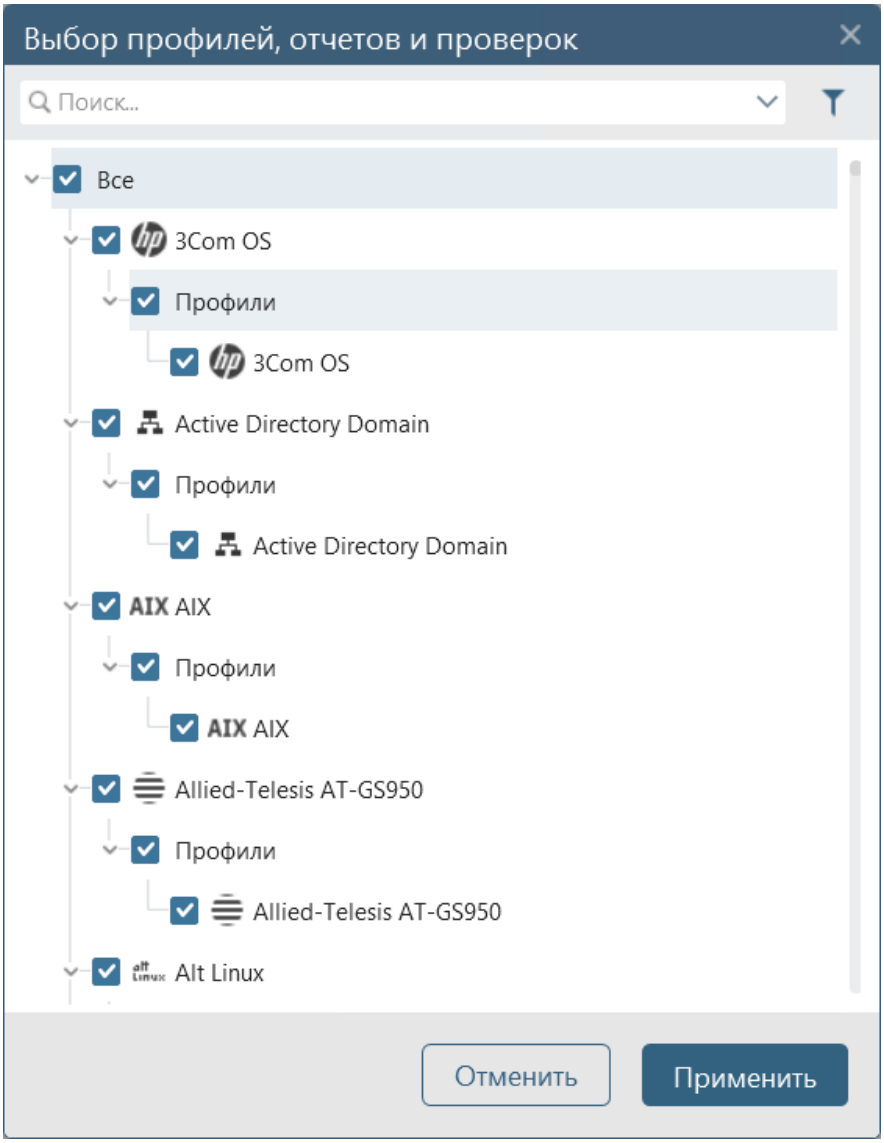


Рисунок 96 – Окно выбора профилей, отчетов и проверок

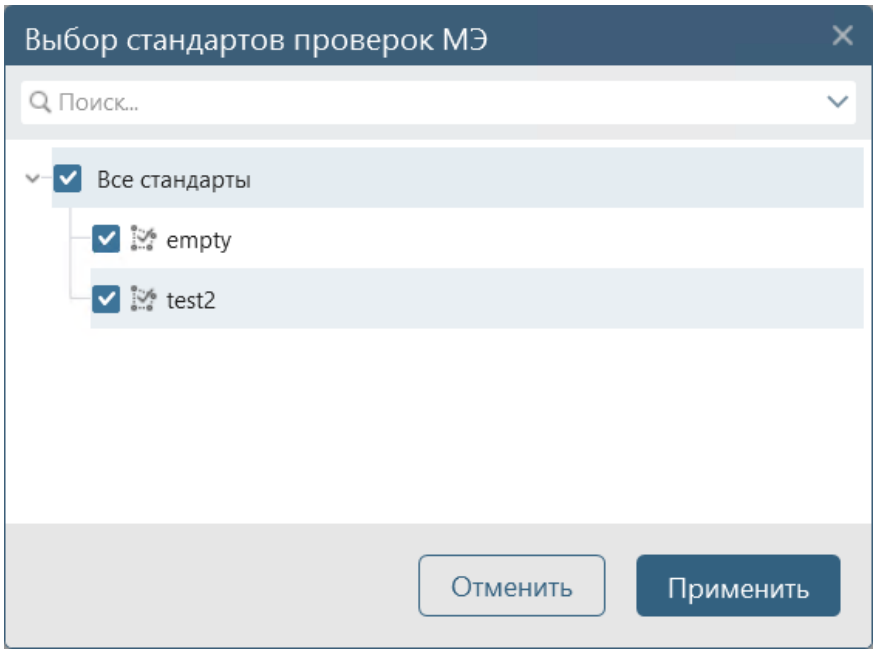


Рисунок 97 – Окно выбора стандартов проверок МЭ

2.9.3. Клонирование расписаний

На основе имеющихся в разделе ***Расписания*** расписаний можно создать (клонировать) новое расписание. Для клонирования расписания необходимо выполнить следующие действия в клиентской консоли комплекса:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выбрать сервер, на котором клонируется расписание.
3) В области *Настройки контроля* нажать кнопку ***Расписания***.
4) В открывшейся форме настройки расписаний (см. рис. 94) выделить необходимое расписание.
5) В строке расписания нажать кнопку ***Меню*** (⋯) и выбрать в раскрывшемся меню пункт ***Клонировать***.
6) В открывшемся окне клонирования расписания (аналогично окну создания расписания (см. рис 95), описание полей окна приведено в таблице 27) изменить имя расписания (обязательно), внести требуемые изменения в остальные параметры исходного расписания.
7) При необходимости отключения/включения расписания снять/установить переключатель в поле ***Активность***.
8) Нажать кнопку ***Сохранить***, окно закроется, в списке расписаний появится строка нового расписания.

Примечание – Для клонирования не доступно расписание ***Обновление базы уязвимостей***.

2.9.4. Запуск расписания вручную

Для запуска расписания без отсрочки необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выбрать сервер, на котором клонируется расписание.
3) В области *Настройки контроля* нажать кнопку ***Расписания***.
4) В открывшейся форме настройки расписаний (см. рис. 94) выделить необходимое расписание.
5) В строке расписания нажать кнопку ***Меню*** (⋯) и выбрать в раскрывшемся меню пункт ***Запустить принудительно***.
6) Будет запущено выполнение заданных в расписании действий с заданными в нем параметрами.

Примечание – Периодичность запуска, заданная в расписании, при этом не изменится.

2.9.5. Настройка использования расписаний

Настройка использования расписаний может быть выполнена как в списке расписаний формы ***Расписания*** для всех устройств (групп) сервера ПК, так и в списке устройств раздела **Устройства** для каждого устройства (группы) отдельно (см. п. 2.7.4 «Настройка режима использования расписаний для устройств»).

Для настройки использования расписания для всех устройств (групп) сервера ПК пользователю необходимо выполнить следующие действия:

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

2) Выбрать сервер, для которого настраивается расписание.

3) В области *Настройки контроля* нажать кнопку ***Расписания***.

4) В открывшейся форме ***Расписания*** в строке изменяемого расписания дважды щелкнуть на цифре в графе ***Устройства*** либо нажать кнопку ***Меню*** ( ) и выбрать в раскрывшемся списке пункт ***Настройки для устройств***. Откроется окно настройки использования изменяемого расписания (рис. 98). В окне выведена вся иерархия папок и устройств, контролируемых текущей серверной частью комплекса, с текущим статусом использования расписания.

5) Для настройки использования расписания для одного устройства/группы необходимо:

- отфильтровать список устройств, нажав кнопку ***Фильтр*** ( ) и выбрав в окне фильтрации (рис. 99) параметры требуемых устройств по их типу и текущему состоянию параметра *Проверка доступности*;
- выполнить поиск устройства/группы с использованием поля *Поиск*;
- выбрать в строке найденного устройства/группы требуемую настройку использования расписания. Перечень возможных значений настройки для групп устройств и устройств приведен в таблице 28.

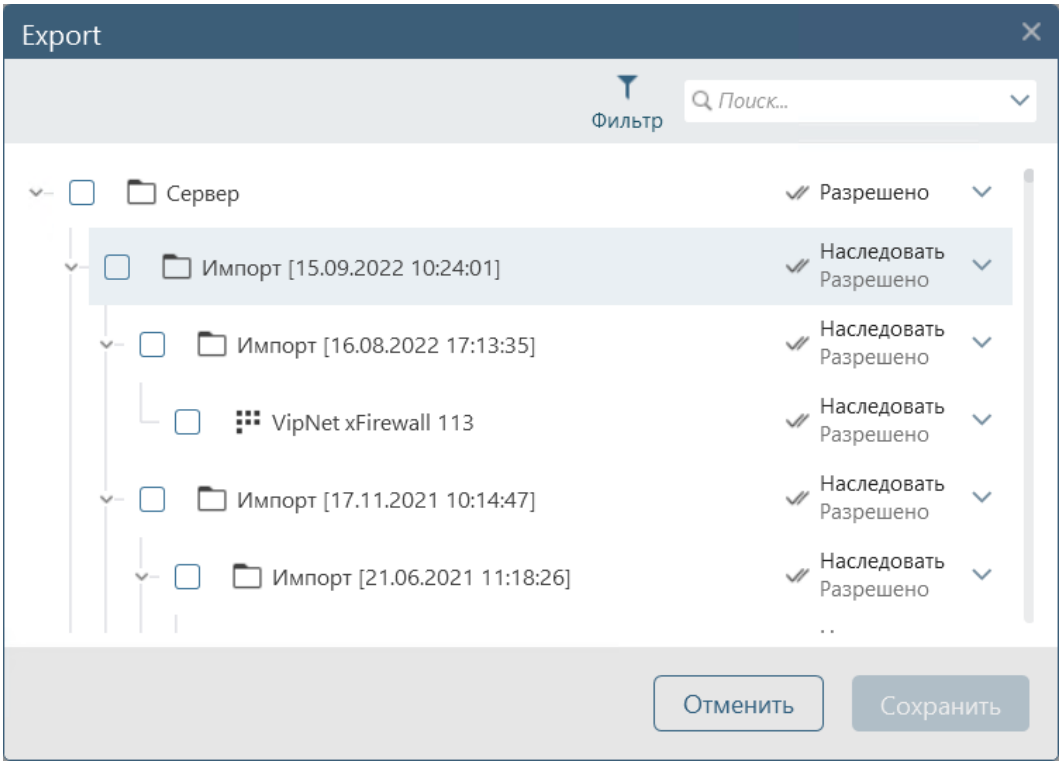


Рисунок 98 – Окно настройки использования изменяемого расписания

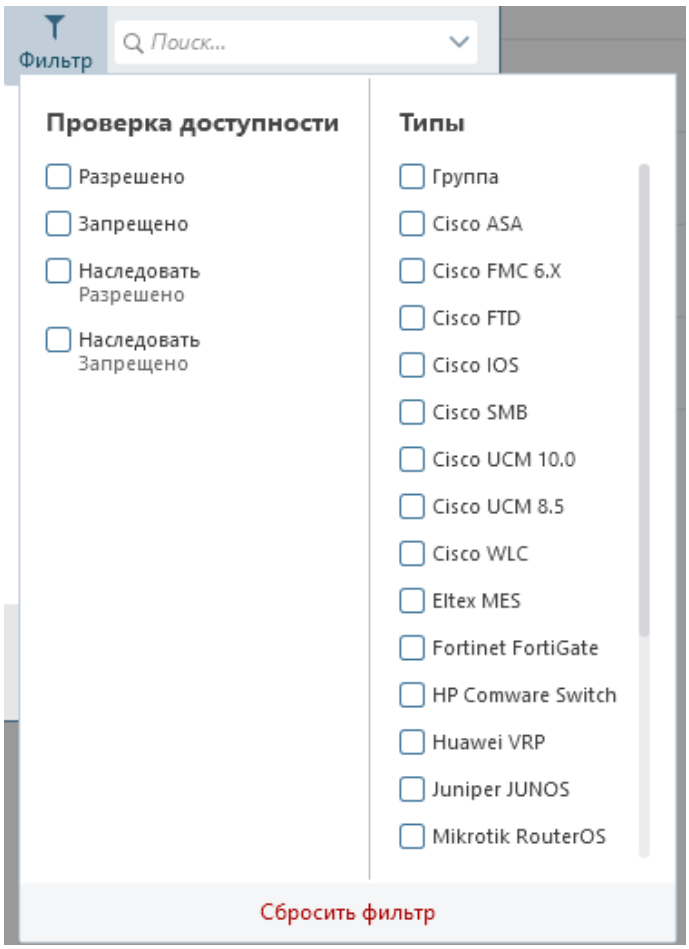


Рисунок 99 – Окно фильтрации списка устройств при настройке использования изменяемого расписания

Таблица 28 – Перечень возможных значений настройки использования расписания для групп устройств и устройств

Тип объекта	Значение настройки
Корневая группа	Возможные значения: – *Разрешено* – разрешить использование расписания; – *Запрещено* – запретить использование расписания
Другие группы и устройства	Возможные значения: – *Разрешено* – разрешить использование расписания вне зависимости от настроек родительской группы; – *Запрещено* – запретить использование расписания вне зависимости от настроек родительской группы; – *Наследовать (XXXXXX)* – применить настройки родительской группы. В скобках отображается значение, установленное в родительской группе: *Разрешено* или *Запрещено*

6) Для настройки использования расписания для нескольких устройств/групп необходимо:

- отфильтровать список устройств, нажав кнопку ***Фильтр*** (▼) и выбрав в окне фильтрации (см. рис. 99) параметры требуемых устройств по их типу и текущему состоянию параметра *Проверка доступности*;

- выполнить поиск устройств/группы с использованием поля *Поиск*;
- установить флаги в строках требуемых устройств/групп устройств. В заголовке окна отобразится общее количество выбранных групп и устройств (рис. 100) и поле выбора настройки использования расписания. Если текущая настройка для выбранных устройств/групп различная, то в поле отображается значение *Разные значения,* если одинаковая, то – текущее значение настройки;
- выбрать в поле выбора настройки использования расписания требуемую настройку использования расписания (см. таблицу 28)

7) Нажать кнопку ***Сохранить***. Окно настройки использования расписания закроется, внесенные изменения будут применены.

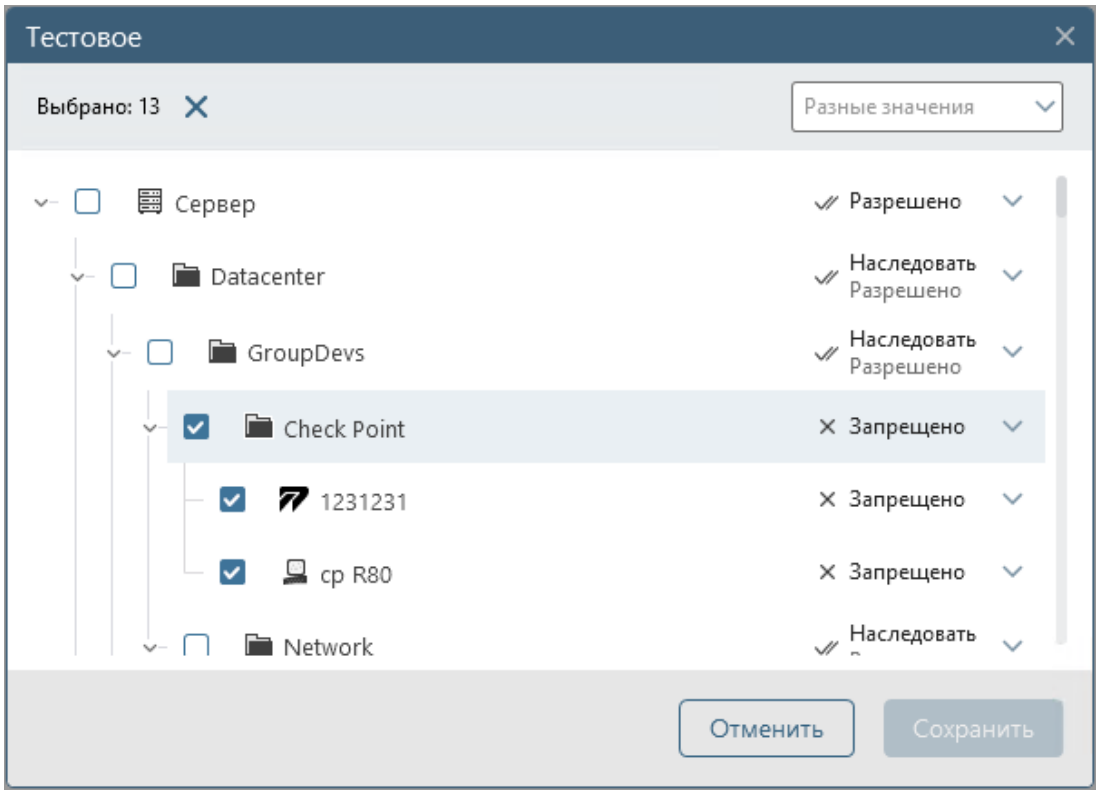


Рисунок 100 – Окно настройки использования изменяемого расписания с выбранными устройствами

2.9.6. Изменение расписания

Изменять настройки расписаний загрузки отчетов (экспорта отчетов и/или устройств в файл) на сервере ПК могут только пользователи с правами *Управление* в категории *Настройки контроля*.

Для изменения расписания пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выбрать сервер, для которого изменяется расписание.
3) В области *Настройки сервера* нажать кнопку ***Расписания.***

4) В открывшейся форме настройки расписаний нажать в строке изменяемого расписания кнопку ***Изменить*** (⚙).

5) В открывшемся окне редактирования расписания (аналогично окну создания расписания (см. рис. 95), описание полей окна приведено в таблице 27) внести требуемые изменения в параметры расписания.

6) При необходимости отключения/включения расписания снять/установить переключатель в поле ***Активность***.

7) Нажать кнопку ***Сохранить*** в окне редактирования расписания, окно закроется и произойдет возврат во вкладку настройки расписаний загрузки отчетов, внесенные изменения будут сохранены.

2.9.7. Удаление расписания

Удалять расписания загрузки отчетов (экспорта отчетов и/или устройств в файл) с сервера ПК могут только пользователи с правами *Управление* в категории *Настройки контроля*.

Для удаления расписания пользователю необходимо выполнить следующие действия:

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

2) Выбрать сервер, для которого удаляется расписание.

3) В области *Настройки контроля* нажать кнопку ***Расписания***.

4) В открывшейся форме настройки расписаний нажать в строке удаляемого расписания кнопку Меню (⋯) и выбрать в раскрывшемся меню пункт ***Удалить***.

5) Подтвердить операцию удаления расписания, нажав кнопку ***Удалить*** в открывшемся окне. Произойдет возврат в форму настройки расписаний загрузки отчетов (экспорта отчетов и/или устройств в файл), удаленное расписание пропадет из списка.

2.10. Настройка профилей подключения

2.10.1. Просмотр списка профилей подключения

Для просмотра списка профилей подключения необходимо:

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

2) Выбрать в поле ***Сервер*** наименование сервера, список профилей подключения которого просматривается.

3) Нажать в панели ***Настройки контроля*** ссылку ***Профили подключения.*** Откроется форма управления профилями аутентификации пользователей на устройствах, контролируемых текущей серверной частью комплекса (рис. 101).

Форма содержит:

- кнопку ***Добавить*** (+) – для перехода в форму добавления профиля подключения. При нажатии открывается меню из пунктов *Профиль*

аутентификации и *Snmp профиль* для выбора типа добавляемого профиля аутентификации (см. п. 2.10.2 «Добавление профиля подключения»);

- кнопку ***Использование*** () – для перехода в окно просмотра и настройки использования профиля подключения (в окне выведена вся иерархия папок и устройств комплекса с текущим статусом использования профиля подключения);
- список имеющихся профилей подключения (сразу после инсталляции сервера ПК профили подключения в форме отсутствуют).

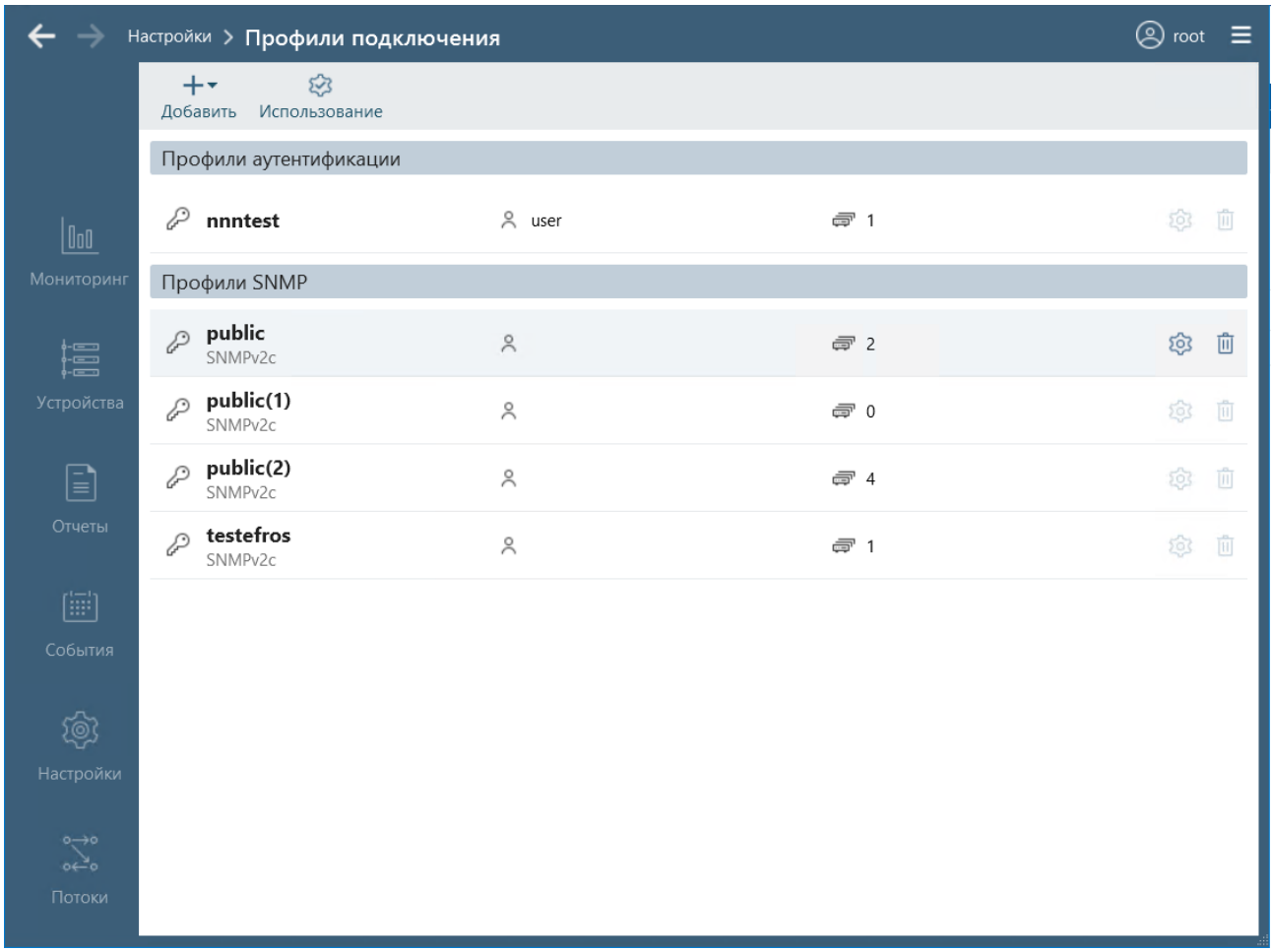


Рисунок 101 – Форма настройки профилей подключения

Для каждого профиля подключения в форме их настройки отображаются данные:

- имя профиля;
- имя пользователя;
- количество устройств, для подключения к которым используется профиль;
- кнопка ***Изменить*** () – для перехода в окно настройки параметров профиля аутентификации (см. п. 2.10.3 «Изменение профиля подключения»);
- кнопка ***Удалить*** () – для удаление профиля аутентификации (см. п. 2.10.4 «Удаление профиля подключения»).

2.10.2. Добавление профиля подключения

Добавлять на сервер ПК профили аутентификации могут только пользователи с правами *Управление* в категории *Настройки контроля*.

Профили добавляются в список в форме настройки профилей подключения и могут быть добавлены при создании учетной записи устройства.

Для добавления профиля аутентификации в форме настройки профилей подключения пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выбрать сервер, для которого добавляется профиль подключения.
3) В области *Настройки контроля* нажать кнопку ***Профили подключения***.
4) В открывшейся форме настройки профилей подключения (см. рис. 101) нажать кнопку ***Добавить*** (+) и, в открывшемся дополнительном списке, выбрать вид добавляемого профиля (профиль аутентификации/SNMP профиль).
5) В открывшемся окне создания профиля аутентификации (рис. 102, состав и описание значений полей окна приведено в таблице 29):

- ввести в поле **Имя профиля** название создаваемого профиля аутентификации;
- в соответствующие поля ввести имя (логин) и пароль учетной записи, от имени которой будет происходить авторизация на контролируемых сервером ПК устройствах;
- для возможности авторизации на контролируемых устройствах в привилегированном режиме ввести соответствующий пароль в поле **Дополнительный пароль**;
- нажать кнопку ***Сохранить***. Окно создания профиля аутентификации закроется и произойдет возврат во вкладку настройки профилей аутентификации, в которой отобразится строка с данными добавленного профиля аутентификации.

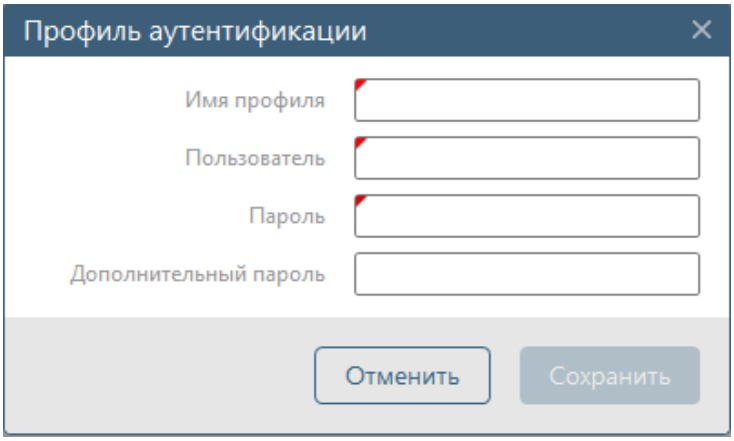


Рисунок 102 – Окно добавления/редактирования профиля подключения

Таблица 29 – Состав и описание полей окна создания/редактирования профиля подключения

Поле	Описание/Назначение
Имя профиля	Имя создаваемого (редактируемого) профиля подключения. Поле обязательно к заполнению
Пользователь	Имя (логин) учетной записи пользователя, которая будет использоваться для авторизации на контролируемом устройстве. Поле обязательно к заполнению
Пароль	Пароль учетной записи пользователя, которая будет использоваться для авторизации на контролируемом устройстве. Поле обязательно к заполнению
Дополнительный пароль	Пароль учетной записи пользователя, для авторизации на контролируемых устройствах в привилегированном режиме. Необходим для некоторых типов устройств. Поле не обязательно к заполнению
Дополнительно для SNMP профиля	
Порт	Порт на устройстве, на который будут отправляться SNMP-запросы
SNMPv2c	Включение (отключение) использования версии 2c протокола SNMP для подключения к контролируемому устройству.
Community	Идентификатор используемый для аутентификации на контролируемом устройстве при использовании протокола SNMPv.2c. Рекомендуемое значение ***public***. Поле обязательно к заполнению при использовании SNMPv2c
SNMPv3	Включение (отключение) использования версии 3 протокола SNMP для подключения к контролируемому устройству
Аутентификация	Выбор алгоритма хеширования при аутентификации контролируемого устройства при использовании протокола SNMPv.3. Можно установить использование алгоритмов ***MD5*** (Message Digest 5), ***SHA*** (Secure Hash Algorithm), либо отказаться от хеширования выбрав значение ***None***
Пользователь	Имя (логин) учетной записи пользователя, которая будет использоваться для авторизации на контролируемом устройстве по протоколу SNMPv.3. Поле обязательно к заполнению при использовании SNMPv.3
Пароль	Пароль учетной записи пользователя, которая будет использоваться для авторизации на контролируемом устройстве по протоколу SNMPv.3. Поле обязательно к заполнению при использовании SNMPv.3
Алгоритм защиты	Выбор алгоритма для подключения к контролируемому устройству при использовании протокола SNMPv.3. Возможные варианты для выбора: – AES128 (Advanced Encryption Standard); – DES (Data Encryption Standard). Для отказа – выбрать значение **«*None*»**
Пароль	Пароль для управления контролируемым устройством при использовании протокола SNMPv.3. Поле обязательно к заполнению при использовании SNMPv.3

При создании SNMP профиля после его выбора при выполнении команды ***Добавить*** (+) откроется окно добавления /редактирования SNMP профиля (рис. 103, состав и описание значений полей окна приведено в таблице 29).

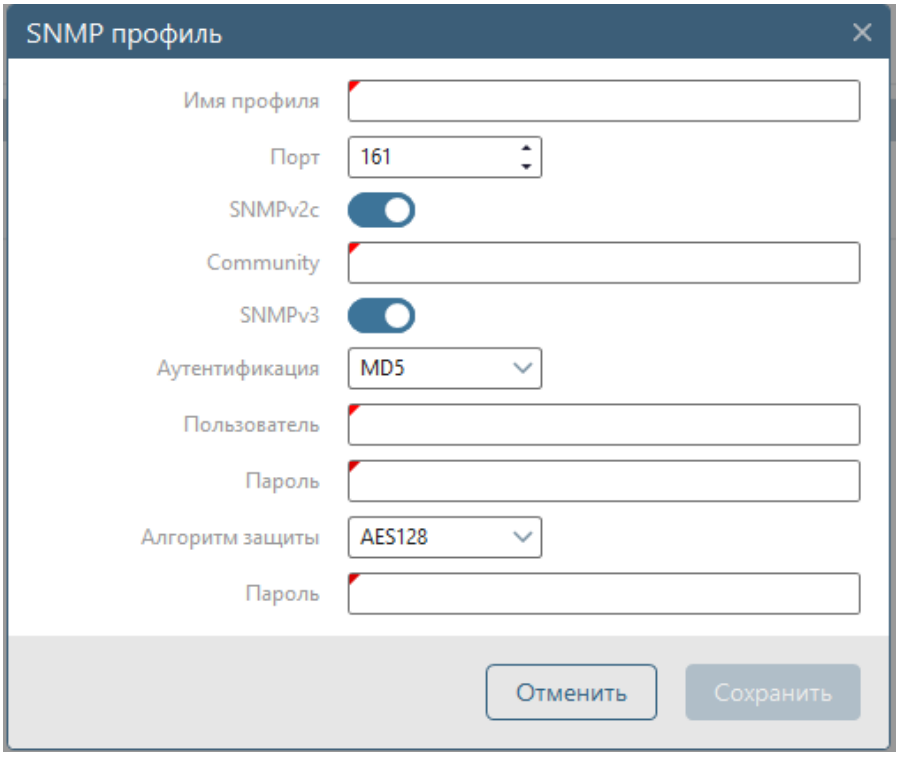


Рисунок 103 – Окно добавления/редактирования SNMP профиля

2.10.3. Изменение профиля подключения

Изменять параметры профилей подключения на сервере ПК могут только пользователи с правами *Управление* в категории *Настройки контроля*.

Профили могут быть изменены как в форме настройки профилей подключения и так и при редактировании учетной записи устройства.

Для изменения параметров профиля подключения в форме настройки профилей подключения пользователю необходимо выполнить следующие действия:

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

2) Выбрать, при необходимости, сервер, для которого изменяется профиль подключения.

3) В области *Настройки контроля* нажать кнопку ***Профили подключения***.

4) В открывшейся форме настройки профилей подключения (см. рис. 101) выделить изменяемый профиль подключения и нажать в строке профиля кнопку ***Настройки*** (⚙) .

5) В открывшемся окне редактирования профиля подключения (см. пример на рис. 102, таблицу 29) внести требуемые изменения в параметры профиля подключения.

6) Нажать кнопку ***Сохранить*** в окне редактирования профиля подключения, окно закроется и произойдет возврат во вкладку настройки профилей подключения, внесенные в редактируемый профиль подключения изменения будут сохранены.

2.10.4. Удаление профиля подключения

Удалять профили аутентификации с сервера ПК могут только пользователи с правами *Управление* в категории *Настройки контроля*.

Для удаления профиля подключения пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выбрать сервер, для которого удаляется профиль подключения.
3) В области *Настройки контроля* нажать кнопку ***Профили подключения***.
4) В открывшейся форме настройки профилей подключения (см. рис. 101) в строке удаляемого профиля подключения нажать кнопку ***Удалить***.
5) Подтвердить операцию удаления профиля, нажав кнопку ***Удалить*** в открывшемся окне. Произойдет возврат в форму настройки профилей подключения, удаленный профиль пропадет из списка.

2.10.5. Настройка режима использования профилей подключения для устройств

Изменять настройки режима использования профилей подключения для устройства могут только пользователи с правами *Управление* в категории *Настройки контроля.*

ВНИМАНИЕ: Назначение профилей подключения типа ***Профиль аутентификации*** для устройств, поддерживающих использование двух профилей аутентификации может быть выполнено только в карточке устройства в разделе **Устройства**!

Для настройки режима использования профилей подключения для отдельного устройства пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) Выбрать сервер, для которого настраивается профиль подключения.
3) В области *Настройки контроля* нажать кнопку ***Профили подключения***.
4) В открывшейся форме настройки профилей подключения (см. рис. 101) нажать в заголовке кнопку ***Использование*** ().
5) В открывшемся окне **Профили подключения** (рис. 104) в строке требуемого устройства выбрать для обоих типов профилей подключения (аутентификации и SNMP) требуемое значение варианта использования (из перечня значений раскрывающихся списков полей ***Профиль аутентификации***, ***SNMP профиль***). Списки полей ***Профиль аутентификации***, ***SNMP профиль*** могут содержать значение *Не доступно* (подключение по соответствующему типу

подключения не доступно) или значение *Отсутствует* (выбрано по умолчанию) и наименования имеющихся в списке формы настройки профилей подключения (см. рис. 101) профилей подключения соответствующего типа.

Примечание – Если устройство поддерживает два профиля аутентификации (например, на рис. 104, это устройства *vCentertest1* и *zVirt*), то в столбце ***Профиль аутентификации*** отображаются оба назначенных для устройства профиля или, если профиль не назначен, то отображается значение *Отсутствует*. Поле не доступно для внесения изменений.

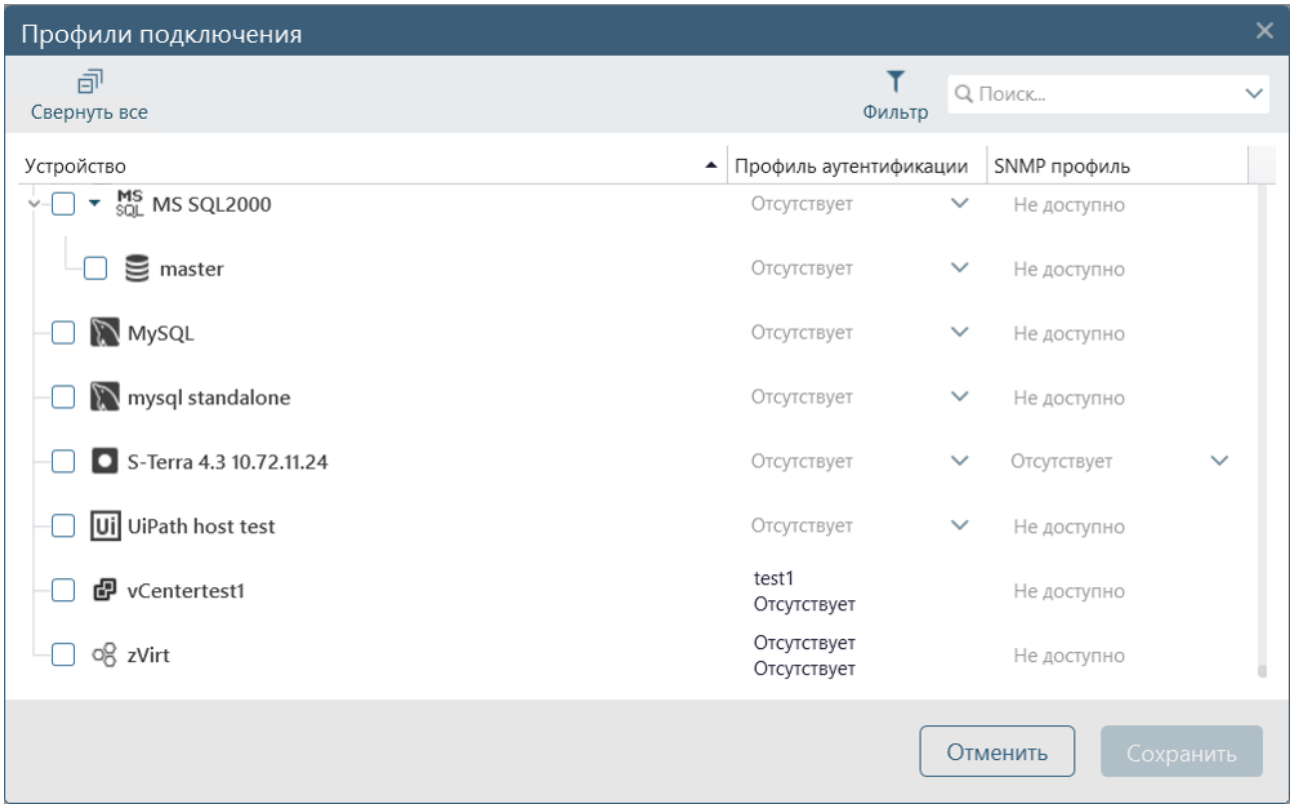


Рисунок 104 – Окно настройки использования профилей подключения для устройств

6) После выбора в окне настройки использования профилей подключения для устройств требуемых профилей подключения нажать кнопку ***Сохранить***. Окно закроется, внесенные изменения будут сохранены.

Для настройки режима использования профилей подключения для группы устройств пользователю необходимо выполнить следующие действия:

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

2) Выбрать сервер, для которого настраивается профиль подключения.

3) В области *Настройки контроля* нажать кнопку ***Профили подключения***.

4) В открывшейся форме настройки профилей подключения (см. рис. 101) нажать в заголовке кнопку ***Использование*** ( ).

5) В открывшемся окне **Профили подключения** выбрать установкой флагов требуемые устройства (рис. 105). В заголовке отобразится общее количество выбранных устройств (для отмены выбора всех устройств одновременно

необходимо нажать кнопку) и добавятся поля выбора профилей подключения обоих типов (аутентификации и SNMP) для выбранной группы устройств. Списки полей содержат значение *Отсутствует* и наименования имеющихся в списке формы настройки профилей подключения (см. рис. 101) профилей подключения соответствующего типа.

Примечание – Если для выбранных устройств ранее выбран один и тот же профиль подключения соответствующего типа, то его наименование (или значение *Отсутствует*) отображается в соответствующем дополнительном поле заголовка, если разные – в поле отображается текст *Разные значения*.

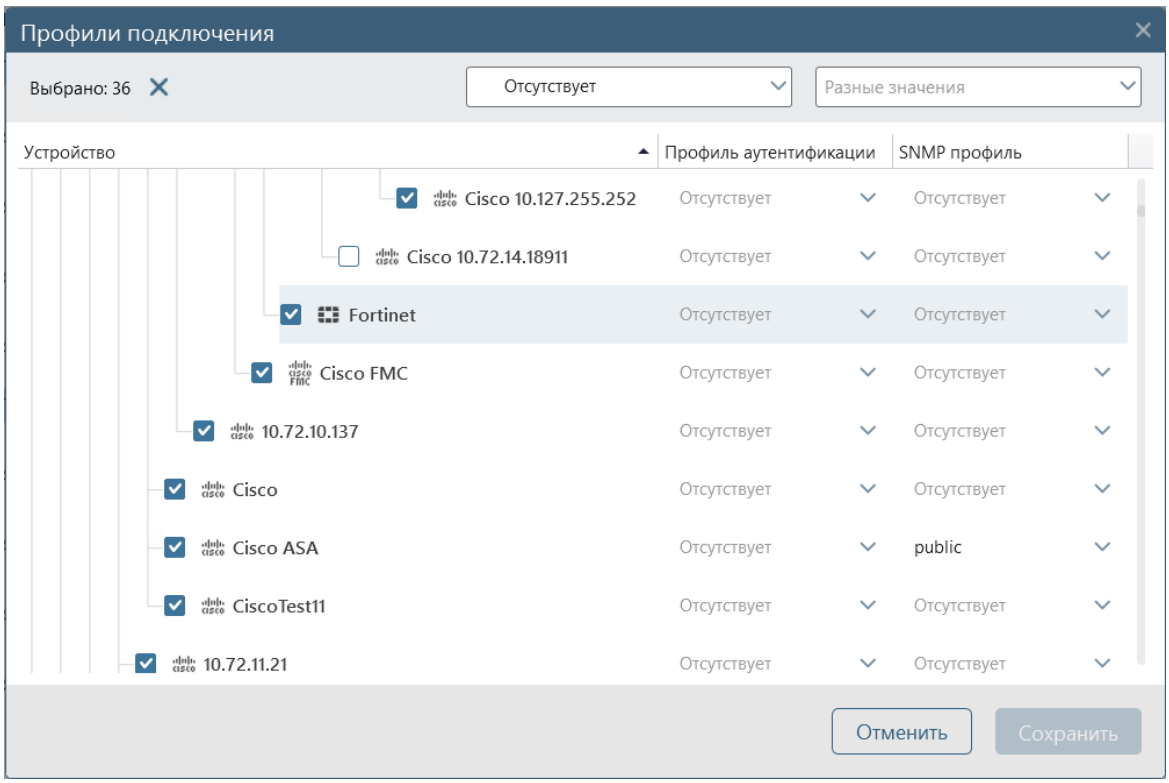


Рисунок 105 – Окно настройки использования профилей подключения для устройств

6) Выбрать в дополнительных полях заголовка для обоих типов профилей подключения (аутентификации и SNMP) требуемое значение *Отсутствует* или наименование одного из имеющихся в списке формы настройки профилей подключения (см. рис. 101) профиля подключения соответствующего типа.

7) Нажать кнопку ***Сохранить***. Окно закроется, внесенные изменения будут сохранены.

Примечание – Если выбранное в списке устройство поддерживает два профиля аутентификации (например, на рис. 104, это устройства *vCentertest1* и *zVirt*), то его настройки изменены не будут.

Примечание – В окне настройки использования профилей подключения для устройств пользователь может свернуть дерево устройств, нажав кнопку ***Свернуть все*** (), найти требуемое устройство, используя поле ***Поиск***, а также выполнить фильтрацию списка устройств по используемому профилю аутентификации, нажав в заголовке окна кнопку ***Фильтр*** () и выбрав установкой флагов в открывшемся окне

фильтрации требуемые значения списков полей ***Профиль аутентификации***, ***SNMP профиль.***

2.11. Настройка проверок межсетевых экранов

2.11.1. Просмотр списка зон сети и стандартов безопасности и зонного анализа МЭ

Для просмотра списка зон сети и стандартов безопасности и зонного анализа МЭ необходимо:

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

2) Выбрать сервер, список зон сети и стандартов зонного анализа которого просматривается, для чего нажать кнопку ***Сервер*** и выбрать в открывшемся окне **Выбор сервера** строку требуемого сервера.

3) Нажать в панели ***Настройки контроля*** ссылку ***Проверки межсетевых экранов.*** Откроется форма настройки проверок МЭ (рис. 106). Форма содержит вкладки:

- ***Стандарты безопасности*** – для ведения списка стандартов безопасности МЭ, содержащих требования для контроля наличия/отсутствия правил МЭ;
- ***Зонный анализ*** – для ведения списка стандартов зонного анализа МЭ, содержащих требования запрета или разрешения прохождения трафика между зонами;
- ***Зоны*** – для ведения списка контролируемых сервером ПК зон сети.

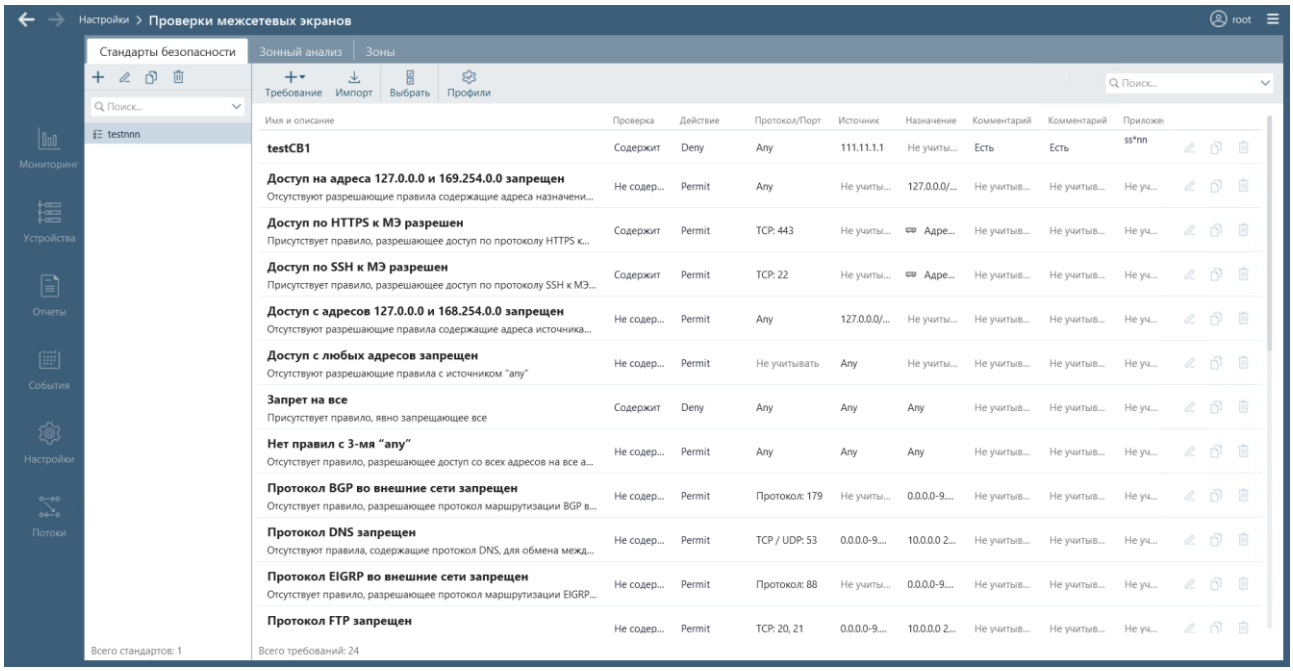


Рисунок 106 – Форма настройки проверок МЭ

2.11.1.1. Просмотр списка стандартов безопасности МЭ

Вкладка ***Стандарты безопасности*** (см. рис. 106), содержащая список стандартов безопасности МЭ, по умолчанию открывается после перехода в форму настройки проверок МЭ. Рабочая область вкладки разделена на:

- панель списка стандартов безопасности;
- область настройки параметров стандартов безопасности.

Панель списка стандартов безопасности содержит список стандартов безопасности МЭ и в заголовке панели:

- кнопку ***Добавить*** () – активна всегда. При нажатии на кнопку открывается окно ***Новый стандарт безопасности МЭ*** для задания имени и описания добавляемого стандарта (см. п. 2.11.3 «Добавление стандартов »);
- кнопку ***Свойства*** () – активна при выборе в списке одного из стандартов. Служит для изменения параметров выбранного стандарта, имени и описания (см. п. 2.11.6 «Изменение стандартов безопасности МЭ и стандартов зонного анализа»);
- кнопку ***Клонировать*** () – активна только при выборе в списке одного из стандартов. Служит для создания нового стандарта на основе выбранного в списке стандарта (см. п. 2.11.3 «Добавление стандартов »);
- кнопку ***Удалить*** () – активна при выборе в списке одного из стандартов. Служит для удаления стандарта (см. п. 2.11.8 «Удаление стандартов безопасности и стандартов зонного анализа»);
- поле ***Поиск*** – для ввода символов из имени искомого стандарта, позволяет искать в списке стандартов те из них, которые удовлетворяют введенному в поле значению.

В списке стандартов безопасности МЭ для каждого стандарта отображается только его наименование. В нижней части панели списка стандартов безопасности отображается общее количество стандартов безопасности.

Область настройки параметров стандартов содержит список требований стандарта, выбранного в панели списка стандартов, и в заголовке области:

- кнопку ***Требование*** () – активна всегда. Предназначена для создания нового требования или для копирования требований из существующего стандарта безопасности. При нажатии кнопки раскрывается меню с пунктами ***Создать новое*** и ***Скопировать из стандарта***. При выборе пункта ***Создать новое*** открывается окно **Требование стандарта безопасности МЭ**, при выборе пункта ***Скопировать из стандарта*** – окно **Добавить правило**, в котором возможно выбрать существующие требования для добавления в новый стандарт (см. п. 2.11.4 «Добавление требований в стандарты безопасности и стандарты зонного анализа»);

- кнопку ***Импорт*** () – активна всегда. Предназначена для импорта требований пользовательского стандарта из файла формата XML. При нажатии на нее открывается стандартное окно используемой ОС для выбора требуемого файла (см. п. 2.11.4.4 «Добавление требований в стандарт безопасности МЭ или зонного анализа путем импорта требований»);
- кнопку ***Выбрать*** () – предназначена для перехода в форму выбора требований стандарта безопасности для экспорта в файл формата XML (рис. 107);
- кнопку ***Профили*** () – предназначена для перехода в окно настройки использования стандарта безопасности МЭ (см. п. 2.11.5 «Настройка использования стандартов безопасности и стандартов зонного анализа»).

Примечание – При отсутствии для стандарта безопасности МЭ требований, кнопка ***Профили*** () неактивна, настройка использования стандарта безопасности МЭ не доступна.

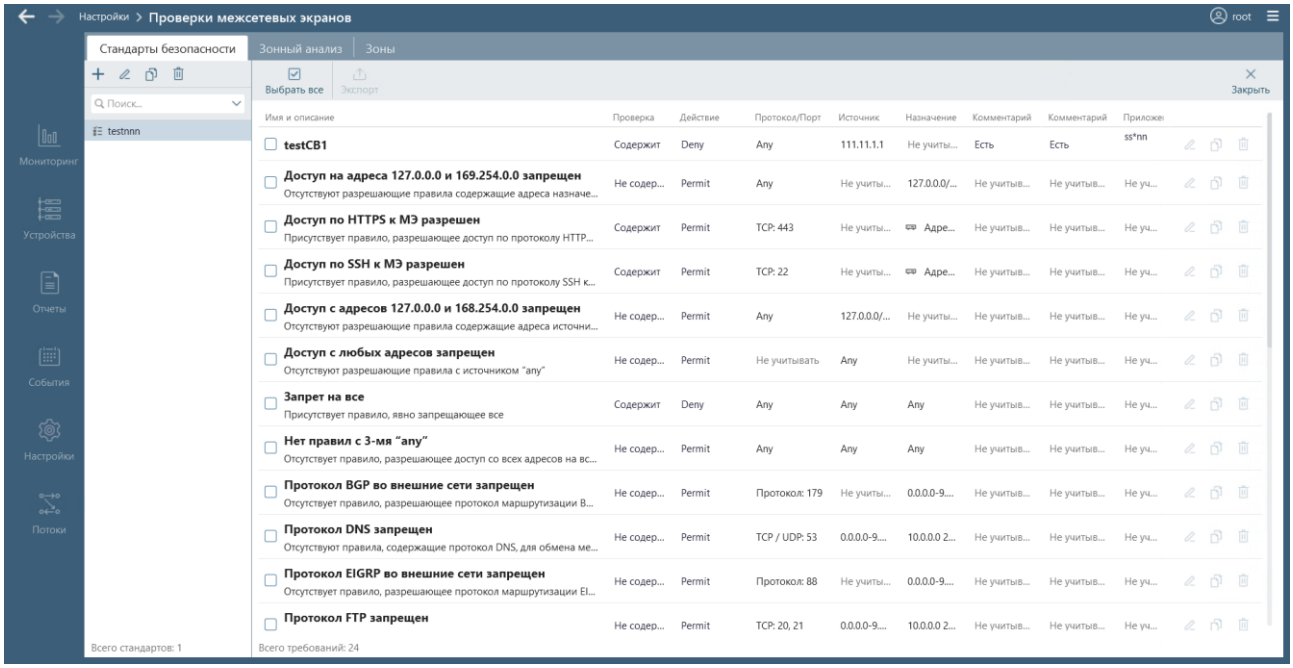


Рисунок 107 – Форма выбора требований стандарта безопасности для экспорта в файл формата XML

Форма выбора требований стандарта безопасности для экспорта в файл формата XML содержит кнопки:

- ***Выбрать все*** () – для выбора всех требований выделенного в списке стандарта и экспорта их в файл формата XML;
- ***Экспорт*** () – активна только после выбора в форме хотя бы одного требования. Предназначена для экспорта требований в файл формата XML (см. п. 2.11.7 «Экспорт требований стандарта безопасности МЭ или зонного анализа»);

- ***Закрыть*** ( ) – предназначена для закрытия формы выбора требований.

Для каждого требования в области настройки параметров стандартов безопасности отображаются его имя, описание и заданные параметры, а также кнопки

- ***Редактировать*** ( ) – для перехода в окно редактирования параметров требования (см. п. 2.11.6.2 «Редактирование требований стандартов»);
- ***Клонировать*** ( ) – для добавления в стандарт нового требования путем копирования имеющегося в стандарте (см. п. 2.11.4.1 «Добавление в стандарт безопасности МЭ нового требования вручную и копированием»);
- ***Удалить*** ( ) – для удаления требования (см. п. 2.11.6.3 «Удаление требований и исключений из стандартов безопасности и стандартов зонного анализа»).

В нижней части области настройки параметров стандартов безопасности отображается общее количество требований стандарта безопасности, выбранного в панели списка стандартов безопасности.

При отсутствии требований в области настройки параметров стандарта безопасности МЭ отображаются кнопки ***Скопировать из стандарта*** и ***Создать новое требование*** дублирующие кнопку ***Требование*** ( ).

2.11.1.2. Просмотр списка стандартов зонного анализа

Рабочая область вкладки ***Зонный анализ*** (рис. 108) разделена на:

- панель списка стандартов зонного анализа;
- область настройки параметров стандартов зонного анализа.

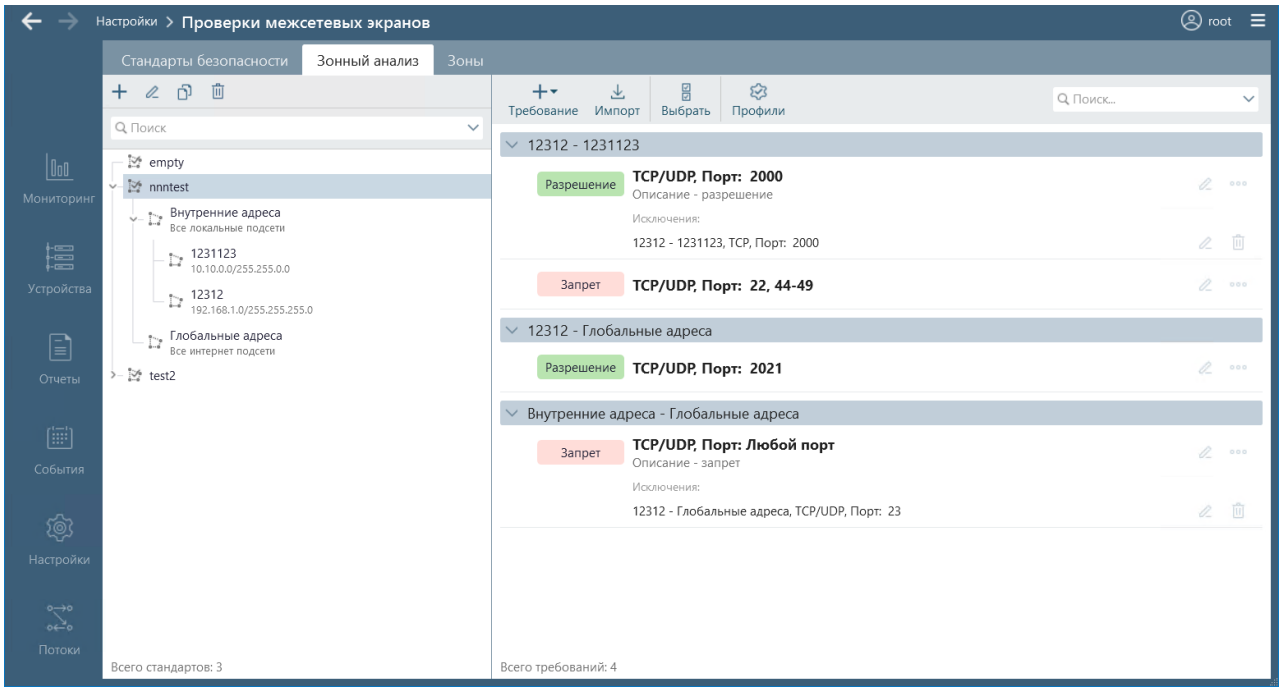


Рисунок 108 – Вкладка ***Зонный анализ***

Панель списка стандартов вкладки ***Зонный анализ*** содержит список стандартов зонного анализа и в заголовке панели:

- кнопку () – активна всегда. При нажатии на кнопку открывается окно **Новый стандарт зонного анализа** для задания имени и описания добавляемого стандарта (см. п. 2.11.3 «Добавление стандартов »);
- кнопку ***Свойства*** () – активна при выборе в списке одного из стандартов. Служит для изменения параметров выбранного стандарта, имени и описания (см. п. 2.11.6 «Изменение стандартов безопасности МЭ и стандартов зонного анализа»);
- кнопку ***Клонировать*** () – активна только при выборе в списке одного из стандартов. Служит для создания нового стандарта на основе выбранного в списке стандарта (см. п. 2.11.3 «Добавление стандартов »);
- кнопку ***Удалить*** () – активна при выборе в списке одного из стандартов. Служит для удаления стандарта (см. п. 2.11.8 «Удаление стандартов безопасности и стандартов зонного анализа»);
- поле ***Поиск*** – для ввода символов из имени искомого стандарта, позволяет искать в списке стандартов те из них, которые удовлетворяют введенному в поле значению.

Список стандартов зонного анализа представляет собой дерево на первом уровне которого содержится наименование стандарта, на втором – тип зон сети (*Глобальные адреса, Внутренние адреса*), указанных в параметрах требований стандарта, и на третьем уровне – наименования зон сети, указанных в параметрах требований стандарта. В нижней части панели списка зонного анализа отображается общее количество стандартов зонного анализа.

Область настройки параметров стандартов зонного анализа содержит список требований стандарта, выбранного в панели списка стандартов, и в заголовке области:

- кнопку ***Требование*** () – активна всегда. Предназначена для создания нового требования или для копирования требований из существующего стандарта зонного анализа. При нажатии кнопки раскрывается меню с пунктами ***Создать новое*** и ***Скопировать из стандарта***. При выборе пункта ***Создать новое*** открывается окно **Новое требование**, при выборе пункта ***Скопировать из стандарта*** – окно **Выбор требований**, в котором возможно выбрать существующие требования для добавления в новый стандарт (см. п. 2.11.4 «Добавление требований в стандарты безопасности и стандарты зонного анализа»);
- кнопку ***Импорт*** () – активна всегда. Предназначена для импорта требований пользовательского стандарта из файла формата XML. При нажатии на нее открывается стандартное окно используемой ОС для выбора требуемого файла (см. п. 2.11.4.4 «Добавление требований в

стандарт безопасности МЭ или зонного анализа путем импорта требований»);

- кнопку ***Выбрать*** ( ) – предназначена для перехода в форму выбора требований для экспорта в файл формата XML или удаления (рис. 109);
- кнопку ***Профили*** ( ) – предназначена для перехода в окно настройки использования стандарта зонного анализа (см. п. 2.11.5 «Настройка использования стандартов безопасности и стандартов зонного анализа»).

Примечание – При отсутствии для стандарта зонного анализа МЭ требований, кнопка ***Профили*** ( ) неактивна, настройка использования стандарта зонного анализа МЭ не доступна.

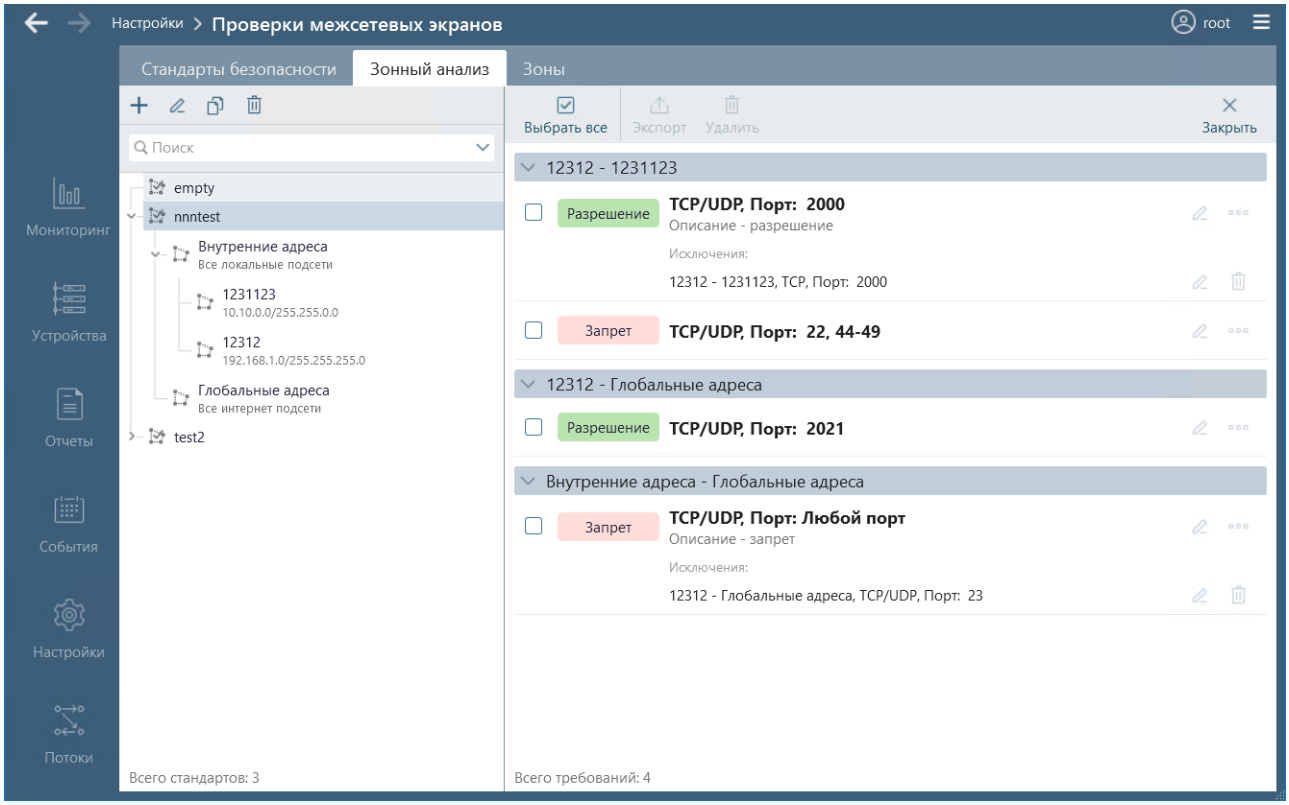


Рисунок 109 – Форма выбора требований стандарта зонного анализа для экспорта в файл формата XML или удаления

Форма выбора требований стандарта и экспорта в файл формата XML содержит кнопки:

- ***Выбрать все*** ( ) – для выбора всех требований выделенного в списке стандарта и экспорта их в файл формата XML или удаления;
- ***Экспорт*** ( ) – активна только после выбора в форме хотя бы одного требования. Предназначена для экспорта требований в файл формата XML (см. п. 2.11.7 «Экспорт требований стандарта безопасности МЭ или зонного анализа»);
- ***Удалить*** ( ) – активна только после выбора в форме хотя бы одного требования. Служит для удаления выбранных требований (см.

п. 2.11.6.3 «Удаление требований и исключений из стандартов безопасности и стандартов зонного анализа»);

- ***Закрыть*** () – предназначена для закрытия формы выбора требований.

Для каждого требования в области настройки параметров стандартов зонного анализа отображаются заданные в нем параметры: тип требования (*Запрет*, *Разрешение*), протокол и порт, описание и параметры исключений (при их наличии). Требования сгруппированы по заданным в требованиях парам источник-получатель.

Каждому требованию и исключению соответствует кнопка ***Изменить*** (), предназначенная для перехода в окно редактирования параметров требования/исключения (см. п. 2.11.6 «Изменение стандартов безопасности МЭ и стандартов зонного анализа»). Кроме того, каждому требованию соответствует кнопка ***Меню*** (), по нажатию которой раскрывается меню с пунктами:

- ***Добавить исключение*** – для перехода в окно добавления исключения к требованию (см. п. 2.11.4.5 «Добавление исключений в настройки требования стандарта зонного анализа»);
- ***Удалить*** – для удаления соответствующего требования (см. п. 2.11.6.3 «Удаление требований и исключений из стандартов безопасности и стандартов зонного анализа»).

Каждому исключению также соответствует кнопка ***Удалить*** () – для удаления исключения требования. Правила удаления исключения аналогичны правилам удаления требований и приведены в пункте 2.11.6.3 «Удаление требований и исключений из стандартов безопасности и стандартов зонного анализа».

В нижней части области настройки параметров стандартов зонного анализа отображается общее количество требований стандарта зонного анализа, выбранного в панели списка стандартов зонного анализа.

При отсутствии требований в области настройки параметров стандартов отображаются кнопки ***Скопировать из стандарта*** и ***Создать новое требование*** дублирующие кнопку ***Требование*** ().

2.11.1.3. Просмотр списка зон сети

Вкладка ***Зоны*** (рис. 110) предназначена для ведения списка контролируемых сервером ПК зон сети и задания параметров зон сети.

Вкладка содержит список зон сети, созданных пользователями и импортированных с устройств (при включенном режиме синхронизации зон и наличии на устройстве включенного отчета *Зоны*).

Заголовок вкладки содержит:

- кнопку ***Зона*** () – для перехода в окно **Новая зона** для задания вручную параметров новой контролируемой зоны;
- кнопку ***Синхронизация зон*** () – для перехода в окно включения/отключения режима синхронизации зон;

- кнопку ***Фильтр*** () – для перехода в окно фильтрации списка зон по типу зоны (импортированная/не импортированная) и источнику импорта (при их наличии) и сброса настройки фильтра;
- поле поиска зон.

Добавленные вручную и автоматически (в режиме синхронизации зон) зоны сети доступны для выбора при создании/редактировании стандартов безопасности МЭ и стандартов зонного анализа, клонирования и удаления. Добавленные вручную зоны сети доступны для внесения изменений, добавленные автоматически зоны сети доступны для просмотра параметров.

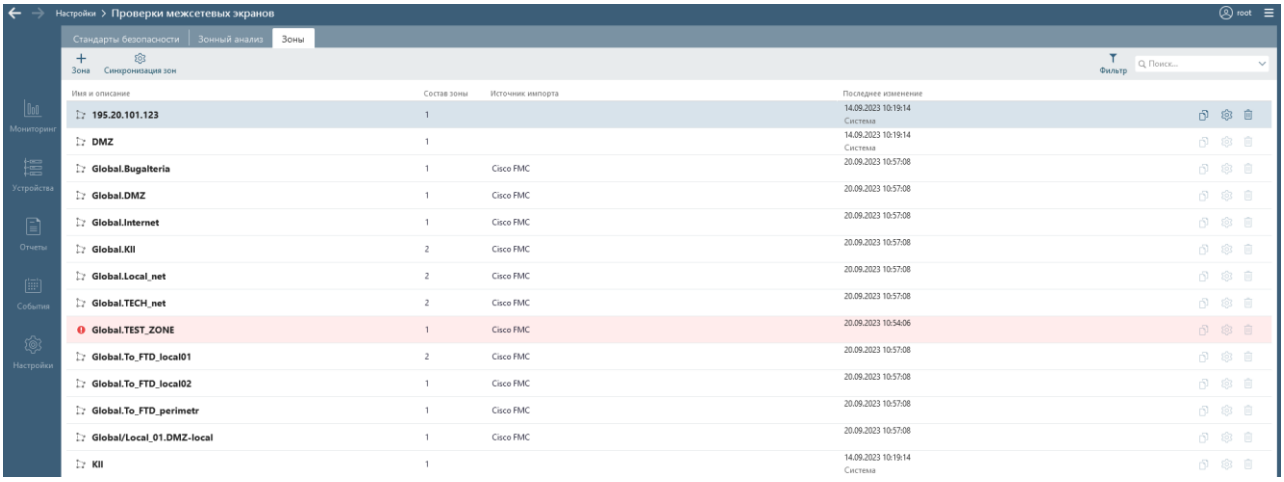


Рисунок 110 – Вкладка ***Зоны***

В нижней части вкладки отображается общее количество зон сети.

Для каждой зоны в списке отображаются параметры:

- имя и описание зоны;
- количество элементов сети зоны;
- наименование источника импорта (для импортированных зон);
- дата и время внесения последнего изменения в параметры зоны и логин пользователя, внесшего изменения.

Кроме того, в строке зон доступны кнопки:

- ***Копировать*** () – для перехода в окно создания зоны вручную путем копирования и редактирования параметров исходной зоны;
- ***Настройка*** () – для редактирования параметров созданной ранее зоны;
- ***Удалить*** () – для удаления зоны.

В случае удаления импортированной зоны с устройства (более не используются на устройстве), при следующей синхронизации (загрузке отчета *Зоны*) строка зоны будет выделена в списке вкладки ***Зоны*** розовым цветом фона (см. рис. 106).

При наведении курсора на пиктограмму «»отобразится всплывающее окно с информацией о причине выделения зоны в списке (рис. 111).

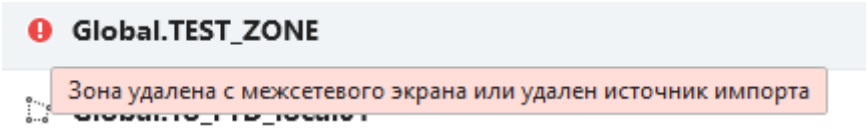


Рисунок 111 – Причина выделения зоны в списке

При удалении устройства из комплекса, все зоны импортированные с данного устройства также автоматически выделяются в списке (рис. 112).

Автоматически такие зоны не удаляются. При необходимости, пользователь должен их удалить самостоятельно. (см. п. 2.11.2.5 «Удаление зон сети»).

Правила ведения списка зон сети приведены в п. 2.11.2 «Ведение списка зон сети».

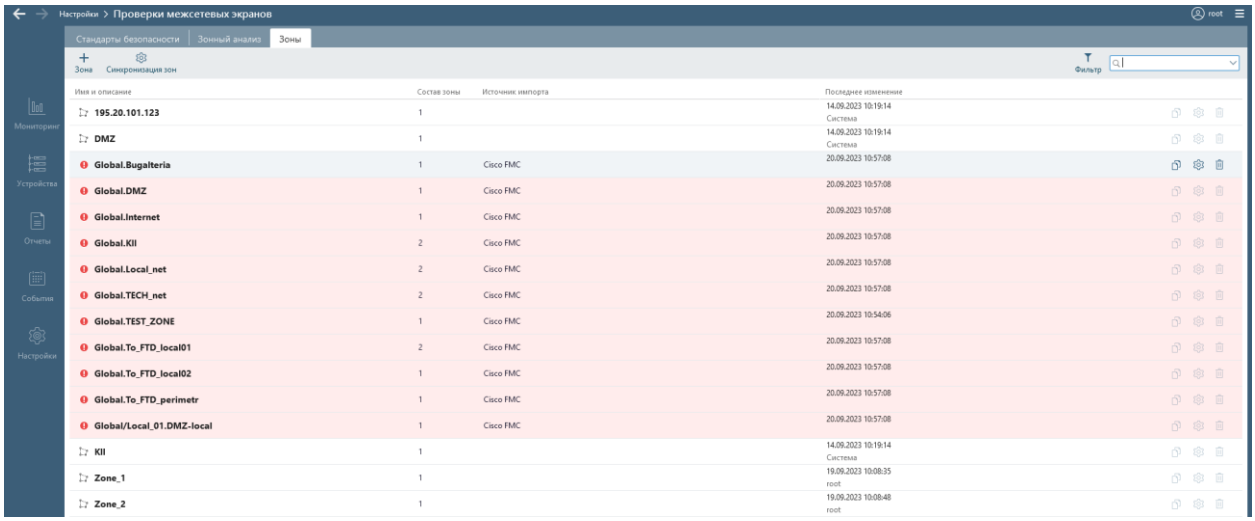


Рисунок 112 – Зоны удаленного устройства

2.11.2. Ведение списка зон сети

2.11.2.1. Добавление зон сети вручную

Для добавления на сервер ПК новой зоны сети пользователем вручную необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**.
2) Выбрать сервер, для которого добавляется зона сети.
3) В области ***Настройки контроля*** нажать кнопку ***Проверки межсетевых экранов.***
4) В открывшейся форме настройки проверок МЭ, перейти на вкладку ***Зоны*** (см. рис. 110).
5) В заголовке вкладки ***Зоны*** нажать кнопку ***Зона*** (+).
6) В открывшемся окне **Новая зона** (рис. 113, состав и описание полей окна приведены в таблице 30) заполнить необходимые поля и нажать кнопку ***Сохранить***.
7) Произойдет возврат во вкладку ***Зоны***, в которой отобразятся данные добавленной зоны (см. рис. 110).

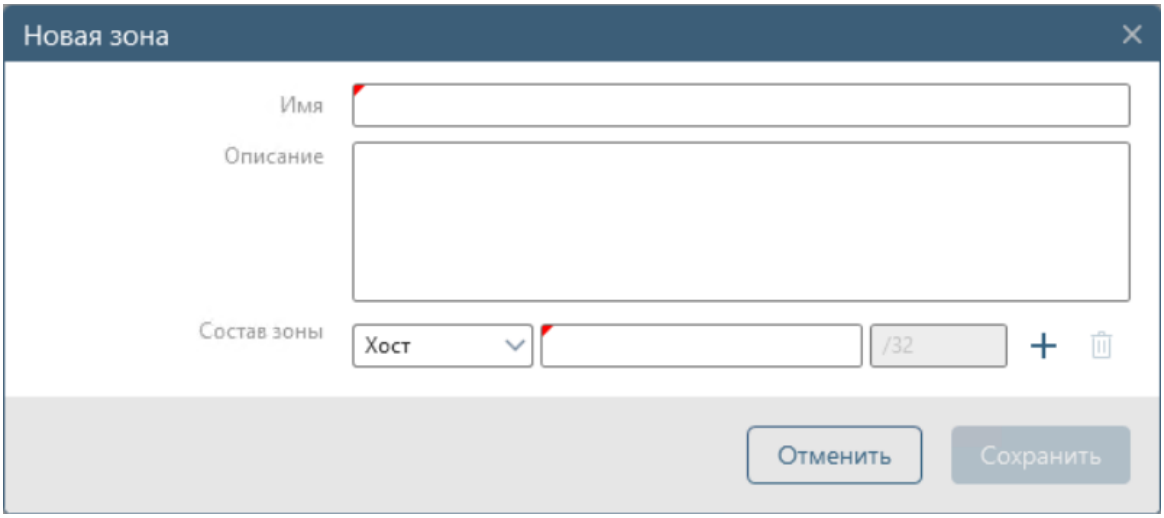


Рисунок 113 – Окно **Новая зона**

Таблица 30 – Состав и описание полей окна создания новой зоны

Поле	Описание/Назначение
Имя	Наименование создаваемой зоны. Имя новой зоны должно быть уникальным, т.е. запрещено повторять имена уже существующих на сервере ПК зон. Поле обязательно к заполнению
Описание	Описание зоны
Состав зоны Тип	Предназначено для ввода параметров входящих в зону элементов сети. Содержит: – поле со списком для выбора типа контролируемой зоны сети: *Хост*, *Подсеть* или *Диапазон*. По умолчанию выбран тип *Хост*; – поле для ввода IP-адреса хоста, подсети или два поля для ввода начального и конечного IP-адресов диапазона сети; – поле со списком для выбора подсети к указанному IP-адресу; – кнопку **Добавить** (+) – для добавления строки с полями ввода параметров элемента сети; – кнопку **Удалить** (🗑) – для удаления элемента сети

2.11.2.2. Добавление зон сети путем импортирования с устройств

Для добавления на сервер ПК зон сети путем импортирования с устройств необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**.
2) Выбрать сервер, для которого добавляется зона сети.
3) В области ***Настройки контроля*** нажать кнопку ***Проверки межсетевых экранов.***
4) В открывшейся форме настройки проверок МЭ, перейти на вкладку ***Зоны*** (см. рис. 110).
5) В заголовке вкладки ***Зоны*** нажать кнопку ***Синхронизация зон*** (⚙).
6) В открывшемся окне **Синхронизация зон** (рис. 114) установить флаг в поле **Разрешить синхронизацию зон**.
7) Нажать кнопку ***Сохранить***.

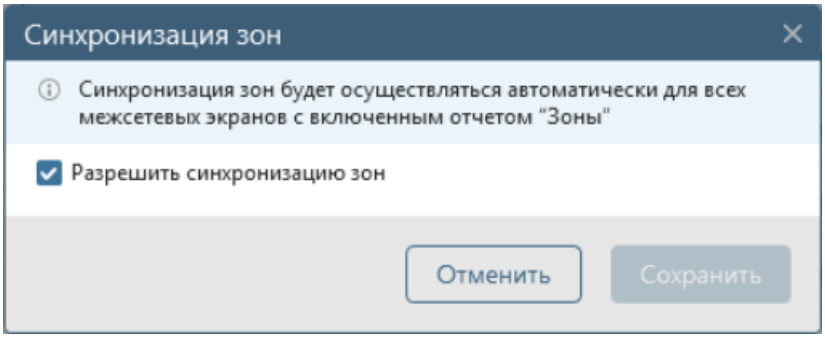


Рисунок 114 – Окно **Синхронизация зон**

При включенном режиме синхронизации зон в список вкладки ***Зоны*** будут автоматически добавляться зоны подключенных к серверу ПК устройств с включенным отчетом *Зоны* при загрузке соответствующего отчета.

2.11.2.3. Добавление зон сети путем копирования имеющейся зоны сети

На основе имеющихся во вкладке ***Зоны*** зон сети можно создать (клонировать) новую зону сети. Для клонирования зоны сети необходимо выполнить следующие действия в клиентской консоли комплекса:

1) Перейти в раздел **Настройки**.
2) Выбрать сервер, для которого добавляется зона сети.
3) В области ***Настройки контроля*** нажать кнопку ***Проверки межсетевых экранов.***
4) В открывшейся форме настройки проверок МЭ, перейти на вкладку ***Зоны*** (см. рис. 110).
5) Нажать в строке исходной зоны сети кнопку ***Копировать*** ().
6) В открывшемся окне клонирования зоны сети (аналогично окну создания зоны сети вручную (см. рис. 113), описание полей окна приведено в таблице 30) внести требуемые изменения в параметры исходной зоны.
7) Нажать кнопку ***Сохранить***, окно закроется, в списке зон сети появится строка новой зоны.

2.11.2.4. Редактирование зон сети

Созданные вручную зоны во вкладке ***Зоны*** можно изменить, для чего – нажать в строке зоны кнопку ***Настройка*** (), внести требуемые изменения в открывшемся окне изменения параметров зоны (рис. 115) и нажать кнопку ***Сохранить***.

Добавленные автоматически зоны не доступны для редактирования, по нажатию кнопки ***Настройка*** () открывается окно просмотра параметров зоны (рис. 116). Поля *Источник импорта зоны* и *Привязанные объекты* служат для информации, а именно, с какого устройства зона была импортирована и к каким объектам (устройство и его интерфейсы) относится состав зоны.

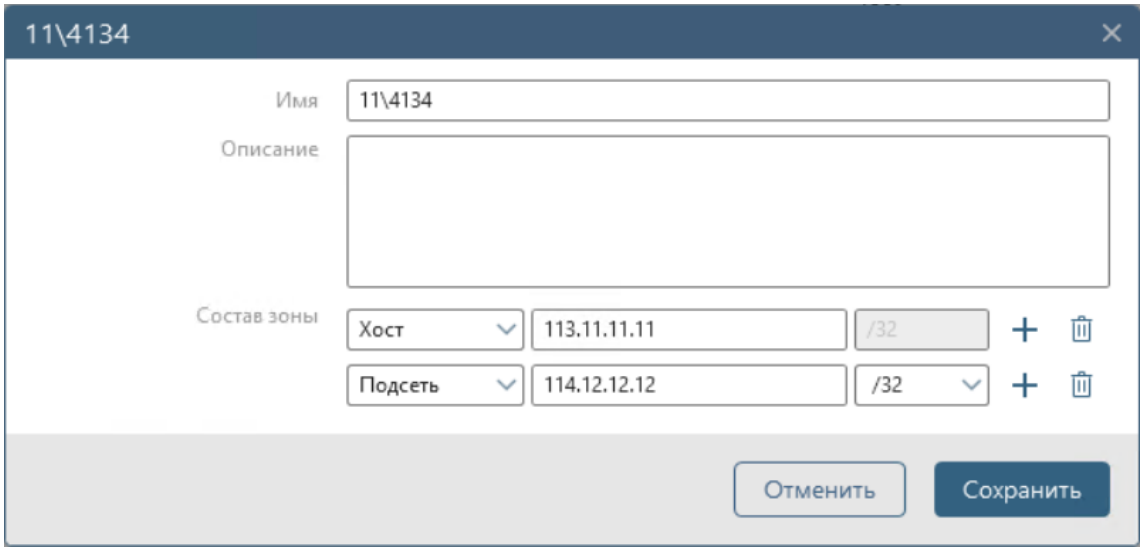


Рисунок 115 – Окно изменения параметров зоны

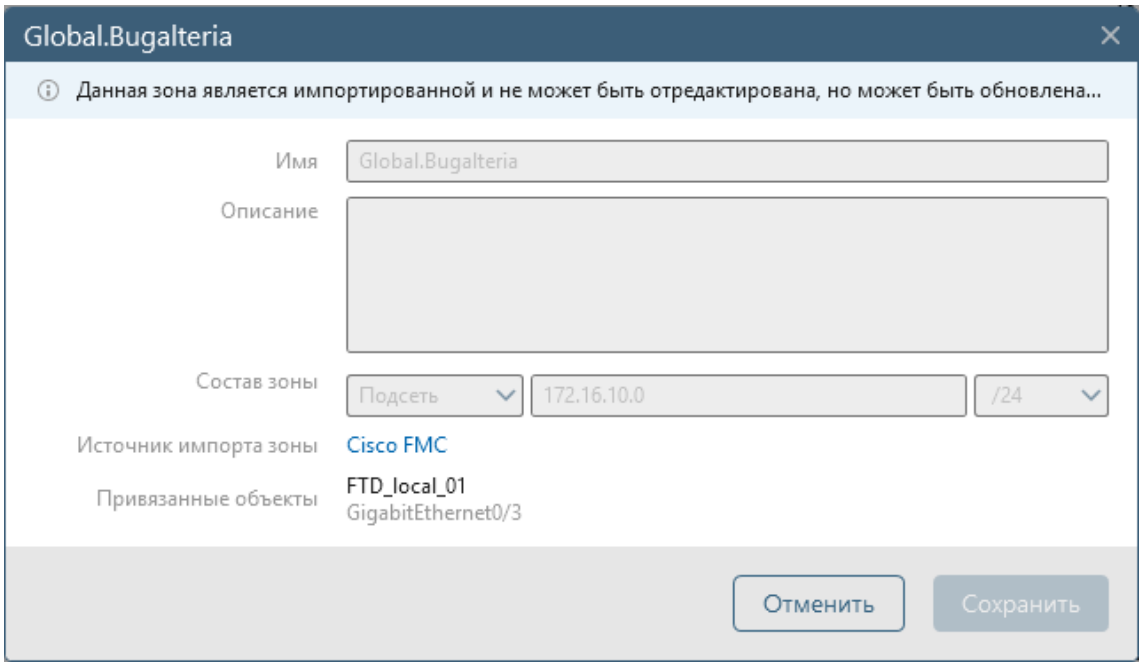


Рисунок 116 – Окно просмотра параметров зоны

2.11.2.5. Удаление зон сети

Для удаления зоны сети (импортированной и добавленной вручную) необходимо нажать в строке зоны кнопку ***Удалить*** (). Если для удаляемой зоны в стандартах безопасности и зонного анализа МЭ есть требования контроля наличия/отсутствия правил МЭ, то в открывшемся окне подтверждения удаления зоны (рис. 117) отобразится перечень таких требований. Для подтверждения удаления зоны необходимо нажать в окне **Удаление** кнопку ***Удалить***. После подтверждения зона будет удалена из списка вкладки ***Зоны***, и из стандартов безопасности и зонного анализа МЭ будут удалены связанные с ней требования.

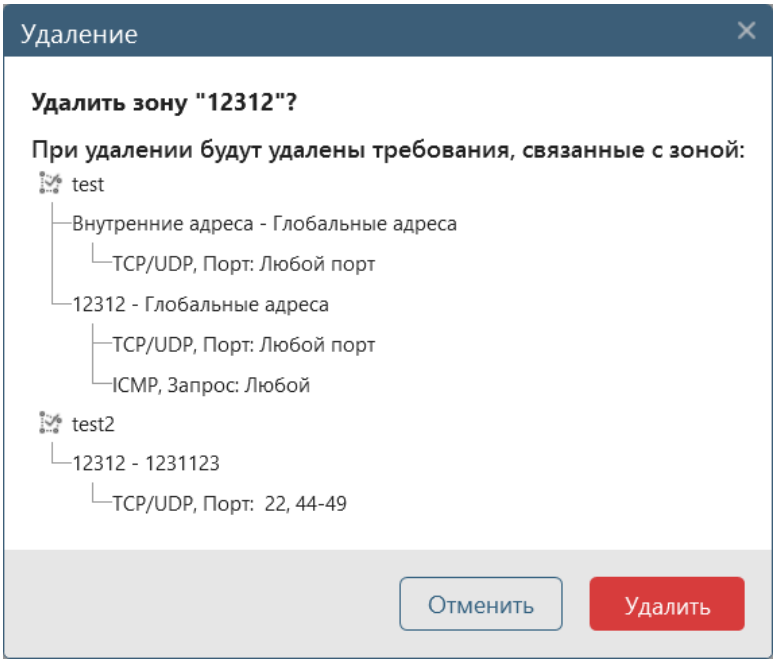


Рисунок 117 – Окно **Удаление зоны**

При удалении добавленной автоматически зоны, если устройство, с которого зона импортирована, не удалено и на нем зона не удалена, при включенном режиме синхронизации она вновь будет автоматически добавлена.

2.11.3. Добавление стандартов безопасности и зонного анализа МЭ

Для добавления стандарта безопасности или стандарта зонного анализа МЭ необходимо выполнить следующие действия:

1) Перейти в разделе **Проверки межсетевых экранов** во вкладку соответственно ***Стандарты безопасности*** или ***Зонный анализ*** и нажать в панели кнопок списка стандартов кнопку ***Добавить стандарт*** (+).

2) В открывшемся окне **Новый стандарт безопасности МЭ/зонного анализа** (рис. 118, состав и описание полей окна приведены в таблице 31) заполнить необходимые поля.

3) Нажать кнопку ***Сохранить.***

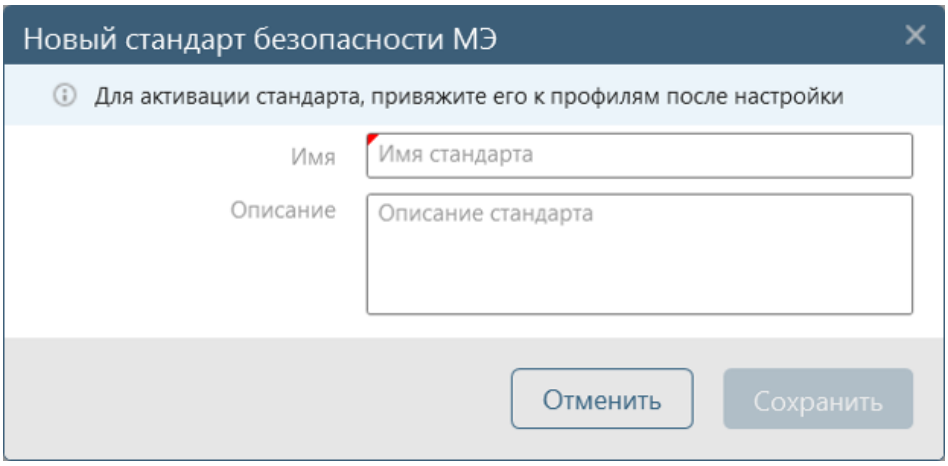


Рисунок 118 – Окно **Новый стандарт безопасности МЭ**

Таблица 31 – Состав и описание полей окна создания нового стандарта безопасности МЭ/зонного анализа

Поле	Описание/Назначение
Имя	Наименование создаваемого стандарта. Поле обязательно к заполнению. Имя стандарта должно быть уникальным
Описание	Текстовое поле для ввода описания создаваемого стандарта

Добавленный стандарт не содержит требований. Необходимо добавить требования в созданный стандарт (см. п. 2.11.4 «Добавление требований в стандарты безопасности и стандарты зонного анализа») и задать параметры режима его использования на контролируемых на сервере ПК устройствах (см. п. 2.11.5 «Настройка использования стандартов безопасности и стандартов зонного анализа»).

После добавления в пользовательский стандарт безопасности МЭ/зонного анализа требований, их можно отредактировать с использованием инструментов вкладки ***Стандарты безопасности/Зонный анализ*** (изменение имени и описания стандарта) и области настройки параметров стандартов (изменение источника и получателя трафика, протокола обмена данными, порта для обмена данными, добавление исключений для требований, входящих в добавленный стандарт, добавление и редактирование описания) (см. п. 2.11.6 «Изменение стандартов безопасности МЭ и стандартов зонного анализа»).

Создание пользовательского стандарта безопасности МЭ/зонного анализа возможно также путем клонирования имеющегося стандарта соответствующего типа, для чего необходимо:

1) Перейти в разделе **Проверки межсетевых экранов** во вкладку соответственно ***Стандарты безопасности*** или ***Зонный анализ*** и нажать в панели кнопок списка стандартов кнопку ***Клонировать*** ( ).

2) В открывшемся окне создания копии выбранного в панели списка стандарта (аналогично окну создания нового стандарта безопасности МЭ/зонного анализа (см. рис. 118)) внести изменения в имя и описание создаваемого стандарта.

3) Нажать кнопку ***Сохранить***

Примечание – Имя стандарта должно быть обязательно изменено (не допускается наличие дубликатов стандартов безопасности МЭ/зонного анализа).

Созданный путем клонирования стандарт будет содержать все требования исходного стандарта. После копирования можно отредактировать параметры созданного стандарта с использованием инструментов вкладки ***Стандарты безопасности*** или ***Зонный анализ*** (изменение имени и описания стандарта) и области настройки требований (изменение типа (для требований стандартов зонного анализа), имени, описания, категории, добавление исключений для требований, входящих в созданный стандарт).

2.11.4. Добавление требований в стандарты безопасности и стандарты зонного анализа

Правила проверок МЭ формируются требованиями, содержащимися в стандартах безопасности и стандартах зонного анализа. Добавление требований в стандарты возможно путем:

– создания вручную новых пользовательских требований;

– копирования требований из существующих стандартов соответствующего типа;

– импорта требований из файлов формата XML;

– в стандартах безопасности дополнительно – клонирования требований с их обязательной корректировкой (наличие полных дубликатов требований не допускается);

Добавленное требование доступно для редактирования с использованием инструментов панели списка вкладки (изменение имени и описания требования) и области настройки параметров стандартов (изменение параметров требования) (см. п. 2.11.6 «Изменение стандартов безопасности МЭ и стандартов зонного анализа»), а также требования стандартов зонного анализа доступны для добавления исключений (см. п. 2.11.4.5 «Добавление исключений в настройки требования стандарта зонного анализа»).

2.11.4.1. Добавление в стандарт безопасности МЭ нового требования вручную и копированием

Для создания вручную нового шаблона пользовательского требования и добавления его в стандарт безопасности МЭ необходимо:

1) Выбрать в списке стандартов безопасности вкладки ***Стандарты безопасности*** требуемый стандарт.

2) Нажать в заголовке рабочей области вкладки кнопку ***Требование*** (+▾) и в раскрывшемся списке выбрать пункт ***Создать новое.***

3) В открывшемся окне **Требование стандарта безопасности МЭ** (рис. 119) заполнить поля ***Имя*** и ***Описание***, задать в соответствии с таблицей 32 параметры требования.

Примечание – Значение *Не учитывать* может быть задано не более чем для двух параметров требования.

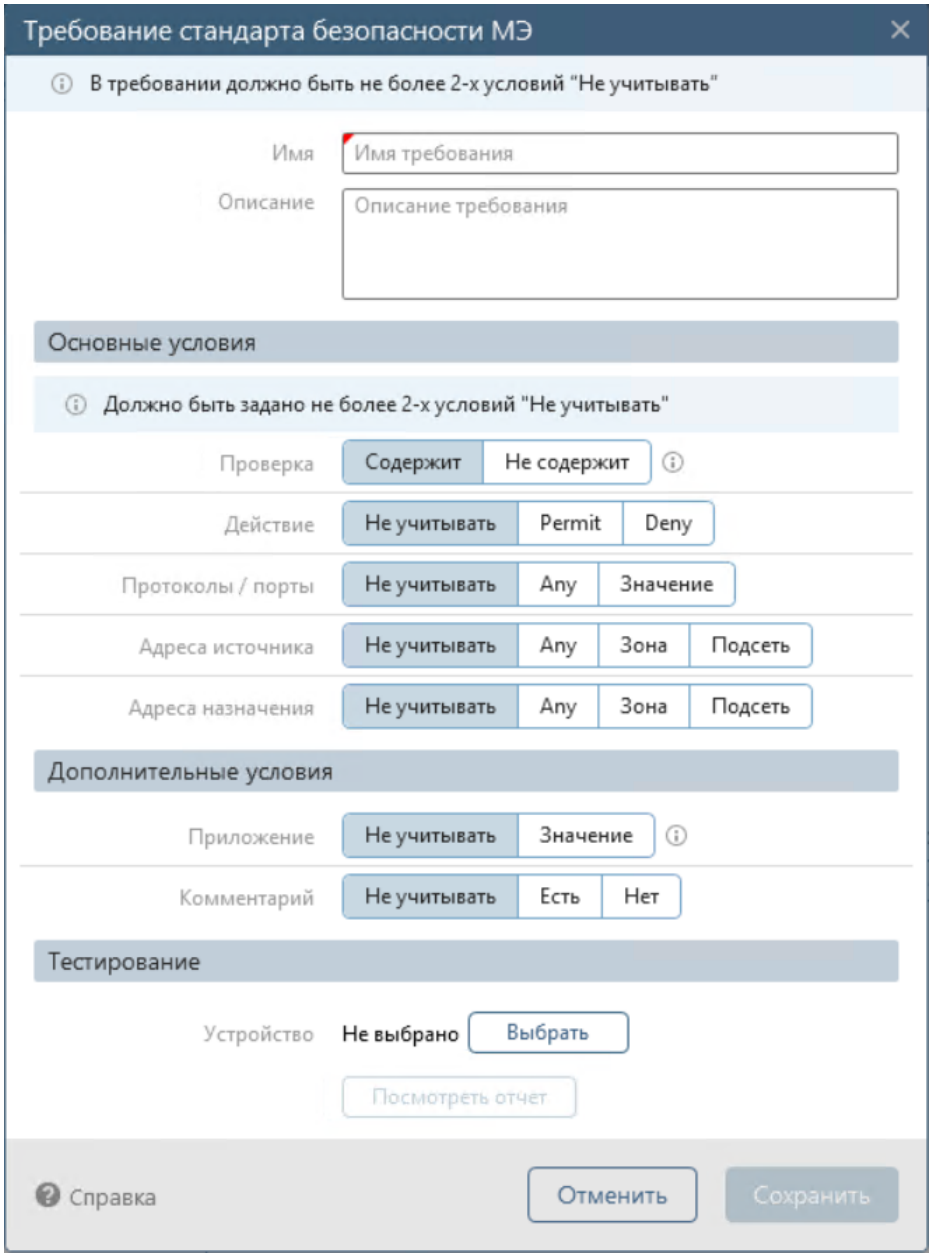


Рисунок 119 – Окно **Требование стандарта безопасности МЭ**

Таблица 32 – Состав и описание полей окна **Требование стандарта безопасности МЭ**

Поле	Описание/Назначение
Имя	Наименование создаваемого требования. Поле обязательно к заполнению. Имя требования должно быть уникальным
Описание	Текстовое поле для ввода описания создаваемого требования
Блок ***Основные условия***	
Проверка	Переключатель для выбора типа проверки *Содержит* или *Не содержит*. При выборе значения: – *Содержит* – нарушением является отсутствие правил в политике, удовлетворяющих условиям проверки. Если есть хотя бы одно правило, удовлетворяющее условиям проверки по параметрам

Поле	Описание/Назначение
	Действие, *Протоколы/порты*, *Адреса источника*, *Адреса назначения*, *Комментарий,* значит нарушения нет; – *Не содержит* – нарушением являются правила, которые удовлетворяют условиям проверки по параметрам *Действие, Протоколы/порты, Адреса источника, Адреса назначения, Комментарий*
Действие	Переключатель для выбора режима учета правил с указанным действием. При выборе значения: – *Не учитывать* – проверка удовлетворяет условию по данному параметру независимо от значения действия правила; – *Permit* – проверка не удовлетворяет условию, если действие правила не является *Permit*; – *Deny* – проверка не удовлетворяет условию, если действие правила не является *Deny*
Протоколы/порты	Переключатель для выбора режима учета правил с указанными протоколами/портами. При выборе значения: – *Не учитывать* – проверка удовлетворяет условию по данному параметру независимо от значения протоколов/портов правила; – *Any* – проверка удовлетворяет условию, только если протокол правила имеет значение *Any*; – *Значение* – результат выполнения условия зависит от положения переключателя ***Проверка***: • для *Содержит* – проверка удовлетворяет условию только, если правило содержит все указанные в проверке значения для протоколов/портов; • для *Не содержит* – проверка не удовлетворяет условию, если есть пересечение с протоколами/портами правила. После выбора значения *Значение* в окне дополнительно отображаются поля (рис. 120) выбора протоколов (*TCP*, *UDP*, *TCP/UDP*, *ICMP* или *Другой протокол*), ввода портов проверки и исключений портов (для протоколов *TCP*, *UDP, TCP/UDP)* или ввода номера IP-протокола (для *Другой протокол*). Примечание – Справа от полей ввода портов и исключений портов проверки расположена кнопка ***Информация*** (ⓘ), по нажатию которой открывается окно с правилами заполнения поля. При выборе значения *Другой протокол* подсказка содержит ссылку на таблицу интернет-протоколов транспортного уровня с соответствующими им номерами
Адреса источника	Переключатель для выбора режима учета правил с указанными адресами источника. При выборе значения: – *Не учитывать* – проверка удовлетворяет условию по данному параметру независимо от значения адреса источника правила; – *Any* – проверка удовлетворяет условию, только если адрес источника правила имеет значение Any; – *Зона* и *Подсеть* – результат выполнения условия зависит от

Поле	Описание/Назначение
	положения переключателя ***Проверка***: • для *Содержит* – проверка удовлетворяет условию, только если правило содержит все указанные в проверке значения для адресов источника; • для *Не содержит* – проверка не удовлетворяет условию, если есть пересечение с адресами источника правила; После выбора значения *Зона* в окне дополнительно отображается поле (см. рис. 117) выбора зоны сети (из списка контролируемых зон сети вкладки ***Зоны***). После выбора зоны: 1. Справа от поля активной становится кнопка ***Просмотреть*** (), по нажатию которой открывается подсказка, содержащая адрес и маску адреса хоста/подсети зоны. 2. Активной становится кнопка ***Добавить исключение***, по нажатию которой добавляется поле выбора исключения (рис. 121). Поле содержит список зон, входящих в основную зону, и кнопки: • ***Просмотреть*** *()* – кнопка становится активна только после выбора зоны-исключения, по нажатию кнопки открывается подсказка, содержащая адрес и маску адреса хоста/подсети зоны; • ***Добавить*** (+) – для добавления поля выбора следующего исключения; • ***Удалить*** *()*.– для удаления исключения. После выбора значения *Подсеть* в окне дополнительно отображаются поля (аналогично полю ***Адреса назначения***, см. рис. 106): 1. ***Адрес устройства*** – при установке в поле флага используются адреса интерфейсов, к которым привязаны исходящие политики. Если к исходящей политике не привязаны интерфейсы, то она работает для всех интерфейсов. Результат выполнения условия зависит от положения переключателя *Проверка*: • для *Содержит* – проверка удовлетворяет условию, только если правило содержит адреса интерфейсов; • для *Не содержит* – проверка не удовлетворяет условию, если есть пересечение с адресами интерфейсов. 2. Поле для ввода адресов подсетей/диапазонов адресов/адресов хостов. 3. Поле для ввода исключения адресов в виде адресов подсетей/диапазонов адресов/адресов хостов. Адреса исключений не должны выходить за рамки основных адресов
Адреса назначения	Переключатель для выбора режима учета правил с указанными адресами назначения. Правила выбора значения переключателя и заполнения дополнительных полей аналогичны полю ***Адреса источника***
Блок ***Дополнительные условия***	
Приложение	Переключатель для выбора режима учета правил с приложениями. При выборе значения:

Поле	Описание/Назначение
	– *Не учитывать* – проверка удовлетворяет условию по данному параметру независимо от приложений; – *Значение* – результат выполнения условия зависит от положения переключателя ***Проверка***: • для *Содержит* – проверка удовлетворяет условию только, если правило содержит хотя бы одно указанное в проверке приложение; • для *Не содержит* – проверка не удовлетворяет условию, если правило не содержит ни одного указанного в проверке приложения. После выбора значения *Значение* в окне дополнительно отображаются (см. рис. 117); – 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 режима учета наличия комментария. При выборе значения: – *Не учитывать* – проверка удовлетворяет условию по данному параметру независимо от наличия комментария к правилу ACL (при этом не важно поддерживаются на устройстве комментарии к правилам или нет); – *Есть* – проверка удовлетворяет условию только при наличии комментария к правилу ACL; – *Нет* – проверка удовлетворяет условию только при отсутствии комментария к правилу ACL
Блок ***Тестирование***	
Устройство	Для выполнения тестового запуска отчета на выбранном в поле ***Устройство*** устройстве. Окно выбора устройства открывается по нажатию кнопки ***Выбрать***. Выбор устройства выполняется путем установки курсора в строке с наименованием требуемого устройства. После нажатия в окне выбора устройства кнопки ***Выбрать*** наименование выбранного устройства отображается в поле ***Устройство*** блока ***Тестирование***. Запуск отчета выполняется после выбора устройства по нажатию кнопки ***Посмотреть отчет***. Отчет содержит перечень правил для указанного устройства, удовлетворяющих заданным параметрам требования

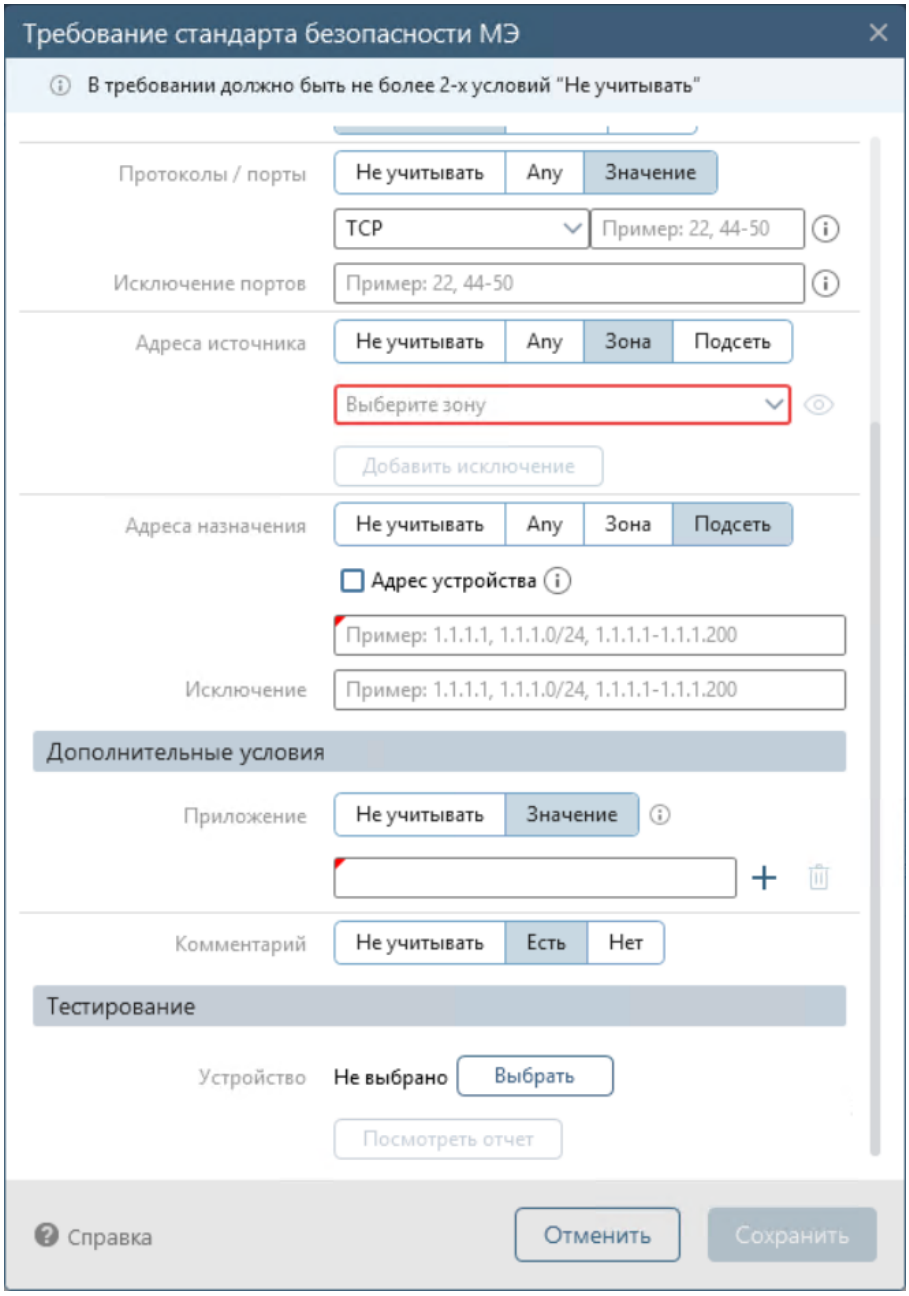


Рисунок 120 – Окно **Требование стандарта безопасности МЭ** с дополнительными полями

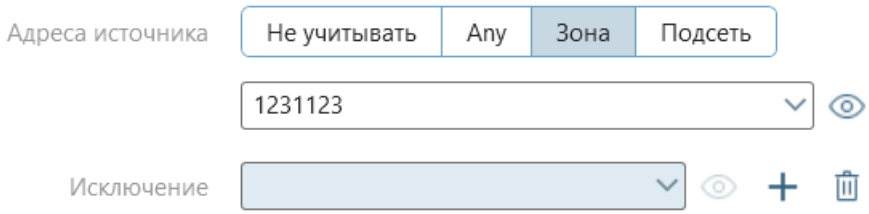


Рисунок 121 – Добавление исключения для адреса источника типа *Зона*

4) Выполнить при необходимости тестовый запуск отчета по сформированному требованию. Внести при необходимости корректировки в параметры требования по результатам тестирования.

5) Нажать кнопку ***Сохранить.*** Произойдет возврат на вкладку ***Стандарты безопасности*** формы настройки проверок МЭ. На вкладке в области настройки требований появится новое требование для выбранного на шаге 1 стандарта

Примечание – При нажатии в окне **Требование стандарта безопасности МЭ** кнопки ***Отменить*** произойдет возврат на вкладку ***Стандарты безопасности*** без добавления нового требования.

Для добавления требования путем копирования имеющегося в стандарте безопасности МЭ требования необходимо:

1) В панели списка стандартов вкладки ***Стандарты безопасности*** выделить необходимый стандарт.
2) В области настройки параметров стандартов безопасности нажать в строке копируемого требования кнопку ***Клонировать*** (). Откроется окно **Требование стандарта безопасности МЭ,** аналогичное окну добавления нового требования (см. рис. 119), с параметрами исходного требования.
3) Внести в соответствии с таблицей 31 необходимые изменения в параметры требования.

Примечание – Созданное путем копирования требование должно отличаться от исходного хотя бы по одному из параметров *Проверка*, *Действие*, *Протоколы/порты*, *Адреса источника*, *Адреса назначения, Приложение, Комментарий* и не должно содержать значение *Не учитывать* более чем для двух параметров.

4) Выполнить при необходимости тестовый запуск отчета по сформированному требованию.
5) Внести при необходимости корректировки в параметры требования.
6) Нажать кнопку ***Сохранить.*** Произойдет возврат на вкладку ***Стандарты безопасности*** формы настройки проверок МЭ. На вкладке в области настройки требований появится новое требование для выбранного на шаге 1 стандарта

Примечание – При нажатии в окне **Требование стандарта безопасности МЭ** кнопки ***Отменить*** произойдет возврат на вкладку ***Стандарты безопасности*** без добавления нового требования.

2.11.4.2. Добавление в стандарт зонного анализа нового требования

Для создания нового шаблона пользовательского требования и добавления его в стандарт зонного анализа необходимо:

1) Выбрать в списке стандартов зонного анализа требуемый стандарт.
2) Нажать в заголовке рабочей области вкладки ***Зонный анализ*** кнопку ***Требование*** () и в раскрывшемся списке выбрать пункт ***Создать новое.***
3) В открывшемся окне **Новое требование** (рис. 122) указать параметры требования в соответствии с таблицей 33.

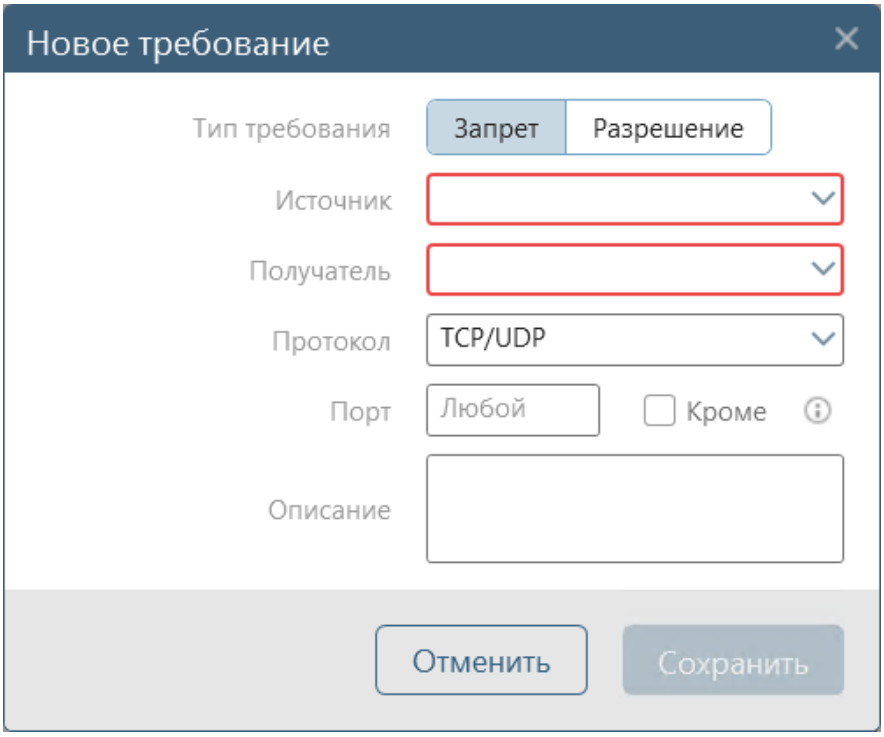


Рисунок 122 – Окно **Новое требование**

Таблица 33 – Состав и описание полей окна **Новое требование**

Поле	Описание/Назначение
Тип требования	Переключатель для выбора типа требования. При выборе значения: – *Запрет* – запрещающее требование; – *Разрешение* – разрешающее требование
Источник	Поле для выбора источника трафика (из списка контролируемых зон сети вкладки ***Зоны***)
Получатель	Поле для выбора получателя трафика (из списка контролируемых зон сети вкладки ***Зоны***)
Протокол	Поле для выбора протокола обмена данными из списка значений: *Любой протокол*, *TCP*, *UDP*, *TCP/UDP*, *ICMP* или *Другой*. При выборе протоколов *TCP*, *UDP, TCP/UDP* в окне отображаются: • поле ввода порта/портов для обмена данными; • поле для флага ***Кроме***. При установке в поле флага, проверяться будут все порты, кроме указанных. При выборе значения *Другой* в окне дополнительно отображается поле ***Номер протокола IP*** для ввода номера IP-протокола. Примечание – Справа от поля ввода портов и поля ***Номер протокола IP*** расположена кнопка ***Информация*** (ⓘ). По нажатию кнопки открывается окно с правилами заполнения поля ввода портов, либо (для поля ***Номер протокола IP***) – таблица интернет-протоколов транспортного уровня с соответствующими им номерами
Описание	Текстовое поле, в которое можно ввести описание создаваемого требования

4) Нажать кнопку ***Сохранить***. Произойдет возврат на вкладку ***Зонный анализ***. На вкладке в области настройки требований появится новое требование для выбранного на шаге 1 стандарта.

При нажатии в окне **Новое требование** кнопки ***Отменить*** произойдет возврат на вкладку ***Зонный анализ*** без добавления нового требования.

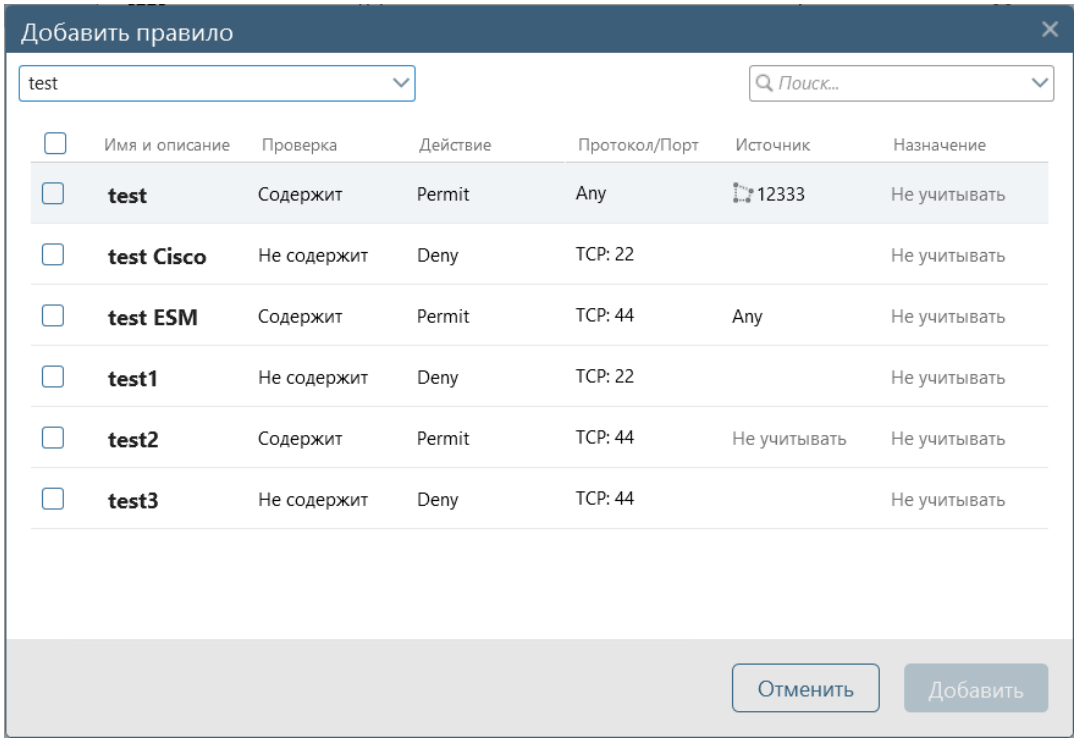
2.11.4.3. Добавление требований в стандарт безопасности МЭ или зонного анализа из базы требований

Для добавления требований в стандарт безопасности МЭ или зонного анализа с использованием базы требований существующих стандартов соответствующего типа, необходимо выполнить следующие действия:

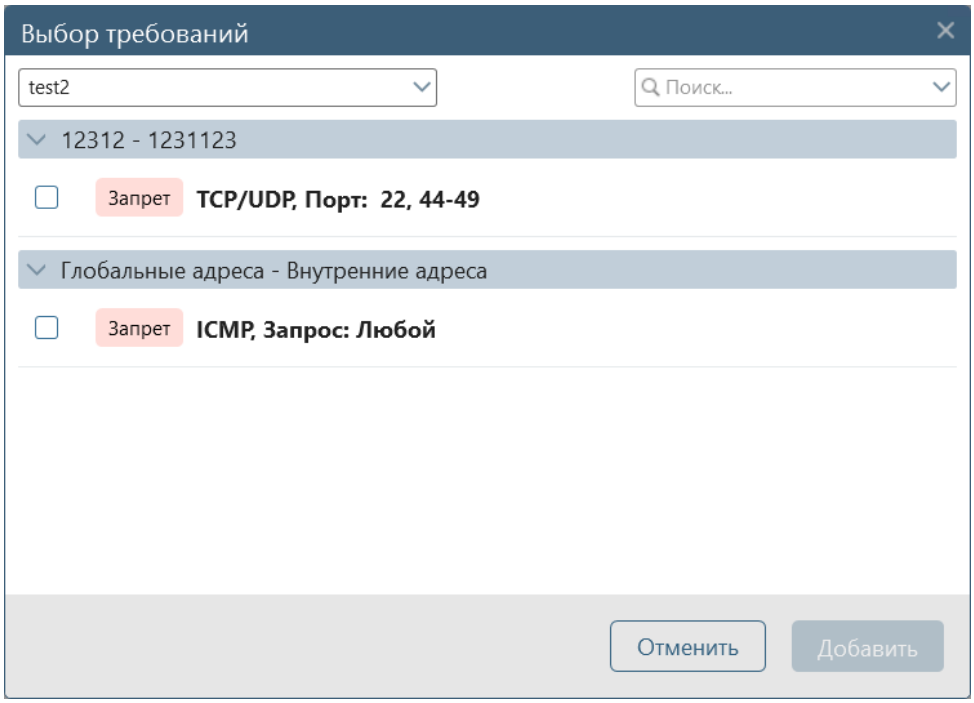
1) Перейти в раздел **Настройки**.
2) Выбрать сервер, для которого удаляется стандарт зонного анализа.
3) В области *Настройки контроля* нажать кнопку ***Проверки межсетевых экранов***.
4) Выбрать вкладку требуемого типа стандартов ***Стандарты безопасности*** или ***Зонный анализ***.
5) В панели списка стандартов выбранной вкладки выделить необходимый стандарт.
6) Нажать в заголовке рабочей области вкладки кнопку ***Требование*** () и в раскрывшемся списке выбрать пункт ***Скопировать из стандарта.***
7) В открывшемся окне (рис. 123, а – для стандартов безопасности МЭ, б – для стандартов зонного анализа) выбрать в поле выбора стандартов необходимый стандарт с копируемым требованием. Список содержит наименования созданных ранее стандартов соответственного безопасности МЭ и зонного анализа, а в окне для стандартов безопасности МЭ дополнительно – стандарт по умолчанию ***Шаблоны требований*** (рекомендуемый набор требований по безопасной настройке правил, в части проверки отсутствия небезопасных протоколов и доступа к устройству).

Примечание – Для поиска добавляемых требований окно содержит поле поиска, по мере ввода в поле символов в окне желтым цветом выделяются строки, содержащие введенные символы, и выполняется фильтрация списка требований. Для отмены фильтрации необходимо в окне поиска нажать кнопку ***Очистить*** (×).

8) Выбрать установкой флагов необходимые требования проверок для их переноса в выбранный на шаге 5 стандарт.
9) Нажать кнопку ***Добавить***. Произойдет возврат на выбранную на шаге 4 вкладку. На вкладке в области настройки требований стандарта, выбранного на шаге 5, появится новое требование, выбранное на шаге 8.



а)



б)

Рисунок 123 – Окно выбора добавляемых требований

2.11.4.4. Добавление требований в стандарт безопасности МЭ или зонного анализа путем импорта требований

Для импорта требований в стандарт безопасности МЭ или зонного анализа, сохраненных в файле формата XML при экспорте требований (см. п. 2.11.7 «Экспорт требований стандарта безопасности МЭ или зонного анализа»), необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**.

2) Выбрать сервер, для которого удаляется стандарт зонного анализа.

3) В области ***Настройки контроля*** нажать кнопку ***Проверки межсетевых экранов***.

4) Выбрать вкладку требуемого типа стандартов ***Стандарты безопасности*** или ***Зонный анализ***.

5) В панели списка стандартов выбранной вкладки выделить необходимый стандарт.

6) В заголовке области настройки параметров стандартов нажать кнопку ***Импорт*** ( ).

7) В открывшемся стандартном окне используемой ОС указать файл xml-формата, содержащий настройки импортируемого правила, и нажать кнопку ***Открыть***. В области настройки параметров появятся новые требования проверки для выбранного на шаге 5 стандарта.

В дальнейшем импортированные требования можно отредактировать (подробнее см. п. 2.11.6 «Изменение стандартов безопасности МЭ и стандартов зонного анализа»).

2.11.4.5. Добавление исключений в настройки требования стандарта зонного анализа

Для добавления исключений в настройки требований требования стандарта зонного анализа необходимо:

1) В панели списка стандартов вкладки **Зонный анализ** выделить необходимый стандарт зонного анализа.

2) В строке редактируемого требования стандарта зонного анализа нажать кнопку ***Меню*** ( ) и выбрать в раскрывшемся меню пункт ***Добавить исключение*** (рис. 124).

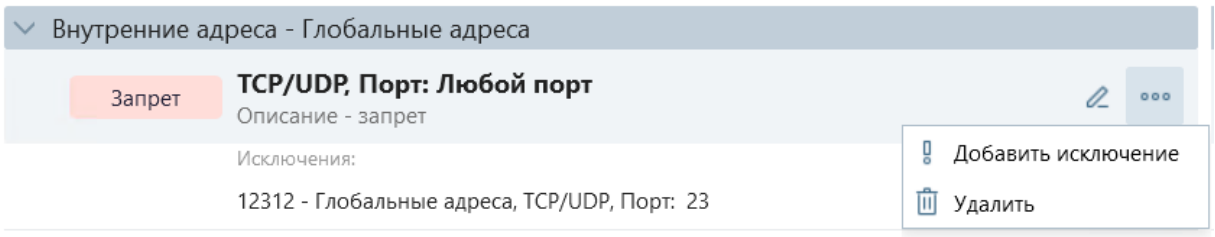


Рисунок 124 – Добавление исключений в требования стандарта зонного анализа

3) В открывшемся окне **Новое исключение** (рис. 125) выполнить настройку состава исключений в выбранном требовании.

4) Нажать кнопку ***Сохранить.***

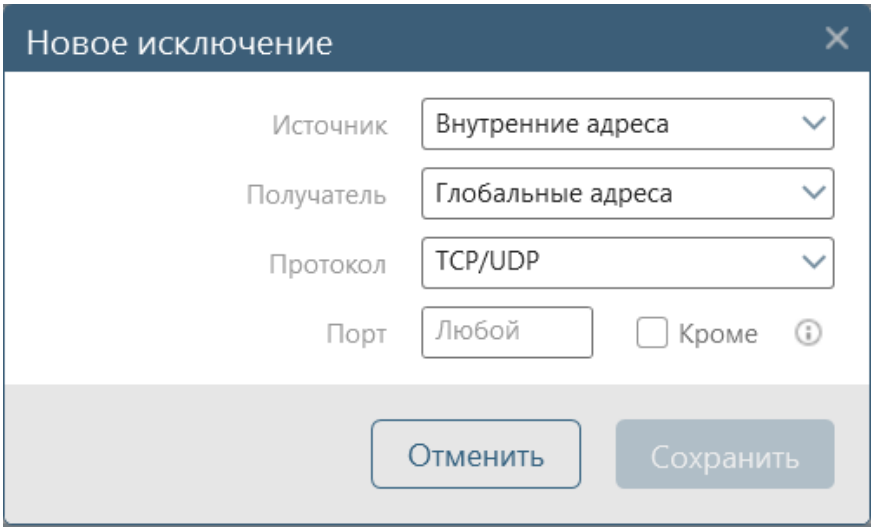


Рисунок 125 – Окно **Новое исключение**

В результате выполненных действий в области настройки параметров стандартов, в поле редактируемого требования стандарта зонного анализа появятся добавленные исключения (рис. 126). Добавленные исключения можно изменить или удалить, нажав соответственно кнопку ***Изменить*** ( ) или ***Удалить*** ( ) в строке исключения.

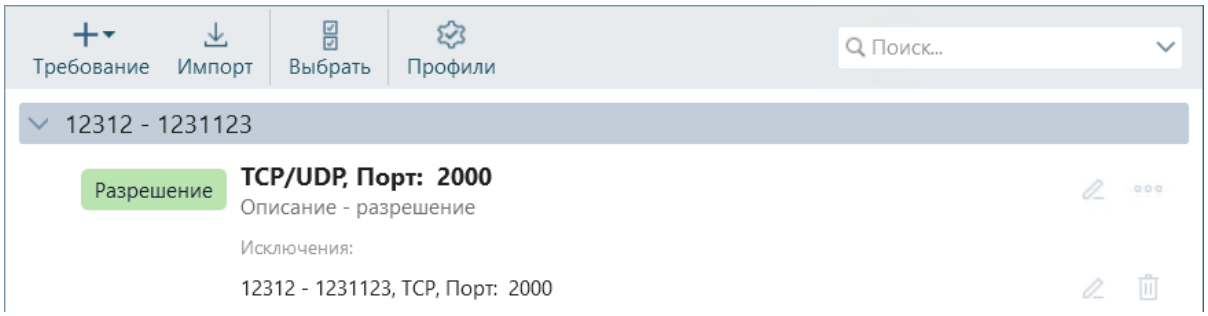


Рисунок 126 – Область настройки параметров стандартов с добавленными исключениями

2.11.5. Настройка использования стандартов безопасности и стандартов зонного анализа

Для активации добавленного стандарта необходимо после добавления в него требований и их редактирования выполнить настройку использования пользовательского стандарта. Для этого необходимо:

1) Перейти в раздел **Настройки**.
2) Выбрать сервер, для которого удаляется стандарт зонного анализа.
3) В области ***Настройки контроля*** нажать кнопку ***Проверки межсетевых экранов***.
4) Выбрать вкладку требуемого типа стандартов ***Стандарты безопасности*** или ***Зонный анализ***.
5) В панели списка стандартов выбранной вкладки выделить необходимый стандарт.
6) В заголовке открывшейся области настройки пользовательского стандарта нажать кнопку ***Профили*** ( ).

7) В открывшемся окне настройки использования стандарта для устройств, контролируемых сервером ПК, (рис. 127) выполнить настройку использования стандарта для всех устройств, к которым он может быть применен. Для этого в области *Использование* в раскрывающемся списке выбрать значение ***Разрешено***.

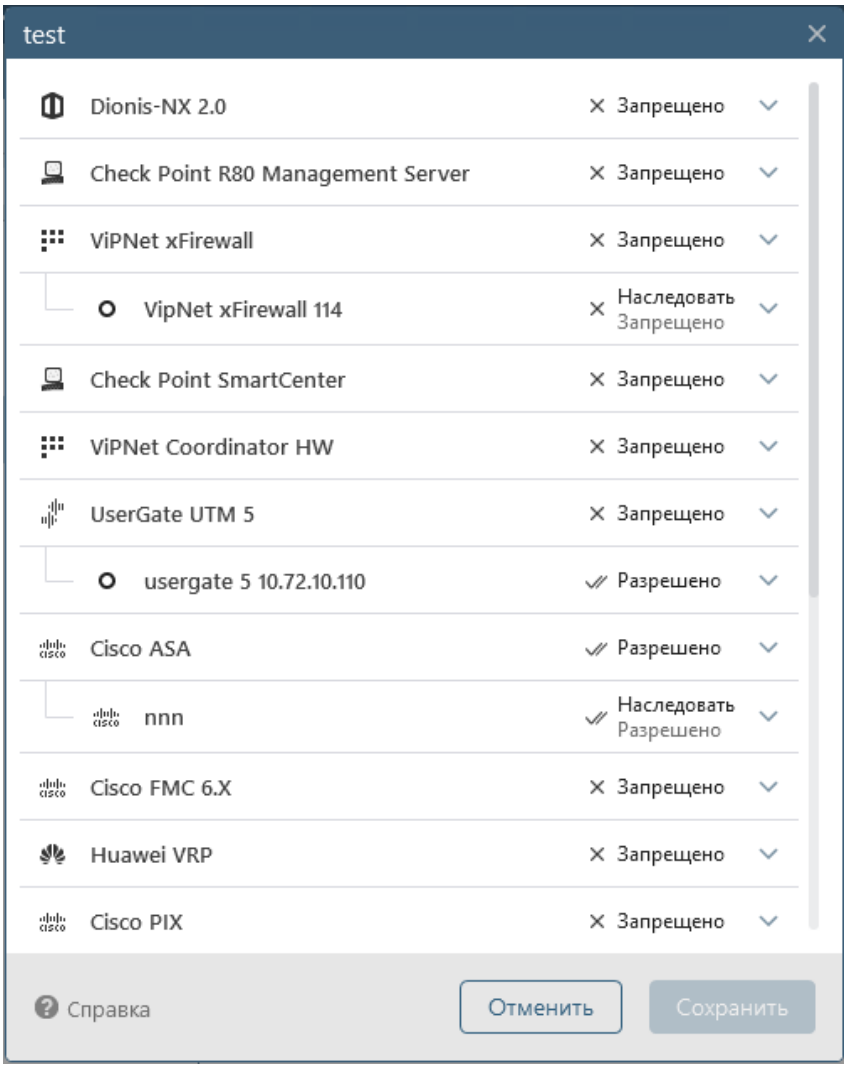


Рисунок 127 – Окно настройки использования стандарта безопасности МЭ или стандарта зонного анализа для устройств

Примечание – В разделе **Устройства** во вкладке ***Отчеты*** устройства, для которого разрешено использование стандарта безопасности МЭ, станет доступен новый отчет типа *Проверки* с наименованием, соответствующим разрешенному стандарту. Во вкладке ***Отчет*** отчета будет содержаться перечень требований стандарта безопасности, для каждого требования будет приведен список правил МЭ, удовлетворяющих заданным параметрам требования, во вкладке ***История изменений*** – перечень версий отчета с зафиксированными изменениями в соответствующем стандарте безопасности МЭ (подробнее описание правил просмотра и сравнения отчетов приведено в документе 643.72410666.00082-01 96 01-03 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 3. Работа с устройствами»).

2.11.6. Изменение стандартов безопасности МЭ и стандартов зонного анализа

2.11.6.1. Изменение имени и описания стандартов безопасности МЭ и стандартов зонного анализа

Для изменения имени и описания стандарта безопасности МЭ или стандарта зонного анализа необходимо выполнить следующие действия в клиентской консоли комплекса:

1) Перейти в раздел **Настройки**.
2) Выбрать сервер, для которого удаляется стандарт зонного анализа.
3) В области ***Настройки контроля*** нажать кнопку ***Проверки межсетевых экранов***.
4) Выбрать вкладку требуемого типа стандартов ***Стандарты безопасности*** или ***Зонный анализ***.
5) В панели списка стандартов выбранной вкладки выделить необходимый стандарт и нажать кнопку ***Свойства*** ( ).
6) В открывшемся окне изменения имени и описания стандарта (на рис. 128 приведен пример окна для стандарта зонного анализа) изменить необходимые параметры и нажать кнопку ***Сохранить***.

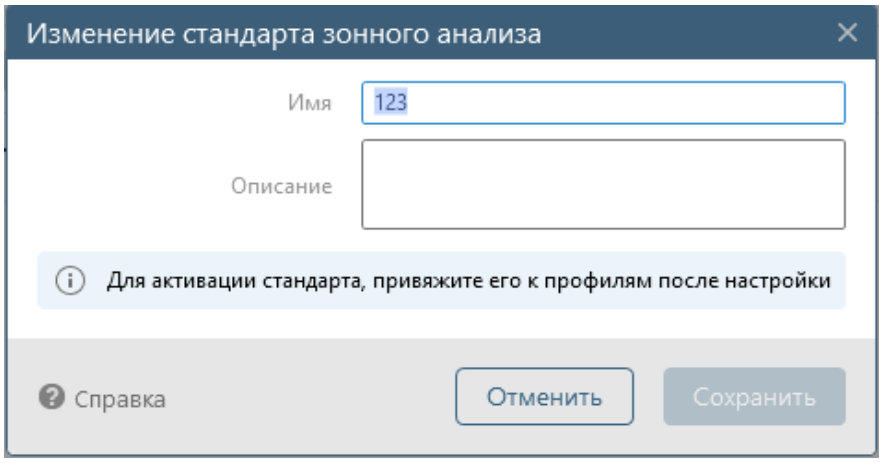


Рисунок 128 – Окно **Изменение стандарта зонного анализа**

7) Произойдет возврат в форму настройки проверок МЭ, в которой отобразятся внесенные в стандарт изменения.

2.11.6.2. Редактирование требований стандартов, исключений требований стандартов зонного анализа

Для редактирования требований стандарта безопасности МЭ необходимо:

1) В панели списка стандартов вкладки ***Стандарты безопасности*** выделить необходимый стандарт безопасности МЭ.
2) В области настройки параметров стандартов безопасности нажать в строке изменяемого требования кнопку ***Редактировать*** ( ). Откроется окно **Требование стандарта безопасности МЭ,** аналогичное окну добавления нового требования (см. рис. 119), с параметрами выбранного требования.

3) Внести в соответствии с таблицей 32 необходимые изменения в параметры требования.

Примечание – При редактировании необходимо учитывать, что измененное требование должно отличаться от остальных требований хотя бы по одному из параметров *Проверка*, *Действие*, *Протоколы/порты*, *Адреса источника*, *Адреса назначения, Приложение, Комментарий* и не должно содержать значение *Не учитывать* более чем для двух параметров.

4) Выполнить при необходимости тестовый запуск отчета по измененному требованию.

5) Внести при необходимости корректировки в параметры требования.

6) Нажать кнопку ***Сохранить.*** Произойдет возврат на вкладку ***Стандарты безопасности*** формы настройки проверок МЭ. На вкладке в области настройки требований отобразятся внесенные изменения для выбранного на шаге 2 требования

Примечание – При нажатии в окне **Требование стандарта безопасности МЭ** кнопки ***Отменить*** произойдет возврат на вкладку ***Стандарты безопасности*** без сохранения внесенных в требование изменений.

Для редактирования требований стандарта зонного анализа необходимо:

1) В панели списка стандартов вкладки ***Зонный анализ*** выделить необходимый стандарт зонного анализа.

2) В области настройки параметров стандартов нажать в строке выбранного для редактирования требования кнопку ***Изменить*** ( ). Откроется окно **Изменение требования,** аналогичное окну добавления нового требования (см. рис. 122), с параметрами выбранного требования.

3) Внести в соответствии с таблицей 33 необходимые изменения в параметры требования и нажать кнопку ***Сохранить***.

4) Произойдет возврат в форму настройки проверок МЭ.

Для редактирования исключений требования стандарта зонного анализа необходимо:

1) В панели списка стандартов вкладки ***Зонный анализ*** выделить необходимый стандарт зонного анализа.

2) В области настройки параметров стандартов нажать в строке выбранного для редактирования исключения кнопку ***Изменить*** ( ). Откроется окно **Изменение исключения,** аналогичное окну добавления нового исключения (см. рис. 125), с параметрами выбранного исключения.

3) Внести необходимые изменения в параметры исключения и нажать кнопку ***Сохранить***.

4) Произойдет возврат во вкладку ***Зонный анализ*** формы настройки проверок МЭ.

2.11.6.3. Удаление требований и исключений из стандартов безопасности и стандартов зонного анализа

Для удаления требования стандарта безопасности МЭ или исключения требования стандарта зонного анализа необходимо в строке удаляемого требования/исключения нажать кнопку ***Удалить*** (🗑) и в открывшемся окне подтверждения нажать кнопку ***Удалить***.

Для удаления одного требования стандарта зонного анализа необходимо в строке удаляемого требования стандарта зонного анализа нажать кнопку ***Меню*** (⋯) и выбрать в раскрывшемся меню пункт ***Удалить***.

Для удаления нескольких требований стандарта зонного анализа необходимо:

1) Нажать в заголовке рабочей области вкладки ***Зонный анализ*** кнопку ***Выбрать*** (☑).
2) В открывшейся форме выбора требований (рис. 129) установкой флагов выбрать требования для удаления и нажать в заголовке рабочей области кнопку ***Удалить*** (🗑). Откроется окно **Удаление требований** (рис. 130), в котором будут перечислены все удаляемые требования.
3) Подтвердить удаление, нажав кнопку ***Удалить***.

В результате выбранные требования/исключения будут удалены из стандарта.

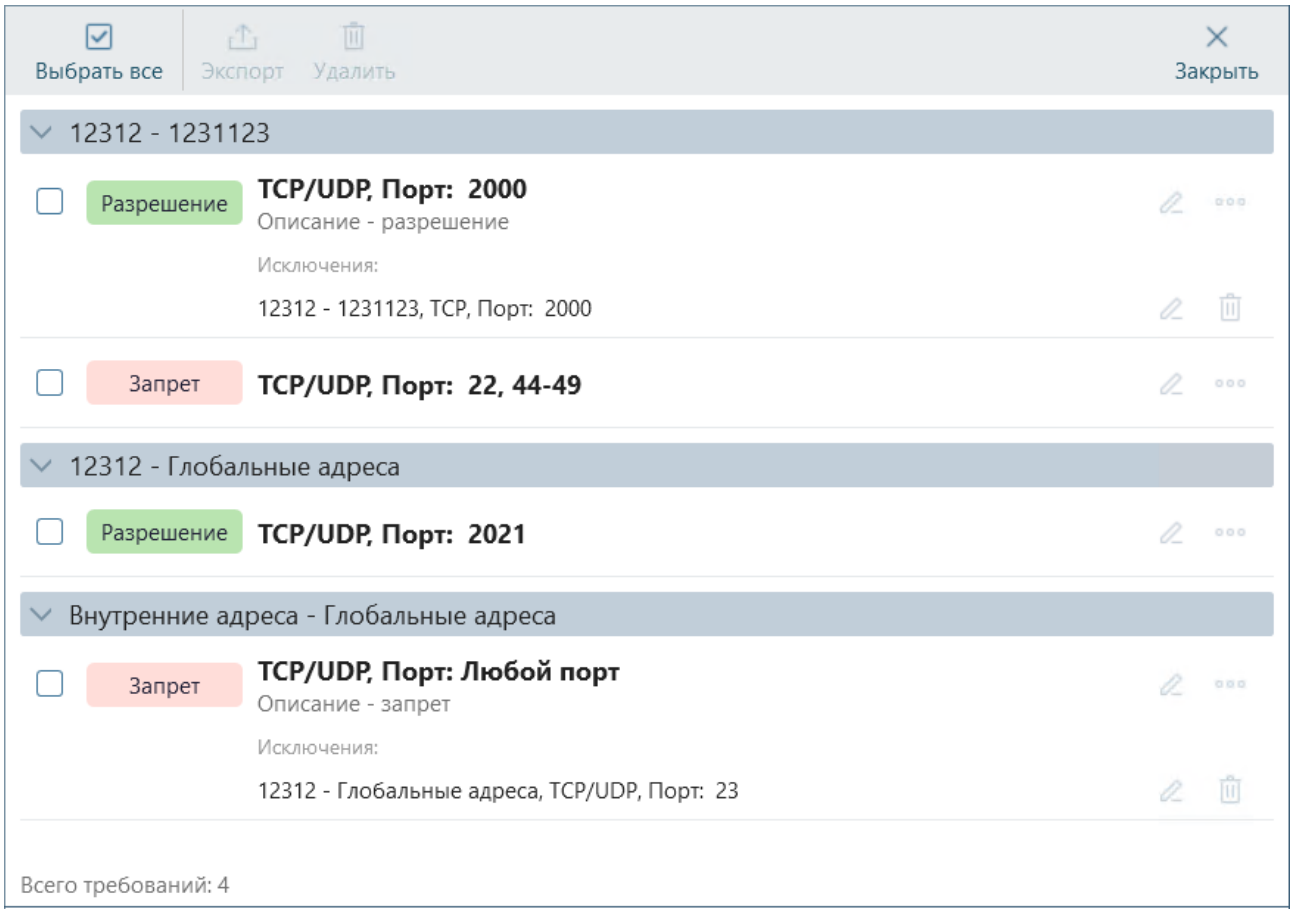


Рисунок 129 – Форма выбора требований

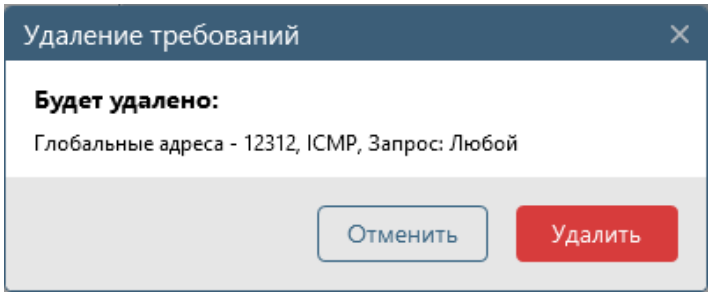


Рисунок 130 – Окно **Удаление требований**

2.11.7. Экспорт требований стандарта безопасности МЭ или зонного анализа

Для экспорта требований стандарта безопасности МЭ или зонного анализа в файл необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**.
2) Выбрать сервер, для которого удаляется стандарт зонного анализа.
3) В области ***Настройки контроля*** нажать кнопку ***Проверки межсетевых экранов***.
4) Выбрать вкладку требуемого типа стандартов ***Стандарты безопасности*** или ***Зонный анализ***.
5) В панели списка стандартов выбранной вкладки выделить необходимый стандарт.
6) В заголовке рабочей области вкладки нажать кнопку ***Выбрать*** ( ).
7) В открывшейся форме выбора требований выбрать установкой флагов требования для экспорта (для выбора всех требований – установить флаг в поле «Выбрать все» заголовка формы) и нажать кнопку ***Экспорт*** ( ).
8) В открывшемся стандартном окне используемой ОС указать имя и каталог размещения файла, в котором будут сохранены настройки выбранных правил проверки, и нажать кнопку ***Сохранить***. Параметры отмеченных требований будут сохранены в файле формата *.xml с заданным именем в указанном каталоге.

2.11.8. Удаление стандартов безопасности и стандартов зонного анализа

Для удаления стандарта необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**.
2) Выбрать сервер, для которого удаляется стандарт зонного анализа.
3) В области ***Настройки контроля*** нажать кнопку ***Проверки межсетевых экранов***.
4) Выбрать вкладку требуемого типа стандартов ***Стандарты безопасности*** или ***Зонный анализ***.
5) В панели списка стандартов выбранной вкладки выделить необходимый стандарт и нажать кнопку ***Удалить*** ( ) в меню панели списка стандартов.
6) В открывшемся окне **Удаление** подтвердить удаление стандарта, нажав кнопку ***Удалить*****.** Выбранный стандарт будет удален с сервера ПК.
7) Произойдет возврат в форму настройки проверок МЭ.

2.12. Экспорт настроек комплекса

В ПК «Efros Config Inspector» v.4 пользователь имеет возможность в разделе **Настройки** выгрузить текущие настройки контроля устройств и список устройств в файл формата .eci. Выгруженные настройки могут быть использованы в дальнейшем для импорта настроек в систему (см. п. 2.13 «Импорт настроек комплекса»).

Для экспорта настроек необходимо:

1) Перейти в раздел **Настройки** и в области ***Настройки контроля*** нажать кнопку ***Экспорт настроек***. Откроется окно **Экспорт настроек** (рис. 131, таблица 34).

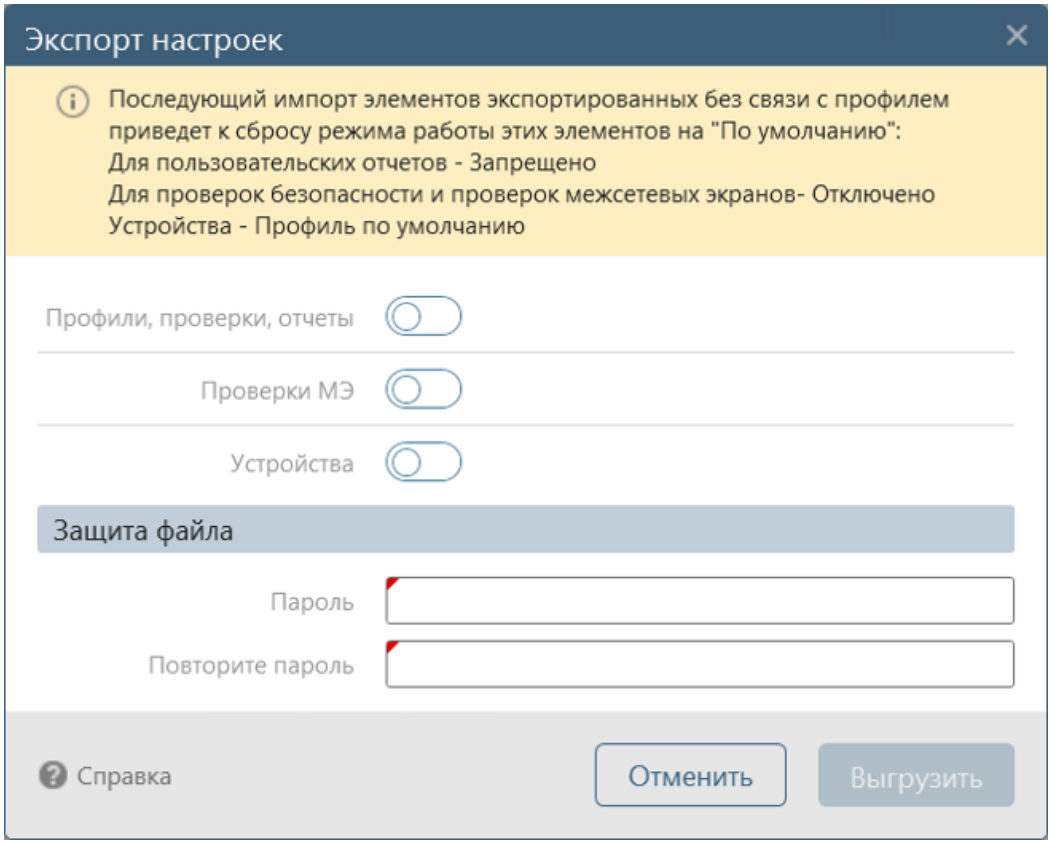


Рисунок 131 – Окно **Экспорт настроек**

Таблица 34 – Элементы окна **Экспорт настроек**

Элемент	Назначение
Переключатель *Профили, проверки, отчеты*	При включенном переключателе (положение ) при экспорте выполняется выгрузка параметров профилей и отчетов, выбранных в поле *Список* (см. ниже). При выключенном переключателе (положение ) поле *Список* в окне не отображается, выгрузка профилей и отчетов не выполняется. Поле *Список* содержит данные о количестве выбранных для выгрузки параметров профилей, проверок и отчетов и кнопку ***Выбрать***, по нажатию которой открывается окно выбора настроек сервера ПК для выгрузки (рис. 132).

Элемент	Назначение
	По умолчанию выбраны все профили устройств, проверки и пользовательские отчеты, имеющиеся на сервере ПК в текущий момент. Примечание – В окне выбора профилей, проверок и отчетов доступен поиск, а также фильтрация списка по типу настройки: *Профиль*, *Отчет*, *Проверка*, и по признаку *Выбрано* (*Да*, *Нет*) Окно фильтрации открывается по кнопке ***Фильтр*** (). После установки флага в поле *Да* признака *Выбрано*, в списке отображаются только выбранные профили, проверки и отчеты. Отмена фильтрации выполняется по нажатию в окне фильтрации ссылки *Сбросить фильтр*
Переключатель *Проверки МЭ*	При включенном переключателе (положение) при экспорте выполняется выгрузка параметров стандартов проверок МЭ, выбранных в поле *Список* (см. ниже). При выключенном переключателе (положение) поле *Список* в окне не отображается, выгрузка стандартов проверок МЭ не выполняется. Поле *Список* содержит данные о количестве выбранных для выгрузки параметров стандартов проверок МЭ и кнопку ***Выбрать***, по нажатию которой открывается окно выбора стандартов проверок МЭ сервера ПК (рис. 133). Окно содержит плоский список стандартов безопасности МЭ (пиктограмма «») и стандартов зонного анализа (пиктограмма «»), имеющихся на сервере ПК в текущий момент. По умолчанию для выгрузки выбраны все стандарты проверок МЭ в списке. Примечание – В окне выбора стандартов проверок МЭ доступен только поиск стандартов, возможность фильтрации списка отсутствует
Переключатель *Устройства*	При включенном переключателе (положение) при экспорте выполняется выгрузка списка устройств, выбранных в поле *Список* (см. ниже) (взаимосвязь с выбранными для выгрузки профилями и отчетами отсутствует). При выключенном переключателе (положение) поле *Список* в окне не отображается, список устройств не выгружается. Поле *Список* содержит данные о количестве выбранных для выгрузки устройств и кнопку ***Выбрать***, по нажатию которой открывается окно **Выбор устройств**. По умолчанию в списке выбраны все устройства. Примечание – В окне выбора устройств доступен поиск устройств, а также фильтрация списка по признаку *Выбрано* и типам устройств
Группа полей *Защита файла*	Содержит поля для ввода пароля и его подтверждения для шифрования файла с выгружаемыми данными

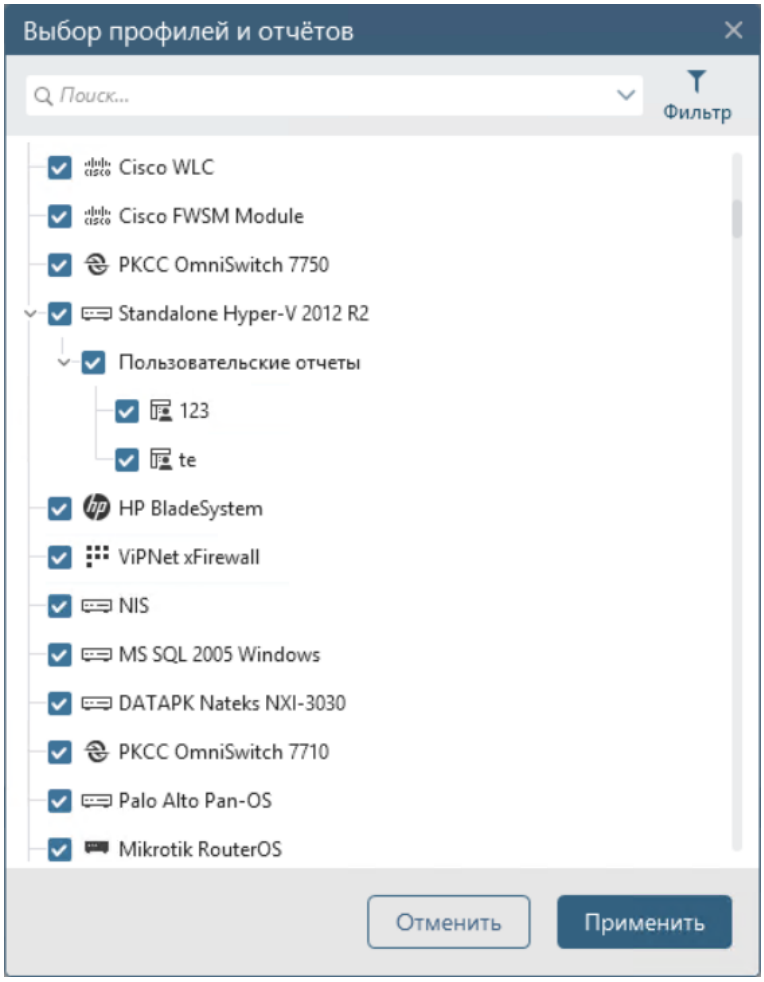


Рисунок 132 – Окно выбора профилей, проверок и отчетов сервера ПК для выгрузки

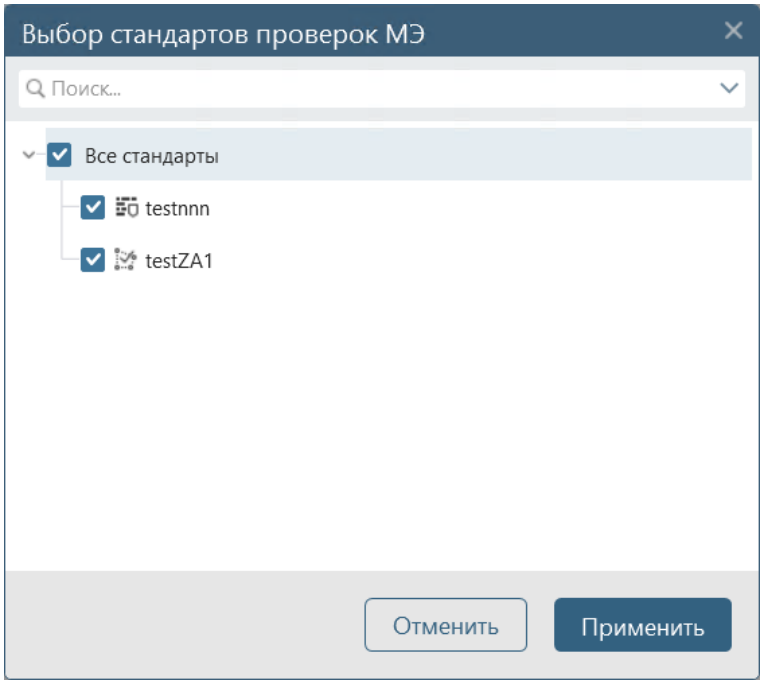


Рисунок 133 – Окно выбора стандартов проверок МЭ сервера ПК для выгрузки

2) Задать в соответствии с таблицей 34 параметры экспорта настроек, для чего

- установкой переключателей в положение *включено* ( ) выбрать тип выгружаемых параметров: *Профили, проверки и отчеты*, *Проверки МЭ* и *Устройства*;
- оставить в полях *Список* для всех выбранных типов параметров состав выбранных для выгрузки данных по умолчанию или изменить состав выгружаемых данных, нажав кнопку ***Выбрать*** и установкой/отменой установки флагов в открывшемся окне выбрать выгружаемые настройки.

3) Ввести в полях группы полей *Защита файла* пароль и его подтверждение для шифрования файла с выгружаемыми данными.

4) Нажать кнопку ***Применить*.**

5) Выбрать в открывшемся стандартном окне ОС каталог для сохранения файла, задать имя файла или оставить присвоенное ему по умолчанию имя «*Настройки - <имя сервера ПК> (<дата выгрузки>).eci*» и нажать кнопку ***Сохранить*** *(**Save**)*.

2.13. Импорт настроек комплекса

В ПК «Efros Config Inspector» v.4 пользователь имеет возможность в разделе **Настройки** импортировать ранее выгруженные настройки комплекса из файла формата .eci.

Примечание – Поддерживается также импорт списка устройств из файла формата xml от более ранних версий ПК «Efros Config Inspector» v.4.

При импорте объектов, экспортированных ранее без связи с профилем, режим работы этих объектов будет установлен в режим «по умолчанию»:

- для пользовательских отчетов – режим «Запрещено»
- для проверок безопасности и МЭ – режим «Отключено»
- для устройств – режим «Профиль по умолчанию».

Для импорта настроек необходимо;

1) Перейти в раздел **Настройки** и в области ***Настройки контроля*** нажать кнопку ***Импорт настроек***.

2) Выбрать в открывшемся стандартном окне ОС файл с импортируемыми настройками.

3) Ввести в открывшемся окне **Импорт настроек** (рис. 134) пароль, с использованием которого был создан файл (см. п. 2.12 «Экспорт настроек комплекса»), и нажать кнопку ***Продолжить***.

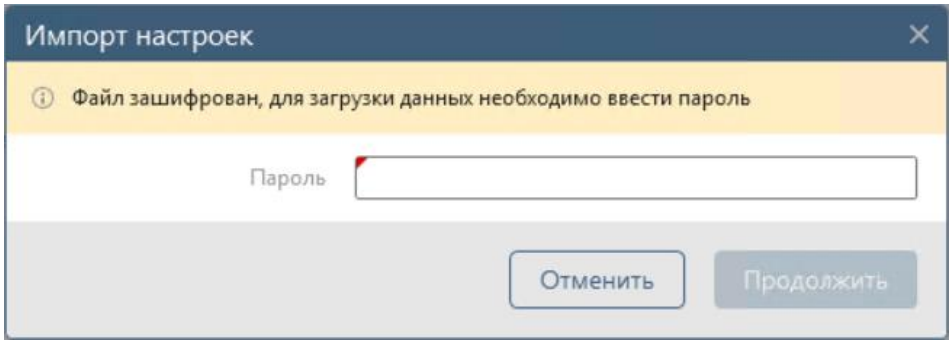


Рисунок 134 – Окно **Импорт настроек**

4) В открывшемся окне со списком доступных для импорта объектов (настроек) (рис. 135) установкой/отменой установки флагов выбрать импортируемые настройки: профили, проверки и отчеты, стандарты проверок МЭ, устройства. При этом:

- при выборе хоста – выбираются все вложенные устройства, доступные для выбора (при этом снятие выбора со вложенных не приводит к снятию выбора с родительского устройства);
- при снятии выбора с родительского хоста – для вложенных так же выбор снимается;
- при выборе хотя бы одного дочернего элемента хоста автоматически выбирается родительский.

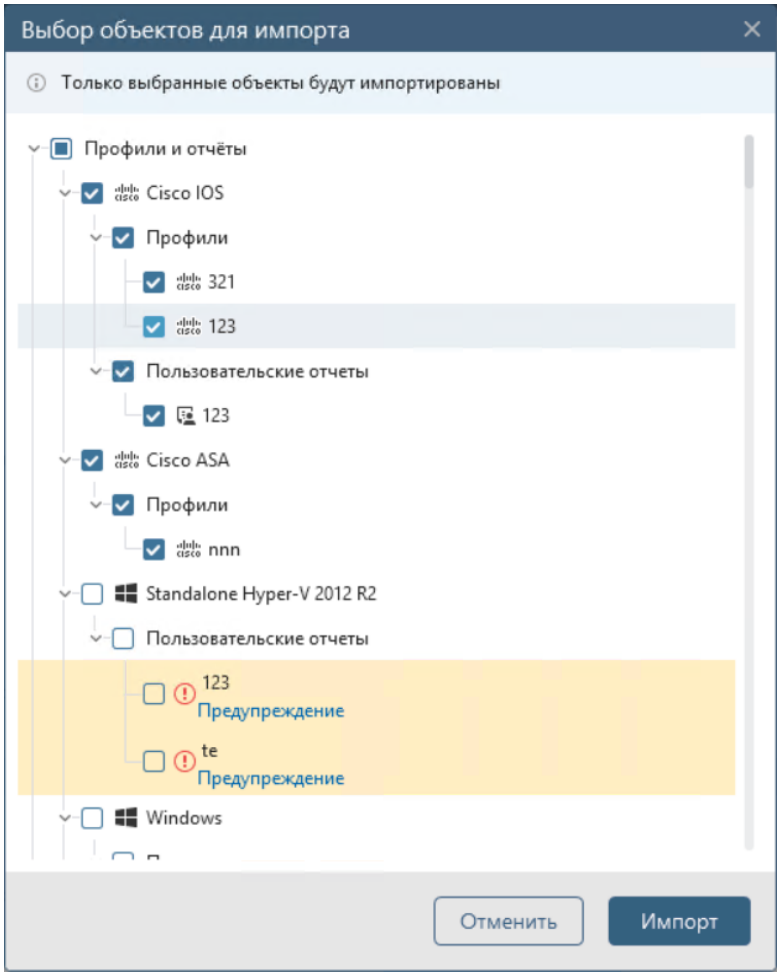


Рисунок 135 – Окно выбора объектов для импорта настроек

Примечание – По умолчанию в окне для импорта выбраны (для них установлены флаги) все объекты, которые можно импортировать. Если для объекта есть ограничения на импорт, то строка объекта выделяется, он по умолчанию не выбран для импорта (отсутствует флаг в соответствующем поле) и по нажатию ссылки *Предупреждение* выводится подсказка с причиной (например, «*Отчет уже существует. Настройки отчета будут заменены*»). Пользователь может выбрать такой объект для импорта.

5) Нажать кнопку ***Импорт***. Запустится процесс импорта выбранных настроек.

6) После успешного завершения импорта, окно **Выбор объектов для импорта** закроется и отобразится уведомление *Импорт завершен*.

Если при попытке импорта настроек обнаружен объект, который невозможно импортировать, то;

- импорт настроек не будет выполнен, в верхней части окна **Выбор объектов для импорта** отобразится сообщение *Некоторые объекты не могут быть импортированы*;
- строка проблемного объекта будет выделена красным цветом фона, в соответствующем поле будет удален флаг, и поле будет заблокировано. Для просмотра подробной информации о причинах отказа в импорте необходимо нажать ссылку ***Подробнее***.

Пользователь может запустить импорт повторно, но уже без такого объекта.

При выборе для импорта файла со списком устройств в формате .xml запрос на ввод пароля не выводится и окно выбора импортируемых устройств не отображается. Если импорт выполнен успешно, отображается соответствующее сообщение.

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. 136. 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.

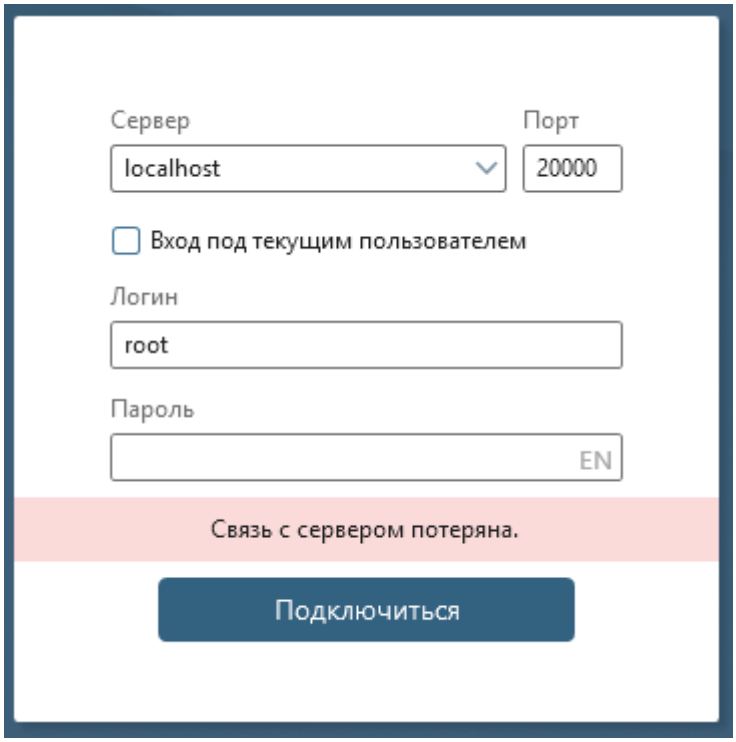


Рисунок 136 – Ошибка сетевого соединения между клиентской консолью и сервером ПК

2) В случае сбоя сетевого соединения между ПК «Efros Config Inspector» v.4 и защищаемыми узлами 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. 137). Запись об обнаружении нарушения будет также занесена в журнал событий раздела **События**.

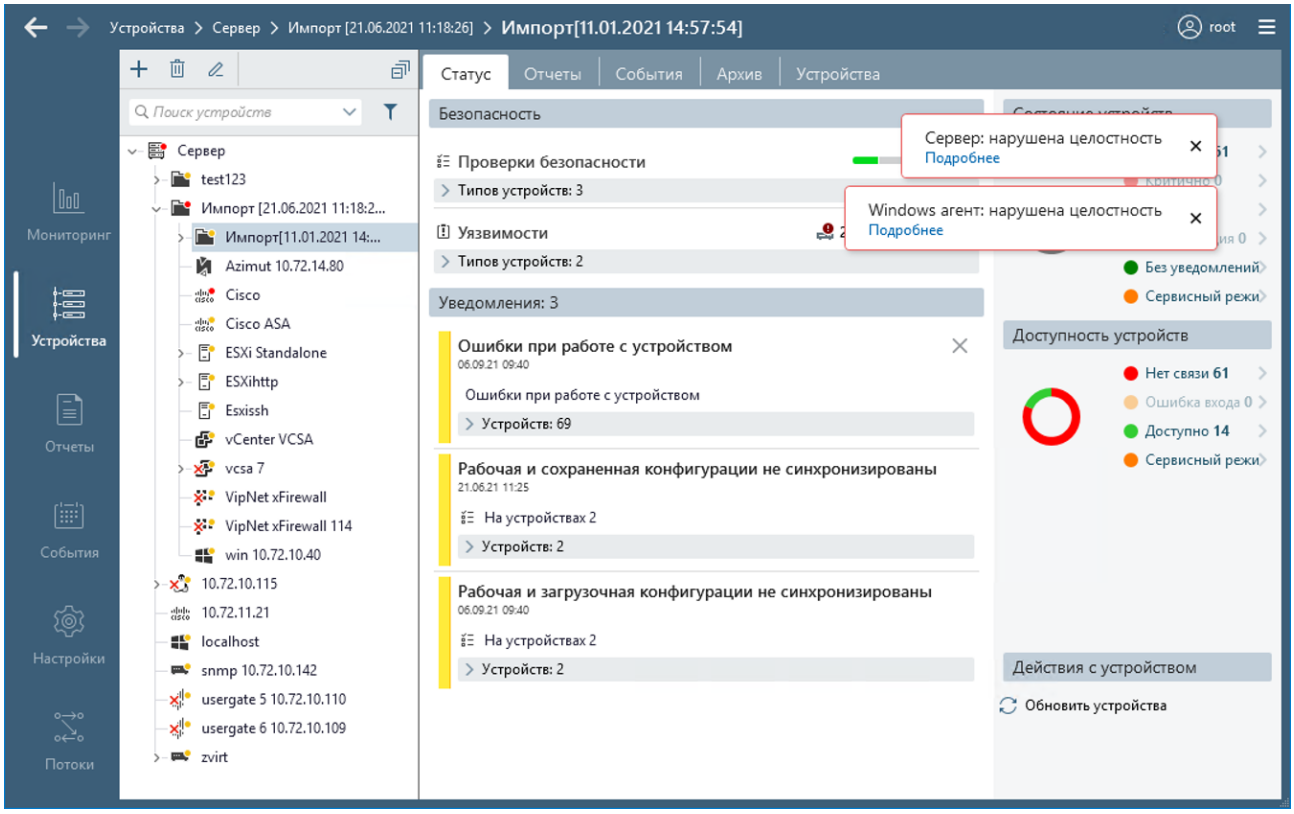


Рисунок 137 – Уведомления об обнаружении нарушения КЦ компонентов комплекса

Пользователь имеет возможность просмотреть перечень обнаруженных нарушений, нажав ссылку ***Подробнее*** (рис. 138). 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.

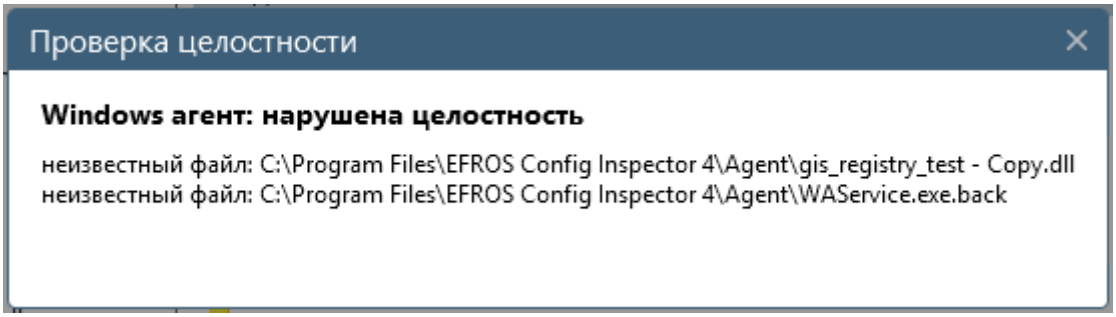


Рисунок 138 – Окно просмотра перечня обнаруженных нарушений при контроле КЦ компонента комплекса

2) В случае обнаружения несоответствия существующих настроек ПК «Efros Config Inspector» v.4 проектным настройкам пользователю с правами настройки контроля устройств (с правами *Управление* в категории *Настройки контроля*) необходимо проинформировать администратора ПК «Efros Config Inspector» v.4 о факте нарушения и привести 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 «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. 139) 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***.

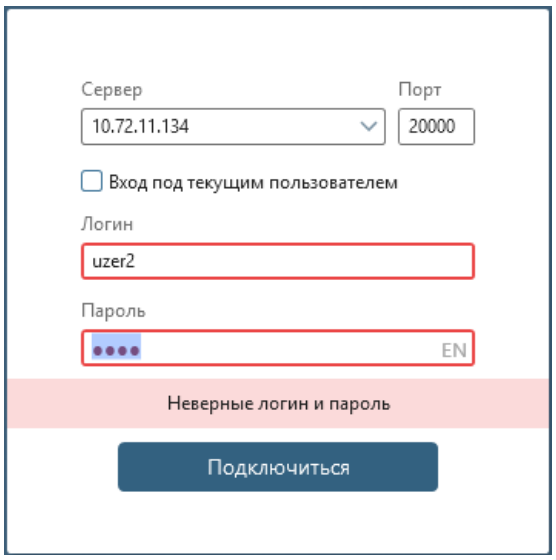


Рисунок 139 – Окно подключения к серверу ПК после ввода неверных данных пользователя

При получении сообщения о временной блокировке IP-адреса после нескольких подряд попытках (от 3 до 8) неверного ввода аутентификационных данных пользователя (рис. 140) 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.

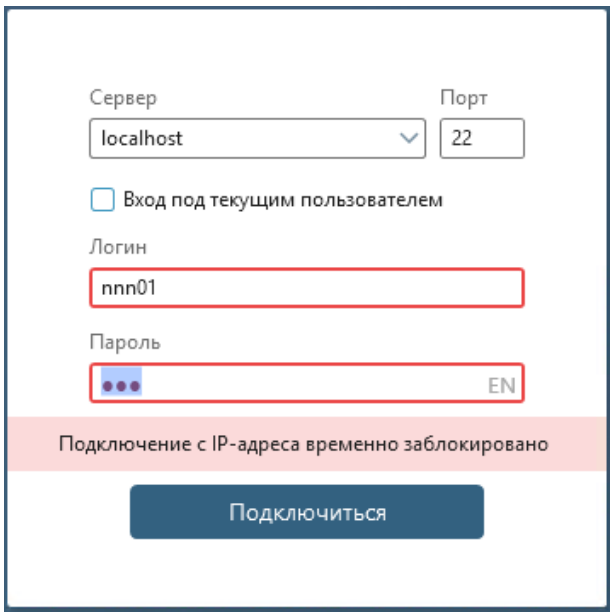


Рисунок 140 – Окно подключения к серверу ПК после превышения количества попыток неверного ввода аутентификационных данных пользователя

При получении сообщения о блокировке учетной записи пользователя (рис. 141) 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.

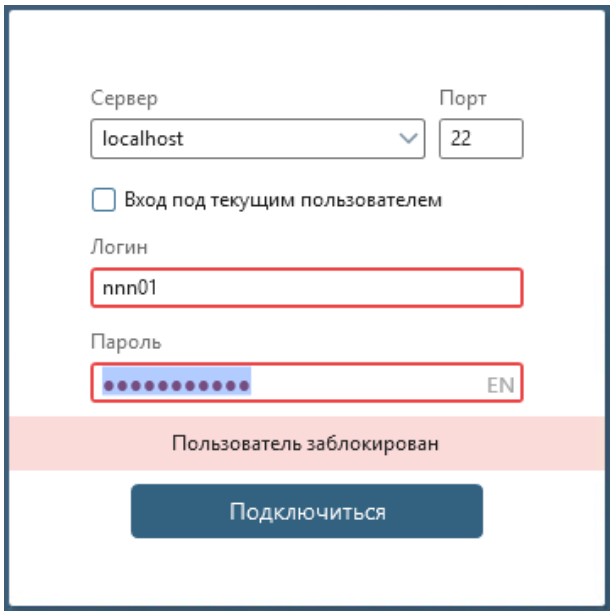


Рисунок 141 – Окно подключения к серверу ПК после ввода аутентификационных данных заблокированного пользователя

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 будут направлены информационные сообщения, связанные с некорректным указанием данных при выполнении функций настройки контроля.

Информационные сообщения, связанные с действиями пользователя по настройке контроля устройств, например:

- «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.

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
ОС	–	операционная система
ПК	–	программный комплекс
ПО	–	программное обеспечение
СКДПУ	–	система контроля действий поставщиков ИТ-услуг
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

Символ	Описание	Пример	Соответствие
{m,}	Не менее m	сто{2,}	сто, **стоо**, **стооо**, **стоооо**
{,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**abababc**dab
(?: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**