ГАЗИНФОРМ СЕРВИС

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

Руководство пользователя
Часть 1

Администрирование

Санкт-Петербург 2023

Аннотация

В документе приведены общие сведения о программном комплексе управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4 (далее по тексту – ПК «Efros Config Inspector» v.4 или комплекс), описания действий по администрированию комплекса с использованием клиентской консоли.

Настоящее руководство предназначено для пользователей ПК «Efros Config Inspector» v.4, имеющих доступ к настройкам комплекса в категории Администрирование (с правами *Просмотр* и *Управление* в категории *Администрирование*).

Содержание

1. Общие сведения о программе

1.1. Назначение программы

1.1.1. Наименование продукта – Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4.

1.1.2. Обозначение продукта – 643.72410666.00082-01.

1.1.3. 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.

1.2. Функции программы

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

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

1.2.2 ПК «Efros Config Inspector» v.4 состоит из следующих компонентов:

1) Сервера ПК «Efros Config Inspector» v.4 (далее – сервер ПК):
   - серверной части – устанавливается на выделенной электронно-вычислительной машине (ЭВМ);
   - клиентской консоли – может быть установлена на сервере ПК либо на других рабочих станциях с подключением к серверу ПК по сети;

- внешних модулей – устанавливаются вместе с серверной частью на сервере ПК, взаимодействуют с серверной частью на программном уровне

2) Windows-агента – устанавливается на контролируемом компьютере с ОС Windows, подключается к серверной части[1] по сети;

3) Коллектора задач (далее – коллектор) – устанавливается на других ЭВМ, подключается к серверной части по сети.

1.2.3. Сервер ПК обеспечивает выполнение функций ПК «Efros Config Inspector» v.4 по контролю сетевого оборудования, серверных и клиентских ОС, СУБД, АСУ ТП, виртуальных сред, а также анализу правил межсетевых экранов и функций по настройке 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.) (далее – ОС «Astra Linux SE»);
- ОС «РЕД ОС» Муром v.7.2, v.7.3, сертификат соответствия № 4060 (выдан ФСТЭК России 12.01.2019 г.) (далее – ОС «РЕД ОС»);
- ОС серии Windows 64-разрядные (далее - ОС Windows (x64)):
  - Windows Server 2008R2 Foundation Edition SP1;
  - Windows Server 2008R2 Standard Edition SP1;
  - Windows Server 2008R2 Enterprise Edition SP1;
  - Windows Server 2008R2 Datacenter Edition SP1;
  - Windows Server 2012/2012R2 Foundation;
  - Windows Server 2012/2012R2 Essentials;
  - Windows Server 2012/2012R2 Standard;
  - Windows Server 2012/2012R2 Datacenter;
  - Windows Server 2016 Standard;
  - Windows Server 2016 Datacenter;
  - Windows Server 2016 Essentials;
  - Windows Server 2019 Standard;
  - Windows Server 2019 Datacenter;
  - Windows Server 2019 Essentials;
  - Windows Server 2022 Standard;
  - Windows Server 2022 Datacenter;
  - Windows Server 2022 Essentials;
  - Windows 7 Professional SP1;
  - Windows 7 Enterprise SP1;
  - Windows 7 Ultimate SP1;

[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 8.1 Core;
- Windows 8.1 Professional;
- Windows 8.1 Enterprise;
- Windows 10 Home;
- Windows 10 Pro;
- Windows 10 Enterprise;
- Windows 11 Home;
- Windows 11 Pro;
- Windows 11 Enterprise.

1.2.4. Клиентская консоль подключается к серверу ПК и предоставляет графический интерфейс для выполнения следующих функций:

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

2) Работа с контролируемыми устройствами:

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

3) Формирование пользовательских отчетов для нескольких выбранных устройств на основе отчетов, загруженных с 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 ПК «Efros Config Inspector» v.4:

- настройки серверной части комплекса:
  а) 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);
  б) управление профилями для гибкой настройки параметров контроля устройств;
  в) управление отчетами, проверками, контролем устройств и групп;
  г) управление проверками устройств, настройка правил и исключений;

д) управление списком устройств в части: графического представления топологической карты локальной сети и установки параметров проверки доступности устройств;
е) настройка расписаний загрузки отчетов и выполнения операций с устройствами;
ж) настройка скрытия/разрешений загрузок и контроля целостности, вычисляемых/получаемых с устройств отчетов;
з) экспорт и импорт настроек комплекса;
и) сканирование сети (поиск сетевых устройств в локальной сети);
к) настройка политики межсетевых экранов при создании пользовательских правил проверок безопасности;

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

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

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

Клиентская консоль подключается к серверу ПК по протоколу HTTPS и TLS. Одновременно к серверу ПК могут быть подключены несколько клиентских консолей. Допускается установка клиентской консоли ПК «Efros Config Inspector» v.4 на ЭВМ, функционирующие под управлением ОС серии Windows.

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

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

1.2.7. 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.

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

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

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

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

- Cisco Systems, Inc. (полный перечень типов сетевого оборудования см. в таблице 1);
- 3Com Corporation (3ComOS);
- ЗАО «Российская корпорация средств связи» (RSOS9000, RS7750, RSOA700, Onyx);
- С-Терра СиЭсПи (NME-RVPN, VPN Gate);
- VMware, Inc. (ESXi, vCenter);
- HP, Inc. (BladeSystem, Comware Switch, Procurve, Virtual Connect, UX, Aruba);
- Allied Telesis (Allied-Telesis AT-GS950);
- Lenovo (ENOS 8.4, Cumulus, FabricOS);
- КриптоПро (КриптоПро TLS шлюз);
- Blue Coat Systems, Inc., ранее Crossbeam Systems, Inc. (XOS v.9);
- Oracle Corporation (СУБД Oracle 10g, SunOS, СУБД MySQL);
- D-Link Corporation (DES, DGS, DGS 1210, DGS 3130/3630);
- ООО «СайберЛимфа» (DATAPK);
- Phoenix Contact (Phoenix contact);
- RAISECOM Technology (ISCOM);
- Korenix Technology Co., Ltd (JetNet);
- Kubernetes;
- ZyXEL Communications Corp. (ZyNOS);
- Zelax (Zelax M-1 Мега, Zelax ZES);
- Edge-core (ECS);
- ExtremeNetworks (Extreme 220 series, ExtremeXOS);
- Check Point Software Technologies, Inc. (R80 Management Server, SecurePlatform, GAiA, SmartCenter, GAiA Embedded, Domain Management Server, Maestro Orchestrator);
- ООО «Кьютек» (QSW);

- MikroTik (Mikrotik RouterOS);
- Moxa, Inc (EDS, MGate, NPort 5100 Series);
- Huawei Technologies Co., Ltd (Quidway);
- Citrix Systems, Inc (XenServer);
- ОАО «ИнфоТеКС» (VipNet Coordinator, VipNet xFirewall, VipNet Prime);
- H3C Technologies (H3C);
- НПП «Фактор-ТС» (Dionis LX и Dionis NX версии 1.1, 1.2 и 2.0);
- Juniper Networks, Inc (JUNOS);
- ООО «Предприятие «Элтекс» (Eltex ESR, ME, MES, MES2428, WLC, WOP/WEP);
- ООО «Бифорком Тек» (коммутаторы серии CS2100);
- ООО «Код Безопасности» (Код Безопасности Континент);
- ООО «ТИОНИКС» (TIONIX);
- Palo Alto Networks, Inc (PanOS 7, 9);
- ОАО НПП «Полигон» (Арлан, ИнЗер);
- UiPath Inc (Uipath Studio, Uipath Orchestrator, Uipath Robot);
- Primo RPA (Primo RPA Orchestrator);
- WatchGuard Technologies, Inc. (WatchGuard Fireware OS, WatchGuard Fireware XTM OS);
- Rockwell Automation, Inc (Rockwell Cisco IOS);
- TFortis (PSW);Siemens AG (Siemens Scalance X-300, X-400 series, Simatic WinCC);
- ОС Unix/Linux (полный перечень ОС см. в таблице 1);
- ОС Microsoft Windows (полный перечень ОС см. в таблице 1);
- Virtual Machine Manager, Hyper-V (полный перечень ПО см. в таблице 1);
- ООО «Базальт СПО» (Альт Сервер Виртуализации 9.2 в PVE исполнении (PVE версия 6.3));
- СУБД Microsoft (MS SQL 2000, 2005, 2008, 2012, 2016);
- СУБД PostgreSQL;
- ООО «Газинформсервис» (СУБД «Jatoba»);
- Firebird Foundation (СУБД Firebird);
- Docker;
- Open Virtualization Alliance (KVM);
- Инфолэнд (zVirt);
- НАТЕКС (NetXpert);
- NSGate (NIS);
- Hirschmann (MAR);
- UserGate (UserGate UTM);
- AVAYA;
- Azimut (Marlin);
- AdAstrA Research Group, Ltd (SCADA TRACE MODE);
- Fortinet (Fortinet FortiGate, Fortinet FortiGate VDOM, Fortinet FortiWLC, Fortinet FortiSwitch);
- РЕД СОФТ (РЕД Виртуализация 7.3.0);
- НПФ «Система-Сервис» (Аргус);

- АО «ЭлеСи» (SCADA Infinity);
- Атомик Софт (SCADA Alpha.HMI);
- ООО «ИнСАТ» (MasterSCADA);
- ФГУП «ЭЗАН» (SCADA-система «Соната»);
- GE Digital (CIMPLICITY, iFix, GENESIS32);
- Schneider Electric (Vijeo Citect SCADA);
- Compressor Controls Corporation (CCC) (TrainTools, TrainView);
- ООО «Газприборавтоматика» (Zond2006, Zond2015);
- Emerson (SCADA DeltaV);
- Yokogawa Electric Corporation (CENTUM VP);
- НПО «Текон-Автоматика» (SCADA АСУД-248);
- ООО «НПА Вира Реалтайм» (ПК «Сириус-ИС»);
- Rubytech (СКАЛА-Р 1.91);
- Verano (RTAP A.08.10 (Windows), RTAP A.09.00 (Linux));
- Wonderware InTouch (7, 8, 10, 11);
- Weidmueller (Weidmueller Advanced Line Managed Switches);
- АО «ТРЭИ» (ПЛК Trei (QNX 6.5));
- АО «ЭЗАН» (ПЛК Ezan (QNX 6.5)).

Приведенный список постоянно пополняется и зависит от состава внешних модулей, используемых в конкретном установленном ПК «Efros Config Inspector» v.4.

Оборудование, поддерживаемое серверной частью ПК «Efros Config Inspector» v.4, установленной на разные платформы (ОС «Astra Linux SE», ОС «РЕД ОС» и ОС Windows (x64)), представлено в таблице 1.

Таблица 1 – Перечень поддерживаемого оборудования серверной частью ПК «Efros Config Inspector» v.4, установленной на различные платформы

Поддерживаемое оборудование	ОС «РЕД ОС»	ОС «Astra Linux SE»	ОС Windows (x64)
3Com OS	ДА	ДА	ДА
AD Domain	ДА	ДА	ДА
Allied-Telesis AT-GS950	ДА	ДА	ДА
Avaya	ДА	ДА	ДА
Cisco (ACS, ACI, ASA, AsyncOS, CatOS, FTD, FWSM Module, IOS, IOS XE, IOS XR, IPS, NX-OS, PIX, SMB, WAP, WLC, FMC 6.x (с поддержкой MDS), Firepower)	ДА	ДА	ДА
Cisco (UCM 10.0, UCM 8.5, Unified Phone 78xx, Unified Phone 88xx)	НЕТ	НЕТ	ДА
Check Point (GAiA, GAiA Embedded, R80 Management Server, SecurePlatform, SmartCenter, Domain Management Server, Maestro Orchestrator)	ДА	ДА	ДА
Crossbeam XOS v.9	ДА	ДА	ДА
DATAPK	ДА	ДА	ДА
Phoenix contact	ДА	ДА	ДА
H3C	ДА	ДА	ДА
Dionis NX (NX 1.1, NX 1.2, NX 2.0)	ДА	ДА	ДА
Dionis LX	НЕТ	НЕТ	ДА

Поддерживаемое оборудование	ОС «РЕД ОС»	ОС «Astra Linux SE»	ОС Windows (x64)
D-Link (DES, DGS, DGS 1210, DGS 3130/3630)	ДА	ДА	ДА
Edge-Core ECS	ДА	ДА	ДА
Eltex (ESR, ME, MES2428, MES, WLC, WOP/WEP)	ДА	ДА	ДА
Extreme 220 series, ExtremeXOS	ДА	ДА	ДА
Fortinet FortiGate, Fortinet FortiGate VDOM, Fortinet FortiWLC, Fortinet FortiSwitch	ДА	ДА	ДА
Hirschmann MAR	ДА	ДА	ДА
HP (BladeSystem, Comware Switch, Procurve, Virtual Connect, UX, Aruba)	ДА	ДА	ДА
Huawei VRP	ДА	ДА	ДА
Juniper JunOS	ДА	ДА	ДА
Korenix JetNet	ДА	ДА	ДА
Kubernetes	ДА	ДА	ДА
Lenovo ENOS 8.4, Cumulus, FabricOS	ДА	ДА	ДА
Mikrotik RouterOS	ДА	ДА	ДА
Moxa (EDS, MGate, NPort 5100 Series)	ДА	ДА	ДА
MS SCVMM (Virtual Machine Manager 2008 R2, 2012 R2, 2016, 2019, SCVMM Group, Hyper-V 2008 (R2 VM, R2 хост, R2 хост с контролем целостности), Hyper-V 2012 (R2 VM, R2 хост, R2 хост с контролем целостности), Hyper-V 2016 (VM, хост, хост с контролем целостности), Hyper-V 2019 (VM, хост, хост с контролем целостности) Standalone Hyper-V (2008 R2, 2012 R2, 2016, 2019))	НЕТ	НЕТ	ДА
Альт Сервер Виртуализации 9.2 в PVE исполнении (PVE версия 6.3)	ДА	ДА	ДА
MS SQL 2000, 2005, 2008, 2012, 2016	ДА	ДА	ДА
PostgreSQL	ДА	ДА	ДА
СУБД «Jatoba»	ДА	ДА	ДА
KVM (актуальные версии Linux)	ДА	ДА	ДА
Nateks (NX-3400, NX-5100, NXI-3030, NXI-3050)	ДА	ДА	ДА
КриптоПро TLS шлюз	ДА	ДА	ДА
NSGate NIS	ДА	ДА	ДА
Palo Alto Pan-OS 7, 9	ДА	ДА	ДА
PKCC (OmniAccess 700, OmniSwitch 6850, OmniSwitch 7710, OmniSwitch 7750, OmniSwitch 9000, Onyx)	ДА	ДА	ДА
QTech QSW	ДА	ДА	ДА
Raisecom ISCOM	ДА	ДА	ДА
Rockwell Cisco IOS	ДА	ДА	ДА
TFortis PSW	ДА	ДА	ДА
Azimut Marlin	ДА	ДА	ДА
Siemens Scalance X-300 series, X-400 series, Simatic WinCC	ДА	ДА	ДА
S-Terra VPN Gate	ДА	ДА	ДА
ViPNet Coordinator HW, ViPNet xFirewall, VipNet Prime	ДА	ДА	ДА
TIONIX	ДА	ДА	ДА
Код Безопасности Континент	ДА	ДА	ДА

Поддерживаемое оборудование	ОС «РЕД ОС»	ОС «Astra Linux SE»	ОС Windows (x64)
Коммутаторы CS2100 (Бифорком Тек)	ДА	ДА	ДА
VMWare vCenter (vCenter (VCSA, Windows), Standalone ESXi с контролем файлов по HTTPS (SSH), VM (5.0, 5.1, 5.5, 6.0, 6.5, 7), Host, Host с контролем целостности файлов по SSH (HTTPS), Folder, Datacenter, vApp, Resource Pool, ESXi ОС с контролем файлов по HTTPS (SSH), Cluster)	НЕТ	НЕТ	ДА
ESXi ОС с контролем файлов по SSH	ДА	ДА	ДА
СКАЛА-Р 1.91	ДА	ДА	ДА
Uipath Studio, Uipath Orchestrator, Uipath Robot	ДА	ДА	ДА
Primo RPA Orchestrator	ДА	ДА	ДА
UserGate UTM 5, 6, 7	ДА	ДА	ДА
WatchGuard Fireware (OS, XTM OS)	ДА	ДА	ДА
ОС Unix/Linux (AIX, Oracle Oracle SunOS, HP-UX, AltLinux, Red Hat, Debian, Manjaro, Ubuntu, Mint, Fedora, FreeBSD, Red OS, Astra Linux)	ДА	ДА	ДА
ОС Windows (xp, vista, 7, 8, 10, 2000, 2003, 2008r2, 2012, 2012r2, 2016, 2019)	ДА	ДА	ДА
РЕД Виртуализация 7.3.0	ДА	ДА	ДА
СУБД Oracle 10g	ДА	ДА	ДА
СУБД MySQL 5.5.7 и выше	ДА	ДА	ДА
СУБД Firebird	ДА	ДА	ДА
Docker	ДА	ДА	ДА
Citrix XenServer	НЕТ	НЕТ	ДА
Zelax M-1-MEGA, Zelax ZES	ДА	ДА	ДА
ZyXEL ZyNOS	ДА	ДА	ДА
zVirt 4.3.3.6-1.el7	ДА	ДА	ДА
Полигон (Арлан, ИнЗер)	ДА	ДА	ДА
SCADA Alpha.HMI	ДА	ДА	ДА
SCADA Infinity	ДА	ДА	ДА
SCADA- Аргус	ДА	ДА	ДА
MasterSCADA	ДА	ДА	ДА
SCADA-система «Соната»	ДА	ДА	ДА
SCADA ПК «Сириус-ИС»	ДА	ДА	ДА
SCADA DeltaV v. 6.3.2	ДА	ДА	ДА
SCADA TRACE MODE v. 5 и 6	ДА	ДА	ДА
GENESIS32	ДА	ДА	ДА
CENTUM VP	ДА	ДА	ДА
CIMPLICITY	ДА	ДА	ДА
iFix 3.5	ДА	ДА	ДА
TrainTools	ДА	ДА	ДА
TrainView	ДА	ДА	ДА
Vijeo Citect v 7.40	ДА	ДА	ДА
SCADA АСУД-248	ДА	ДА	ДА
SCADA RTAP A.08.10 (Windows), RTAP A.09.00 (Linux)	ДА	ДА	ДА
Zond2006	ДА	ДА	ДА
Zond2015	ДА	ДА	ДА
Wonderware InTouch (7, 8, 10, 11)	ДА	ДА	ДА
Weidmueller Advanced Line Managed Switches	ДА	ДА	ДА

Поддерживаемое оборудование	ОС «РЕД ОС»	ОС «Astra Linux SE»	ОС Windows (x64)
ПЛК Trei (QNX 6.5)	ДА	ДА	ДА
ПЛК Ezan (QNX 6.5)	ДА	ДА	ДА

Отличие функций ПК «Efros Config Inspector» v.4, установленного на разные платформы (ОС «Astra Linux SE», ОС «РЕД ОС» и ОС Windows (x64)), представлено в таблице 2.

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

Таблица 2 – Функциональные различия ПК «Efros Config Inspector» v.4 при развертывании на различных платформах

Функции	ОС «РЕД ОС»	ОС «Astra Linux SE»	ОС Windows (x64)
Идентификация и аутентификация пользователей под доменной учетной записью	ДА	ДА	ДА
Наличие клиентской консоли, для локальной установки совместно с серверной частью, реализующей графический интерфейс для управления функциями комплекса	НЕТ (используется консоль, установленная на сервере под управлением ОС серии Windows)	НЕТ (используется консоль, установленная на сервере под управлением ОС серии Windows)	ДА

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

Структура комплекса, его функциональные возможности (функции), перечень решаемых с помощью комплекса задач, условия применения, описаны в разделе 1 документа 643.72410666.00082-01 31 01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Описание применения».

1.2.10. Активный аудит контролируемого оборудования осуществляется с использованием протоколов, указанных в таблице 3. Список протоколов и модулей, с использованием которых на сервере ПК может осуществляться активный аудит сетевого и серверного оборудования, может быть расширен за счет разработки и включения в программный комплекс соответствующих внешних модулей.

Таблица 3 – Протоколы, используемые на сервере ПК для аудита оборудования

Протокол	Где используется	Устройства/Функции	Поддерживаемые ОС
SSH*	Модули взаимодействия с сетевыми устройствами	Сетевые устройства	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
Telnet			

Протокол	Где используется	Устройства/Функции	Поддерживаемые ОС
SCP, SFTP	Модуль управления устройствами, Модуль взаимодействия с устройствами Континент, Dionis, Docker	Копирование файлов конфигураций и шаблонов проверок безопасности	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
LDAP	Модуль взаимодействия с Active Directory	Active Directory	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
CPMI	Модуль взаимодействия с устройствами CheckPoint	CheckPoint SmartCenter	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
LEA			
Cisco Administrative XML (AXL)	Модуль взаимодействия с сетевыми устройствами Cisco UCM	Cisco UCM	ОС Windows (x64)
XenAPI	Модуль взаимодействия с Citrix XenServer	Citrix XenServer	ОС Windows (x64)
REST (HTTP/HTTPS)	Модули взаимодействия с устройствами Cisco, Check Point, Скала-Р, SCADA Cimplicity, UiPath, zVirt, Proxmox, Tionix, Primo RPA и Docker	Cisco ACS Cisco Firepower Cisco ACI CheckPoint R80 Check Point Domain Management Server Скала-Р SCADA Cimplicity UiPath zVirt Proxmox Tionix Primo RPA Docker	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
WMI	Модуль взаимодействия с Hyper-V	Загрузка настроек Hyper-V	ОС Windows (x64)
PowerShell (WinRM)		Выполнение проверок соответствия Hyper-V	ОС Windows (x64)
SMB	Модуль взаимодействия с Active Directory	Загрузка файлов групповых политик	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
	Модуль взаимодействия с Hyper-V	Загрузка файлов ВМ Hyper-V	ОС Windows (x64)

Протокол	Где используется	Устройства/Функции	Поддерживаемые ОС
Microsoft RTC API	Модуль отправки сообщений через MS Lync	Отправка сообщений в Lync	ОС Windows (x64)
Microsoft Exchange Web Services Managed API	Модуль отправки сообщений через MS Exchange	Отправка писем через MS Exchange	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
SMTP	Модуль отправки писем по протоколу SMTP	Отправка писем SMTP	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
Syslog	Модуль отправки syslog-сообщений	Отправка Syslog-сообщений администраторам сети	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
	Модуль Syslog-сервер	Syslog-сервер приема сообщений	
SNMP	Сканер сети для последующего добавления найденных устройств в список устройств	Поиск устройств в сети (SNMP сканер)	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
		Приём сообщений	
		Загрузка сведений по интерфейсам/маршрутам для сетевых устройств	
VIX API (SOAP, HTTPS)	Модуль взаимодействия с vCenter	vCenter, загрузка настроек	ОС Windows (x64)
HTTPS		vCenter, загрузка файлов ВМ	ОС Windows (x64)
Microsoft TDS	Модуль взаимодействия с MS SQL	СУБД MS SQL	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
Oracle .Net	Модуль взаимодействия с Oracle	СУБД Oracle	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
PostgreSQL Protocol	Модуль взаимодействия с PostgreSQL, Jatoba	СУБД PostgreSQL, Jatoba	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
Firebird Wire Protocol	Модуль взаимодействия с Firebird	СУБД Firebird	ОС Windows (x64) ОС «Astra Linux SE», ОС «РЕД ОС»
MySQL	Модуль взаимодействия с MySQL	СУБД MySQL	ОС серии Windows ОС «Astra Linux SE», ОС «РЕД ОС»
XML-RPC	Модуль взаимодействия с UserGate	UserGate	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»

Протокол	Где используется	Устройства/Функции	Поддерживаемые ОС
DioNIS Control Protocol (DCP)	Модуль взаимодействия с Dionis	Dionis LX	ОС Windows (x64),
Проприетарный на базе HTTPS	Windows-агент	Сбор данных с ОС Windows от агента	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
		Прием сообщений от Windows-агента	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
	Сервер	Подключение консоли к серверу	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
		Взаимодействие между серверами в иерархии	ОС Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
	Коллекторы	Приём-передача сообщений коллектору комплекса	ОС Windows (x64)

* Используемая в комплексе ПК «Efros Config Inspector» v.4 библиотека libssh поддерживает следующие параметры подключения:

- **Ciphers** – chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr,aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc;
- **MACs** – hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1;
- **KexAlgorithms** – diffie-hellman-group-exchange-sha1,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group18-sha512,diffie-hellman-group16-sha512,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1,ext-info-c;
- **HostKeyAlgorithms** – ssh-ed25519,ecdsa-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha2-nistp256,rsa-sha2-512,rsa-sha2-256,ssh-rsa

1.3. 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 базе данных уязвимостей (БДУ) и обновление БДУ;
- настройка подключения к БДУ через прокси-сервер;
- настройка и проверка подключения к серверу «Efros Security Center Flow Server».

Пользователи, которым назначены права:

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

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

Доступ пользователей к конкретным устройствам зависит от назначенных им администратором комплекса прав доступа. Перечень и описание назначаемых пользователям прав доступа приведен в таблице 4.

Таблица 4 – 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

Право доступа	Описание
	настроек пользователей); – проверка подключения (доступности)
Полный доступ (изменение настроек)[2)]	– добавление устройств; – изменение параметров устройств; – изменение настроек контроля устройств; – выполнение операций с устройствами. Например, операции: добавить пользователя или скопировать running в startup для устройств Cisco IOS, конфигурировать, восстановить конфигурацию

[1)] Загрузка и обновление отчетов доступны пользователям с правами *Чтение* – только при отключенном режиме *Запретить загрузку конфигураций для пользователей с правами «чтение»* (см. пункт 2.4.8 «Настройка параметров безопасности учетных записей пользователей комплекса»).

[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, администрированию комплекса и к устройствам пользователь может менять локальные настройки клиентской консоли комплекса.

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.

1.4. Сведения о технических и программных средствах, обеспечивающих выполнение программы

1.4.1 ПК «Efros Config Inspector» v.4 должен устанавливаться на ЭВМ[3] согласно требованиям эксплуатационной документации на комплекс.

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

1.4.2. 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».

2. Настройка комплекса в клиентской консоли

2.1. Запуск и общее описание консоли

После установки и настройки ПК «Efros Config Inspector» v.4 в БД комплекса по умолчанию создается встроенная учетная запись – пользователь с полными правами доступа к функциям ПК «Efros Config Inspector» v.4 (**root** с паролем по умолчанию **root**).

Учетные записи остальных пользователей создаются в ПК «Efros Config Inspector» v.4 встроенным пользователем или другими пользователями с правами *Управление* категории *Администрирование*, учетные записи которых также должен создать встроенный пользователь.

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.

После запуска консоли в открывшемся окне подключения к серверу (рис. 1) следует указать:

1) В поле ***Сервер*** – ввести IP-адрес сервера ПК или его DNS-имя. Если серверная и клиентская часть комплекса установлены на один компьютер, то в поле ***Сервер*** можно ввести *127.0.0.1* или *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 серверу ПК 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 ОС Windows, при этом в поле ***Логин*** отобразится имя учетной записи текущего пользователя ОС Windows.

3) В поле ***Порт*** – ввести корректный номер TCP-порта для соединения клиентской консоли с сервером ПК. По умолчанию используется TCP-порт 20000.

4) Нажать кнопку ***Подключиться***.

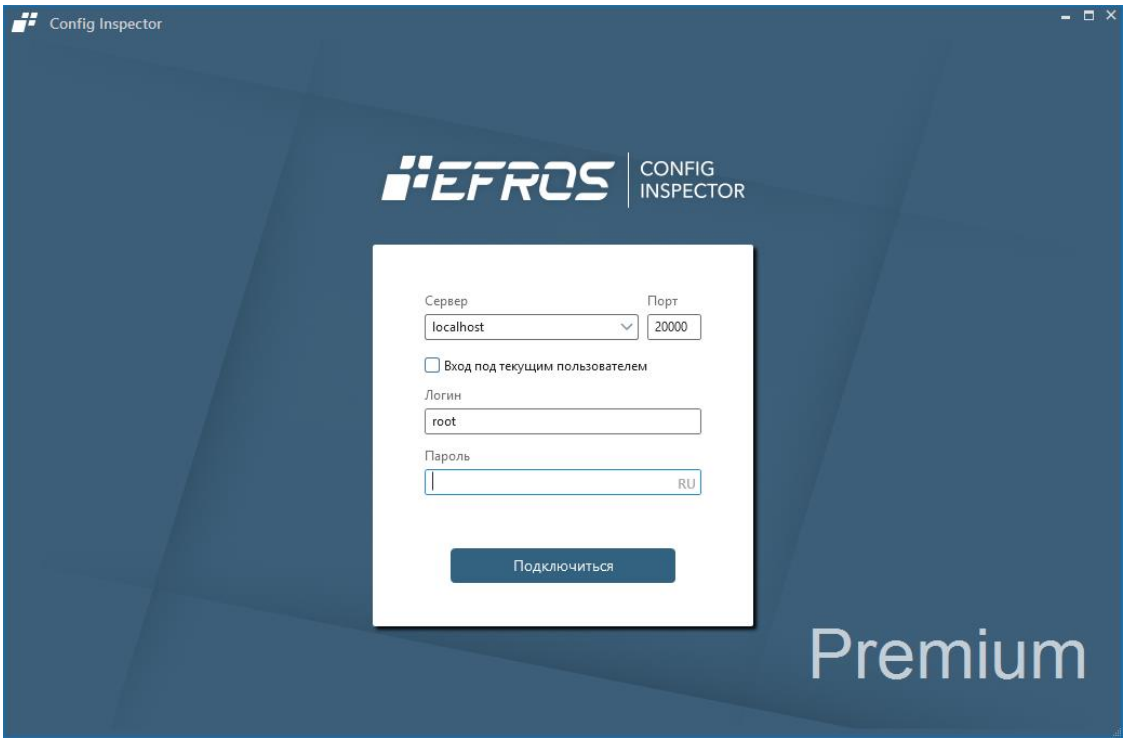


Рисунок 1 – Клиентская консоль, окно подключения

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 2.4.5.

После успешного завершения процесса аутентификации пользователя комплекса на сервере ПК откроется окно клиентской консоли комплекса. По умолчанию открывается раздел консоли по работе с устройствами (рис. 2).

Консоль имеет заголовок, панель выбора раздела и рабочую область.

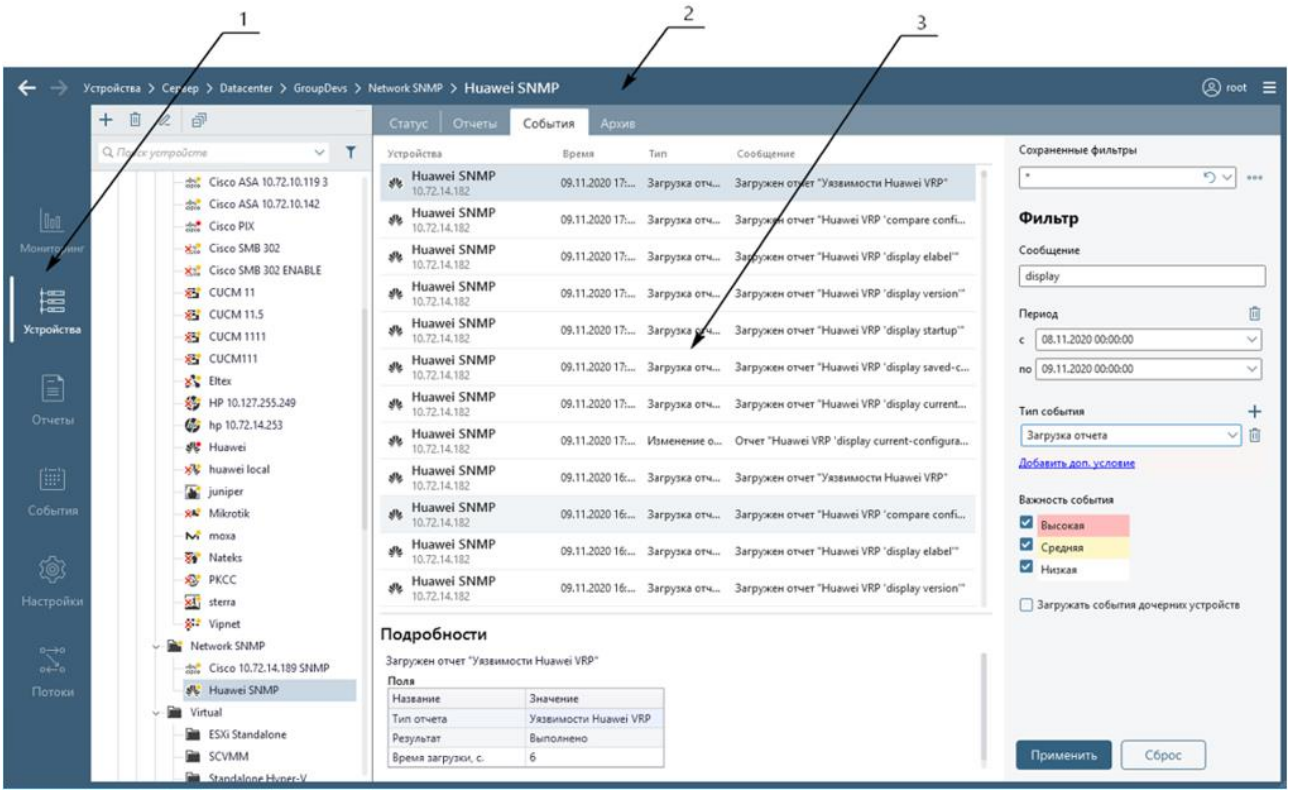


Рисунок 2 – Клиентская консоль, раздел **Устройства**

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 (рис. 3). Содержит панели

  а) ***Настройки контроля:***

  - ***Обработчики событий*** – задание триггеров для обработки событий, произошедших в работе сервера комплекса и/или устройств;
  - ***Профили*** – управление профилями для гибкой настройки параметров контроля устройств;
  - ***Устройства*** – управление и формирование списка устройств, управление отчетами, проверками, контроль доступности и конфигурации устройств.

Примечание – Дополнительно под кнопкой ***Устройства*** доступны ссылки ***Карта и Доступность устройств*** предназначенные, соответственно, для графического представления топологической карты локальной сети на основе информации контролируемых на текущем сервере ПК устройств и установки параметров проверки доступности устройств.

- ***Профили подключения*** – настройка параметров аутентификации пользователя на контролируемом комплексом оборудовании;
- ***Проверки безопасности*** – создание стандартов и настройка требований проверок безопасности для устройств;
- ***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;
- ***Экспорт настроек*** – экспорт выбранных настроек в файл формата .eci (профилей устройств, пользовательских отчетов и проверок, стандартов проверок межсетевых экранов, 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;
- ***Проверки межсетевых экранов*** – добавление стандартов проверок с возможностью анализа движения трафика по зонам (подсетям) и правил межсетевых экранов, настройка требований проверок безопасности межсетевых экранов;

б) ***Администрирование:***

- ***Модули*** – создание пользовательских, установка, подключение, отключение и настройка внешних модулей;
- ***Пользователи и группы*** – управление пользователями комплекса и правами доступа. 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, отключение пользователя);
- ***База данных*** – настройка сроков хранения данных в БД комплекса, 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;
- ***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 сервером ПК;

- ***Потоки*** – настройка и проверка подключения комплекса к серверу «Efros Security Center Flow Server» (далее – сервер «Flow Server»).

– ***Потоки*** – раздел предназначен для доступа к функционалу работы с данными, полученными с сервера «Flow Server». Функции программного компонента «Flow» комплекса доступны при активной лицензии, содержащей права на его использование. Вкладки раздела:
  – ***Триггеры*** – для задания триггеров с правилами формирования событий о зафиксированной сетевой активности;
  – ***События*** – для просмотра и анализа информации.

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».

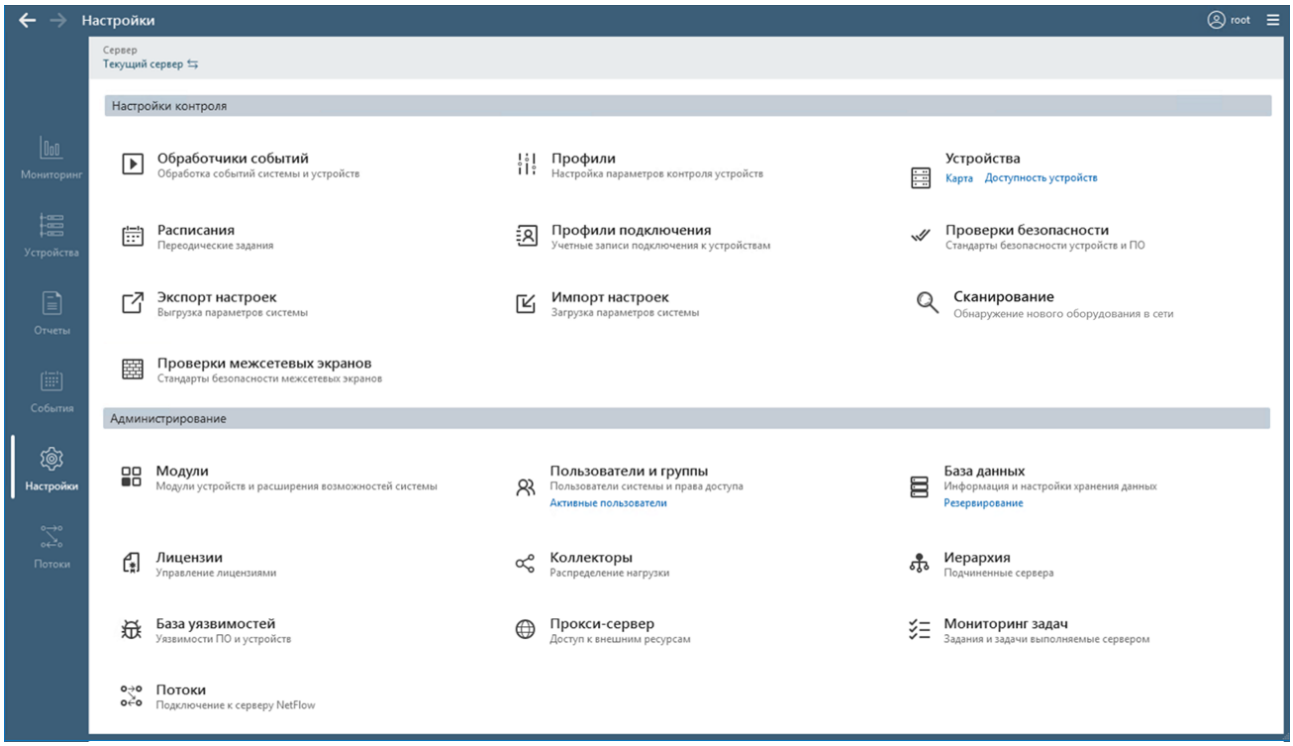


Рисунок 3 – Раздел **Настройки** клиентской консоли для главного в иерархии сервера

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 настройки контроля устройств пользователями, которым назначен доступ к настройкам комплекса в категории *Настройки контроля*, приведены в документе «643.72410666.00082-01 96 01-02 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 2. Настройки контроля».

Состав устройств, данные по которым доступны пользователю в разделах, и доступные действия с устройствами зависят от назначенных пользователю прав доступа к устройствам (см. пункт 1.3 «Пользователи ПК «Efros Config Inspector» v.4»).

Заголовок (рис. 2, поз. 2) содержит:

- 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 логин появляется возможность смены пароля либо выхода из консоли;
- кнопку вызова меню ☰, описание пунктов которого приведено в таблице 5.

Таблица 5 – Состав и описание пунктов меню заголовка клиентской консоли

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

Рисунок 4 – Окно просмотра сведений о программе

Более подробное описание и сведения о настройках, доступных в меню заголовка клиентской консоли, приведены в разделе 2 документа «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»).

В рабочей области (рис. 2, поз. 3) отображаются данные выбранной вкладки активного в текущий момент времени раздела консоли. Если при настройке 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. По умолчанию при открытии клиентской консоли в рабочей области отображается вкладка ***Статус*** раздела **Устройства**.

В заголовке раздела **Настройки** (см. рис. 3) расположена кнопка ***Сервер***, по нажатию которой открывается окно выбора сервера (рис. 5) 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***.

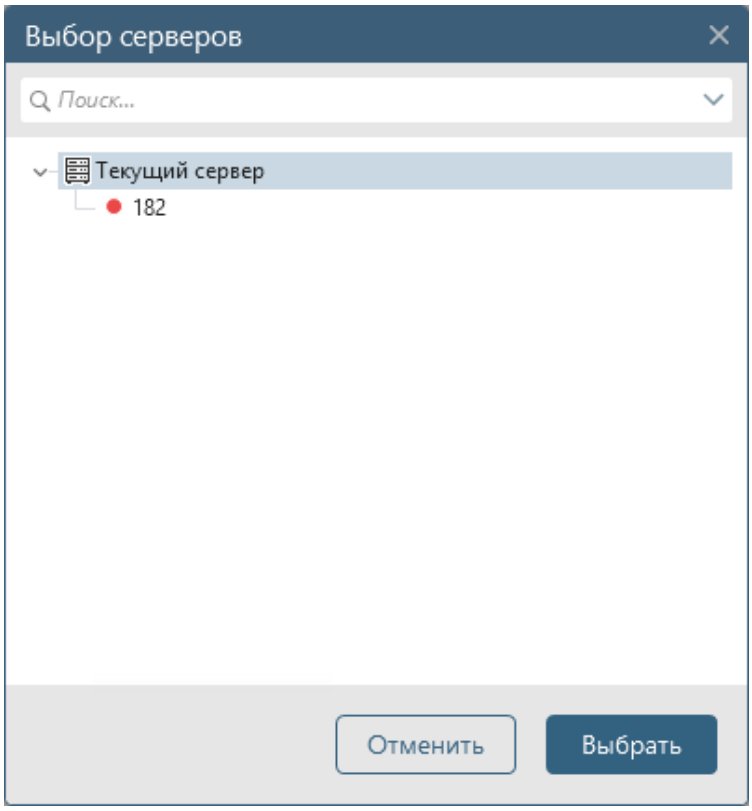


Рисунок 5 – Окно выбора сервера для настройки

В клиентской консоли пользователям, которым назначен доступ к настройкам комплекса в категории *Администрирование* (далее – администратор) доступны следующие настройки программного комплекса (для пользователей с правами *Просмотр* данные форм настройки доступны только для просмотра, для пользователей с правами *Управление* – для внесения изменения):

- ***Управление лицензиями комплекса.*** Активация, обновление лицензии для использования функциональных возможностей программного комплекса в полном объеме, удаление лицензии;
- ***Настройка внешних модулей***. Установка, подключение, отключение и настройка внешних модулей, обеспечивающих работу с устройствами;
- ***Формирование списка пользователей комплекса***. Список пользователей комплекса определяет, какие пользователи могут подключаться к серверу из консоли клиентской части;
- ***Настройка сроков хранения данных в БД ПК***. Настройка используется для экономии места на жестком диске;
- ***Настройка коллекторов задач***. Добавление новых коллекторов, настройка коллекторов;
- ***Настройка иерархии серверов***. Формирование иерархии серверов. Добавление новых серверов и настройка доступа к подчинённым серверам;
- ***Настройка обновления уязвимостей***. Настройка обновления базы данных уязвимостей;
- ***Настройка подключения к прокси-серверу БДУ.*** Настройка подключения комплекса к прокси-серверу БДУ;

– ***Просмотр списка задач комплекса.*** Контроль выполнения задач комплекса, просмотр логов операции для задач, выполнение которых завершилось с ошибкой;

– ***Настройка «Flow Server»***. Настройка и проверка подключения комплекса к серверу «Flow Server».

Перед выполнением настроек сервера ПК необходимо выбрать настраиваемый сервер в поле ***Сервер***. После выбора подчиненного сервера в форме становятся не доступны функции (рис. 6):

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

Кроме того, администратору доступен функционал по работе с устройствами и в том числе формирование списка подключенных к комплексу устройств (см. пункт 2.12 «Формирование списка и управление списком устройств»).

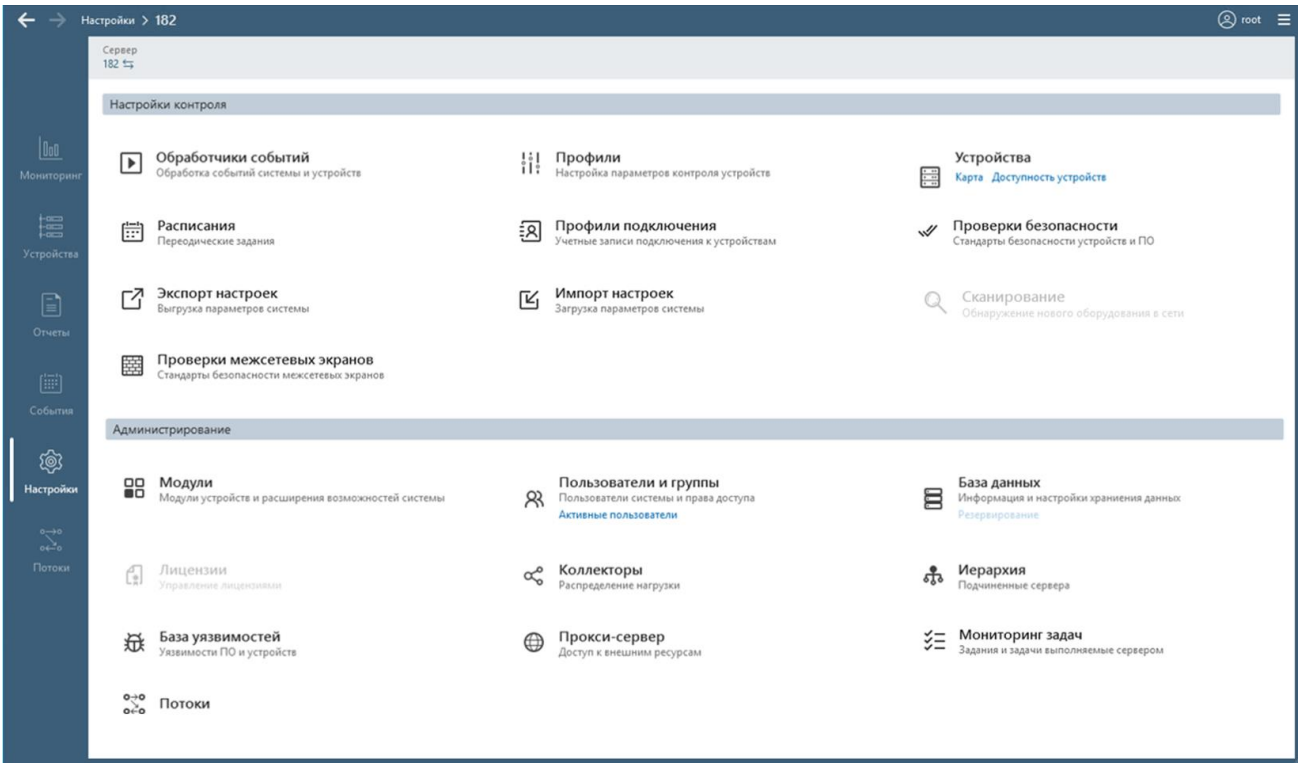


Рисунок 6 – Раздел ***Настройки*** для подчиненного сервера

2.2. Управление лицензиями комплекса

Для использования функциональных возможностей программного комплекса в полном объеме необходимо активировать лицензию на право использования продукта. В лицензии также указано максимальное количество устройств по типам, которое можно будет контролировать на сервере ПК с использованием вводимой лицензии.

Примечание – Управление лицензиями для серверов ПК в системе с иерархией серверов выполняется для каждого сервера ПК отдельно.

Пользователь может:

- активировать лицензию в соответствии с пунктами 2.2.1 – 2.2.3;
- просмотреть параметры активированных ранее лицензий (см. п. 2.2.4 «Просмотр параметров лицензий»);
- удалить лицензию по кнопке ***Удалить*** (🗑) (см. п. 2.2.5 «Удаление лицензии»);
- обновить активированную ранее лицензию по кнопке ***Обновить*** (см. п. 2.2.6 «Обновление лицензии»).

ВНИМАНИЕ: После окончания срока действия лицензии и при удалении лицензии в клиентской консоли будут скрыты все элементы за исключением подраздела ***Лицензирование*** раздела **Настройки,** и для возобновления работы ПК «Efros Config Inspector» v.4 необходимо выполнить активацию лицензии!

Примечание – Если ранее уже была активирована лицензия с использованием ключа старого формата, то при попытке добавления новой лицензии (по нажатию кнопки ***Добавить***) в соответствии с рисунком 7 откроется окно с предупреждением о необходимости удаления старой лицензии. Для активирования новой лицензии необходимо удалить все прежние лицензии, активированные с использованием ключа старого формата, и выполнить активацию новой лицензии в соответствии с пунктами 2.2.1 – 2.2.3.

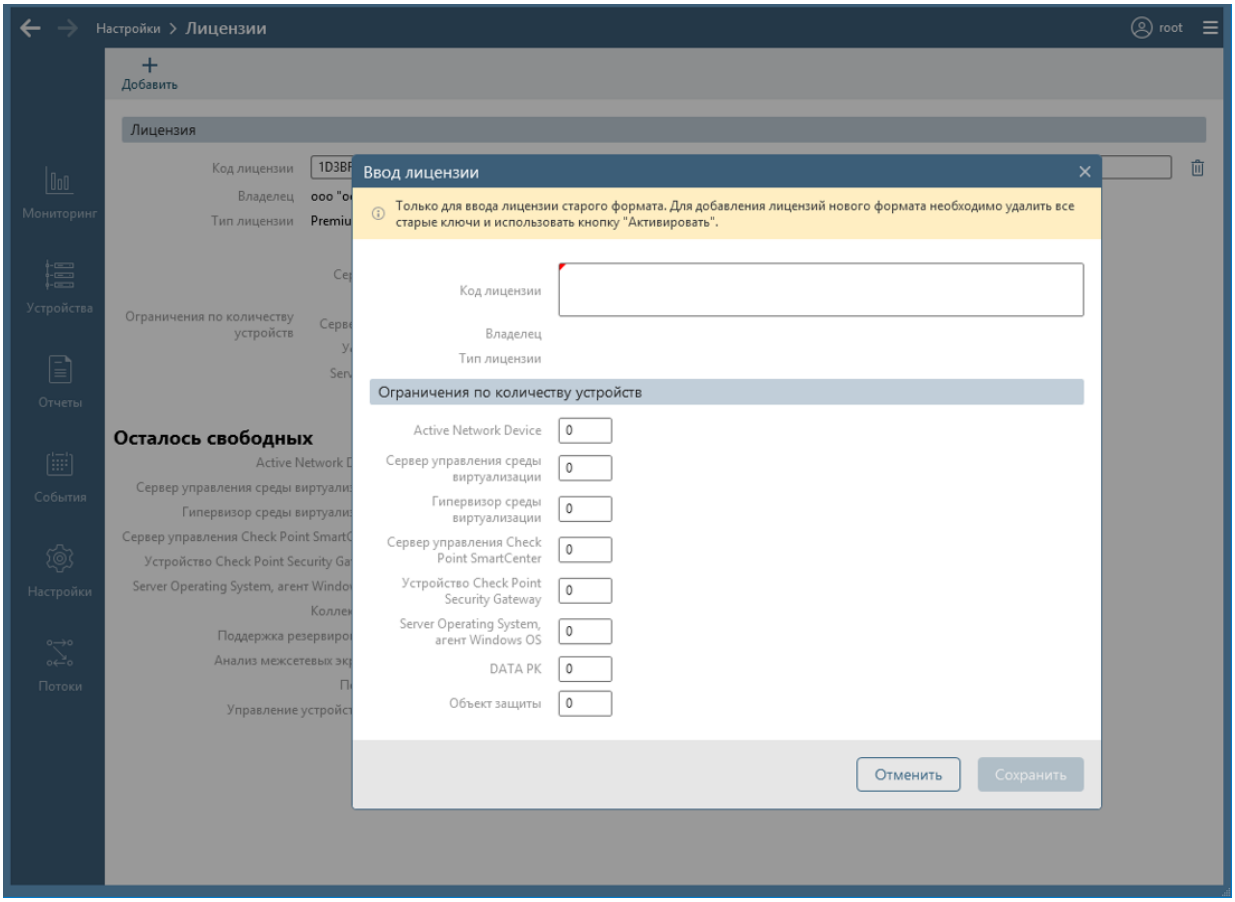


Рисунок 7 – Окно с предупреждением о необходимости удаления старой лицензии

2.2.1. Активация продукта

Для активации лицензии администратору комплекса необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки,** нажав соответствующую кнопку в панели выбора раздела клиентской консоли.

2) В области *Администрирование* (рис. 8) нажать кнопку ***Лицензии***.

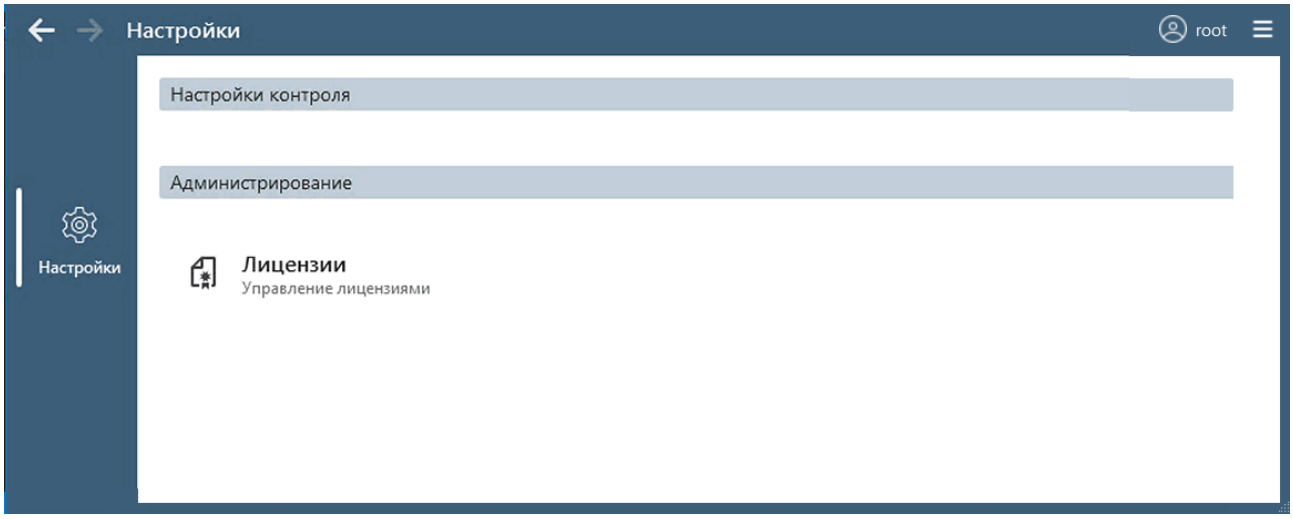


Рисунок 8 – Раздел **Настройки** до активации лицензии

3) В открывшейся форме управления лицензиями комплекса нажать кнопку ***Активировать***.

4) В открывшемся окне **Активация лицензии** (рис. 9) ввести в соответствующее поле ключ продукта, полученный от поставщика программного комплекса, и нажать кнопку ***Далее***.

При отсутствии подключения к серверу активации будет предложена офлайн активация лицензии (см. п. 2.2.2 «Офлайн активация лицензии»).

При вводе кода лицензии (система активации продукта для более ранних версий комплекса) будет выполнена активация продукта по коду лицензии (см. п. 2.2.3 «Активация продукта по коду лицензии»).

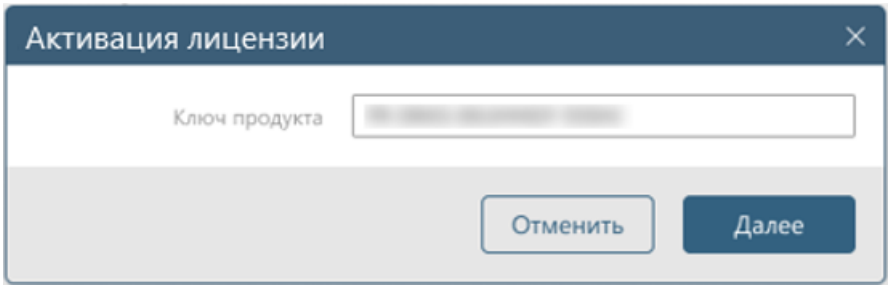


Рисунок 9 – Окно **Активация лицензии**

5) В открывшемся окне (рис. 10) ввести E-mail адрес для отправки кода активации и нажать кнопку ***Далее***.

6) В открывшееся окно (рис. 11) ввести код активации из полученного по электронной почте письма и нажать кнопку ***Далее***.

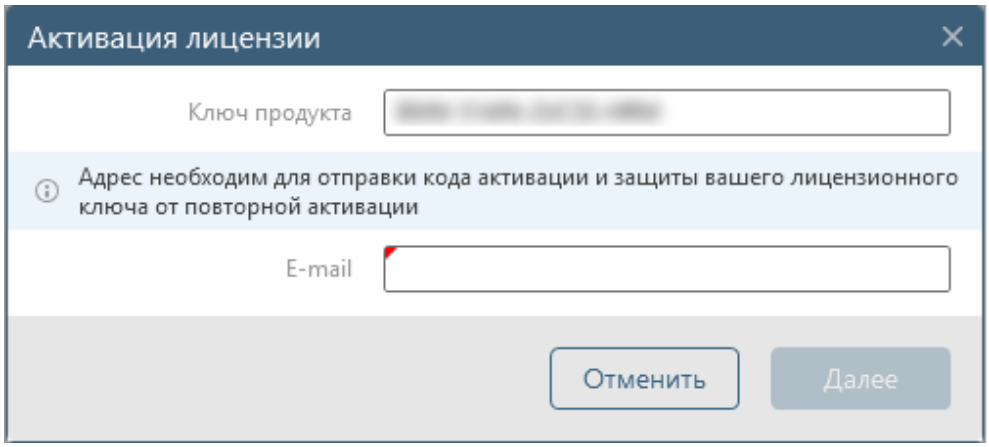


Рисунок 10 – Окно **Активация лицензии** с полем для ввода E-mail адреса

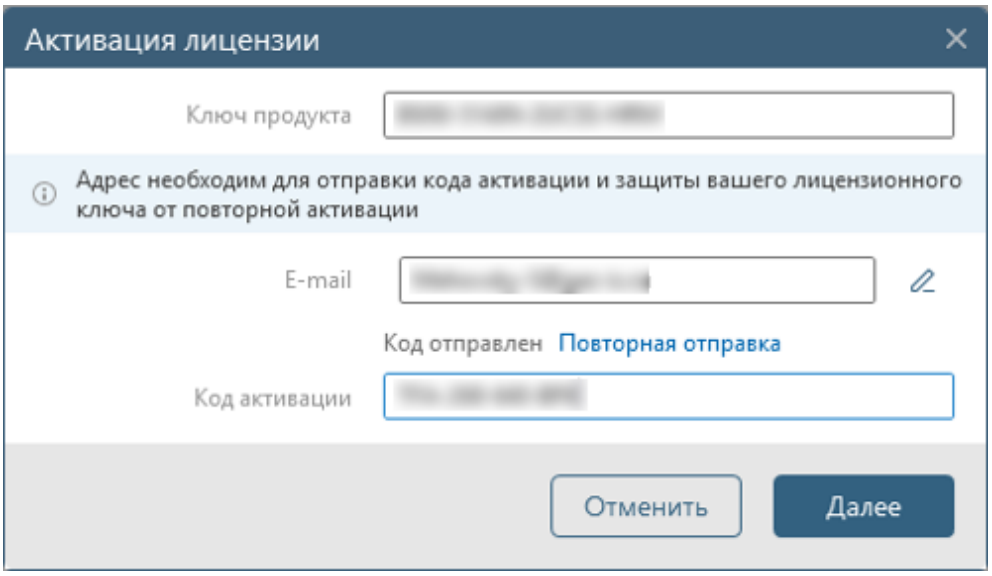


Рисунок 11 – Окно **Активация лицензии** с введенным кодом активации

7) При успешном завершении активации лицензии будет выведено сообщение о завершении активации копии продукта (рис. 12). На указанный адрес электронной почты придёт письмо с вложенным файлом активации, контактной информацией и реквизитами ООО «Газинформсервис» для обращения в техническую поддержку.

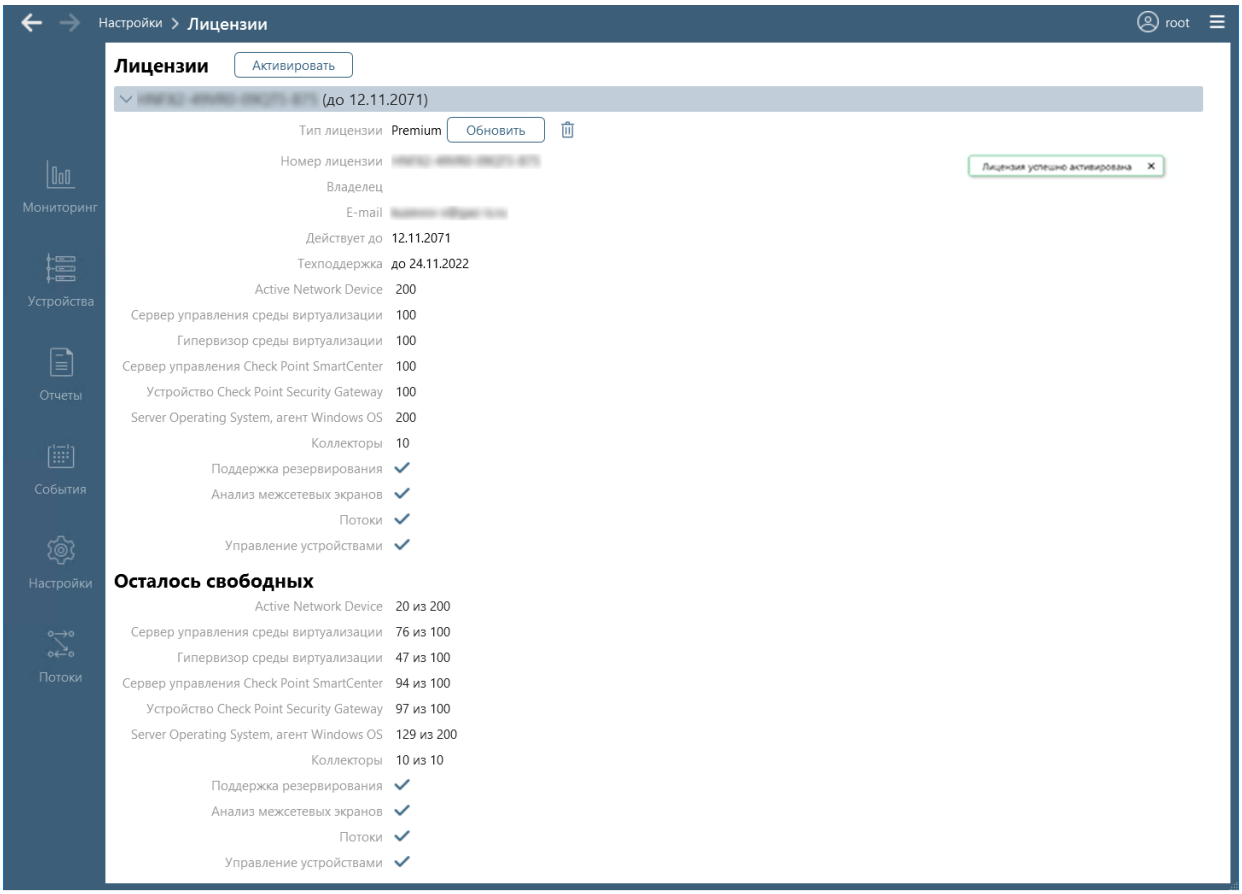


Рисунок 12 – Вид раздела **Лицензия** при успешном завершении активации лицензии с введенным кодом активации

2.2.2. Офлайн активация лицензии

Для офлайн-активации лицензии администратору комплекса необходимо выполнить следующие действия:

1) При отсутствии подключения к серверу активации продукта, после ввода ключа продукта в окне **Активация лицензии,** откроется окно с предложением повторить попытку подключения к серверу или активировать лицензию через браузер (рис. 13). Необходимо выбрать вариант продолжения активации лицензии и нажать кнопку ***Далее.*** При выборе варианта ***Повторить попытку*** будет выполнена попытка повторного подключения к серверу активации.

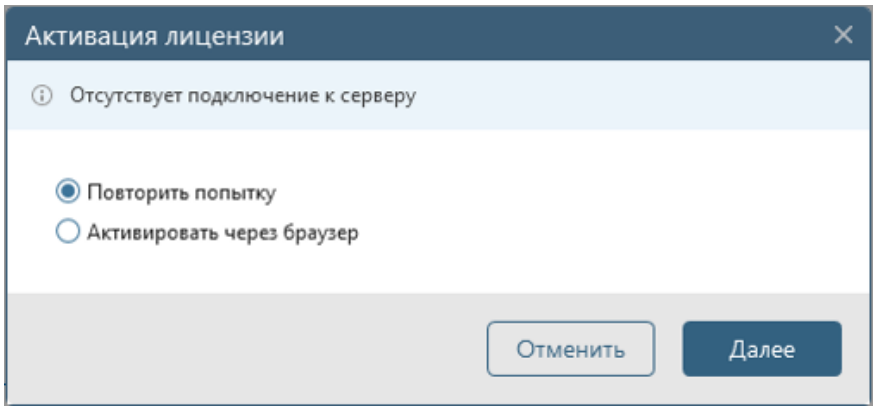


Рисунок 13 – Окно **Активация лицензии** с предложением выполнить активацию через браузер

2) При выборе варианта ***Активировать через браузер*** откроется окно для ввода адреса электронной почты пользователя (рис. 14). В открывшемся окне ввести E-mail адрес для отправки кода активации и нажать кнопку ***Далее***.

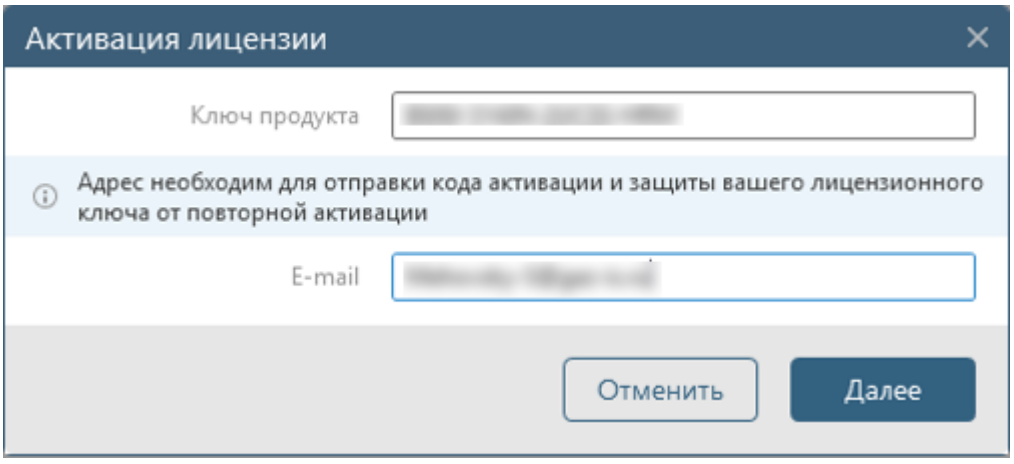


Рисунок 14 – Окно **Активация лицензии** с полем для ввода E-mail адреса

3) В результате выполненных действий в окне активации лицензии появится инструкция по проведению офлайн активации лицензии (рис. 15).

Скопировать код в буфер или сохранить в файл, выбрав соответствующую ссылку в пункте 1 инструкции.

Перейти на страницу центра офлайн активации продуктов ООО «Газинформсервис» для получения файла активации, выбрав в окне активации ссылку ***Сервер лицензирования*** (ведет на страницу центра офлайн активации продуктов: license.gaz-is.ru/offlineactivate/) в пункте 2 инструкции.

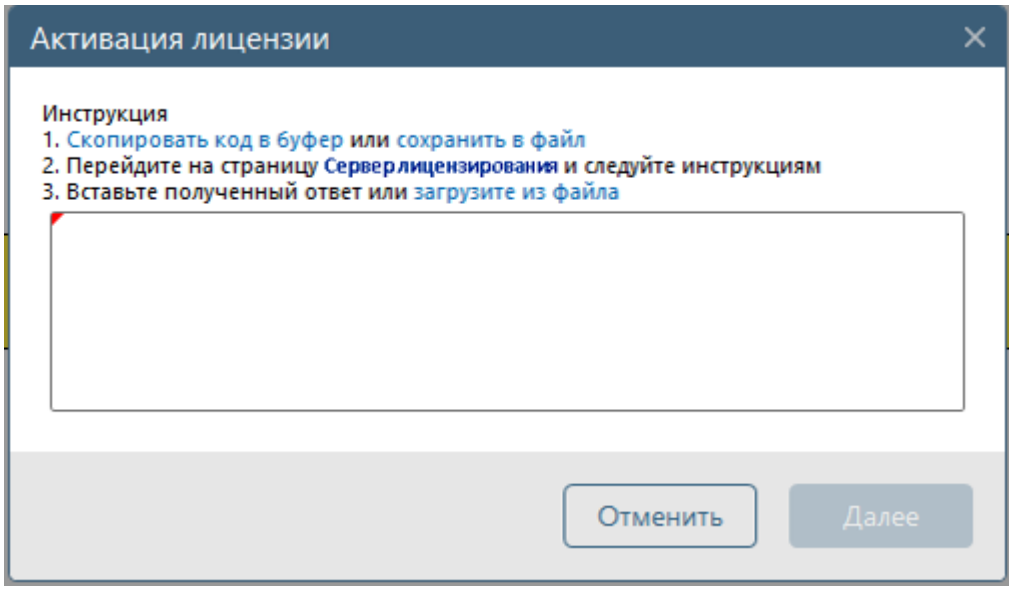


Рисунок 15 – Окно **Активация лицензии** с инструкцией

4) В поле ввода активационного запроса окна центра офлайн активации продуктов (рис. 16) вставить скопированные в буфер или файл данные и нажать кнопку ***Активировать***.

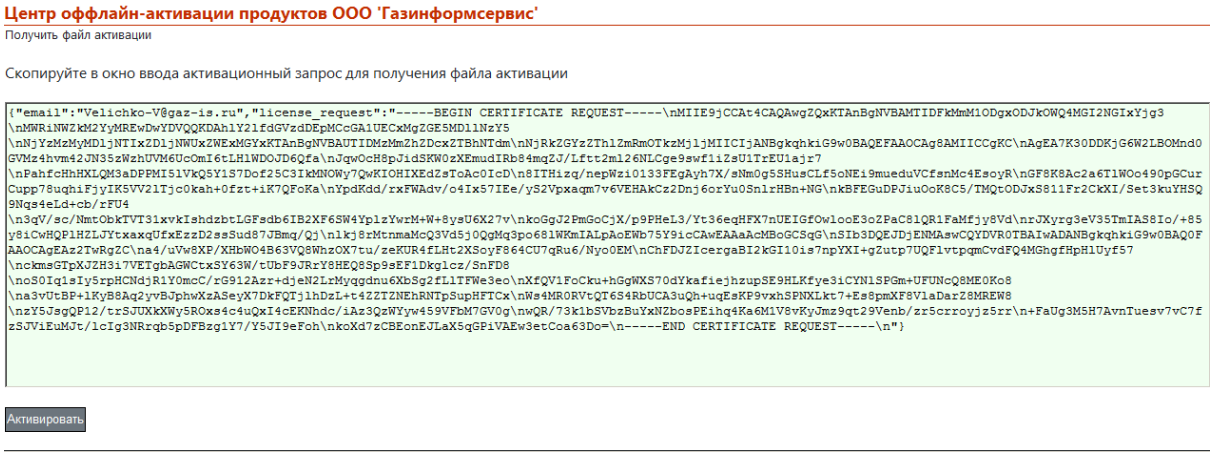


Рисунок 16 – Страница центра офлайн активации продуктов ООО «Газинформсервис»

5) В результате выполненных действий, в поле ввода активационного запроса появится сообщение ***Активация прошла успешно*** (рис. 17). Далее скопировать файл активации, нажав ссылку ***Скопировать в буфер обмена***, в окне центра офлайн активации продуктов.

6) В окно **Активация лицензии** (см. рис. 15) из буфера вставить файл активации и нажать кнопку ***Далее***.

7) При успешном завершении активации лицензии будет выведено сообщение о завершении активации копии продукта. На указанный адрес электронной почты придёт письмо с вложенным файлом активации и реквизитами ООО «Газинформсервис».

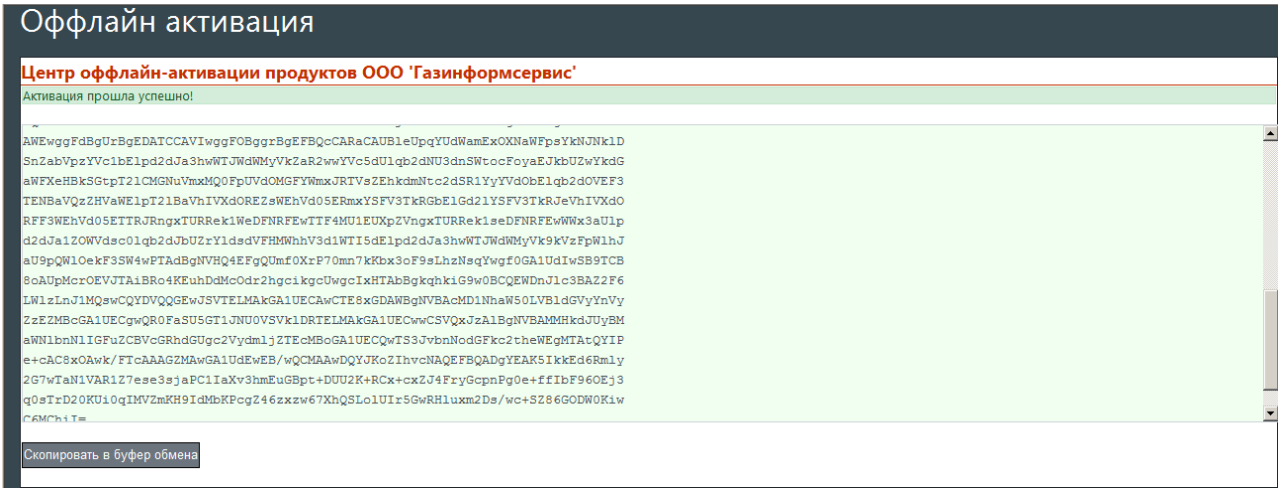


Рисунок 17 – Страница центра офлайн активации продуктов ООО «Газинформсервис» с результатами активации

2.2.3. Активация продукта по коду лицензии

Для активации продукта по коду лицензии администратору комплекса необходимо выполнить следующие действия:

1) При вводе кода лицензии (система активации продукта для более ранних версий комплекса) в поле ***Ключ продукта*** откроется окно **Активация лицензии** (рис. 18). В открывшемся окне нажать ссылку ***перейти в старое окно***

ввода лицензии и перейти в окно **Ввод лицензии** (рис. 19). Описание элементов управления, расположенных в окне Ввод лицензии, приведено в таблице 6.

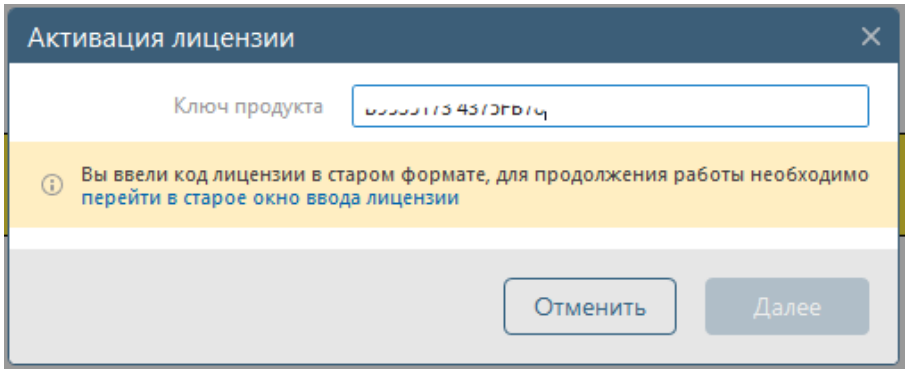


Рисунок 18 – Окно **Активация лицензии** для перехода к активации по коду лицензии

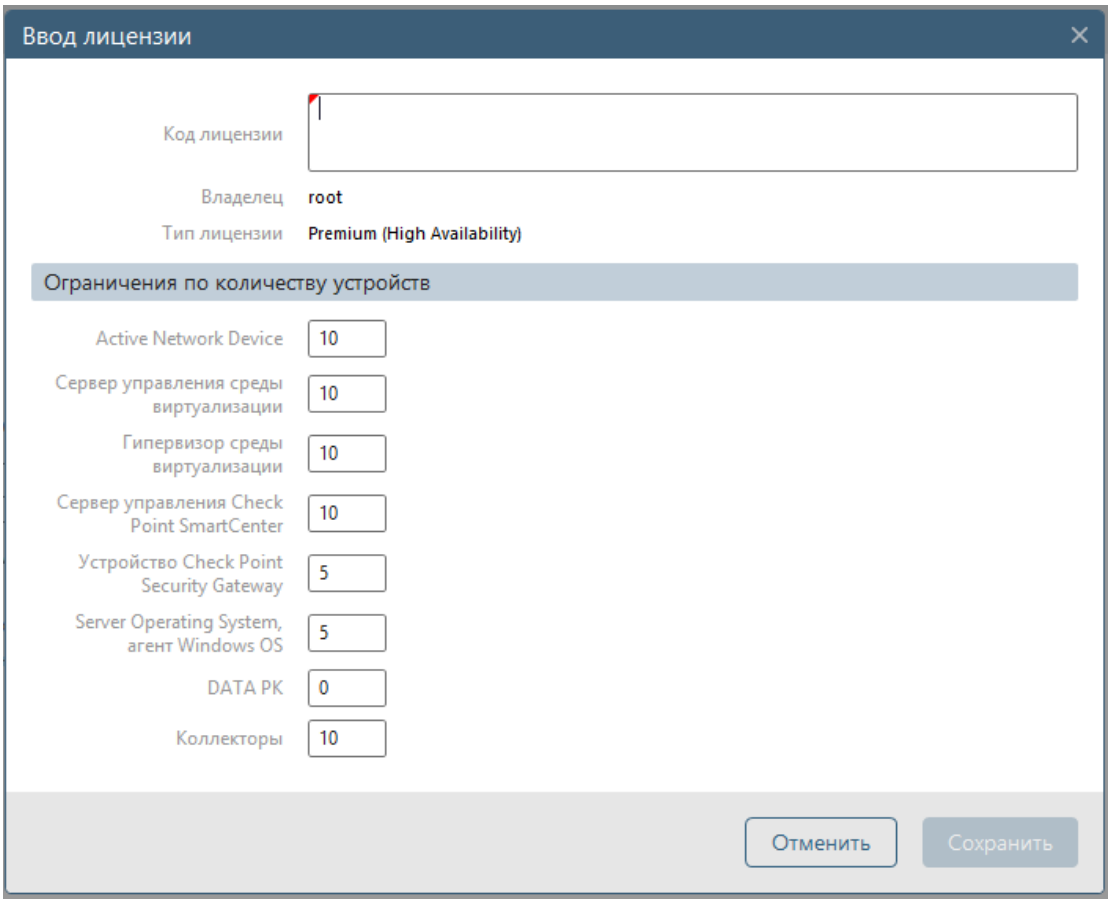


Рисунок 19 – Окно **Ввод лицензии**

Таблица 6 – Элементы управления окна ввода данных лицензии комплекса

Поле	Назначение
Код лицензии	Поле ввода кода лицензии, полученного от поставщика программного комплекса
Владелец	Имя организации-обладателя лицензии. Поле недоступно для редактирования
Тип лицензии	Используются *Premium* или *Standard* типы лицензий комплекса. Поле недоступно для редактирования

Поле	Назначение
Ограничения по количеству устройств	Список поддерживаемых комплексом типов устройств с указанием числа максимально возможного оборудования по типам, которое будет контролироваться на текущем сервере ПК с использованием вводимой лицензии. Поля недоступны для редактирования

2) В поле ***Код лицензии*** окна **Ввод лицензии** ввести имеющийся код лицензии и нажать кнопку ***Сохранить***.

3) При успешном завершении активации лицензии будет выведено сообщение о завершении активации копии продукта и откроется форма просмотра и изменения лицензионной информации комплекса (см. рис. 12).

2.2.4. Просмотр параметров лицензий

Для просмотра параметров лицензий администратору комплекса необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, нажав соответствующую кнопку в панели выбора раздела консоли.

2) В области *Администрирование* нажать кнопку ***Лицензии***.

3) В открывшейся форме управления лицензиями комплекса (рис. 20) будут отображаться блоки индивидуальных параметров лицензий с заголовками в формате: <номер лицензии> (до <дата окончания действия лицензия>) и блок **Осталось свободных** с обобщенными данными по всем активным лицензиям.

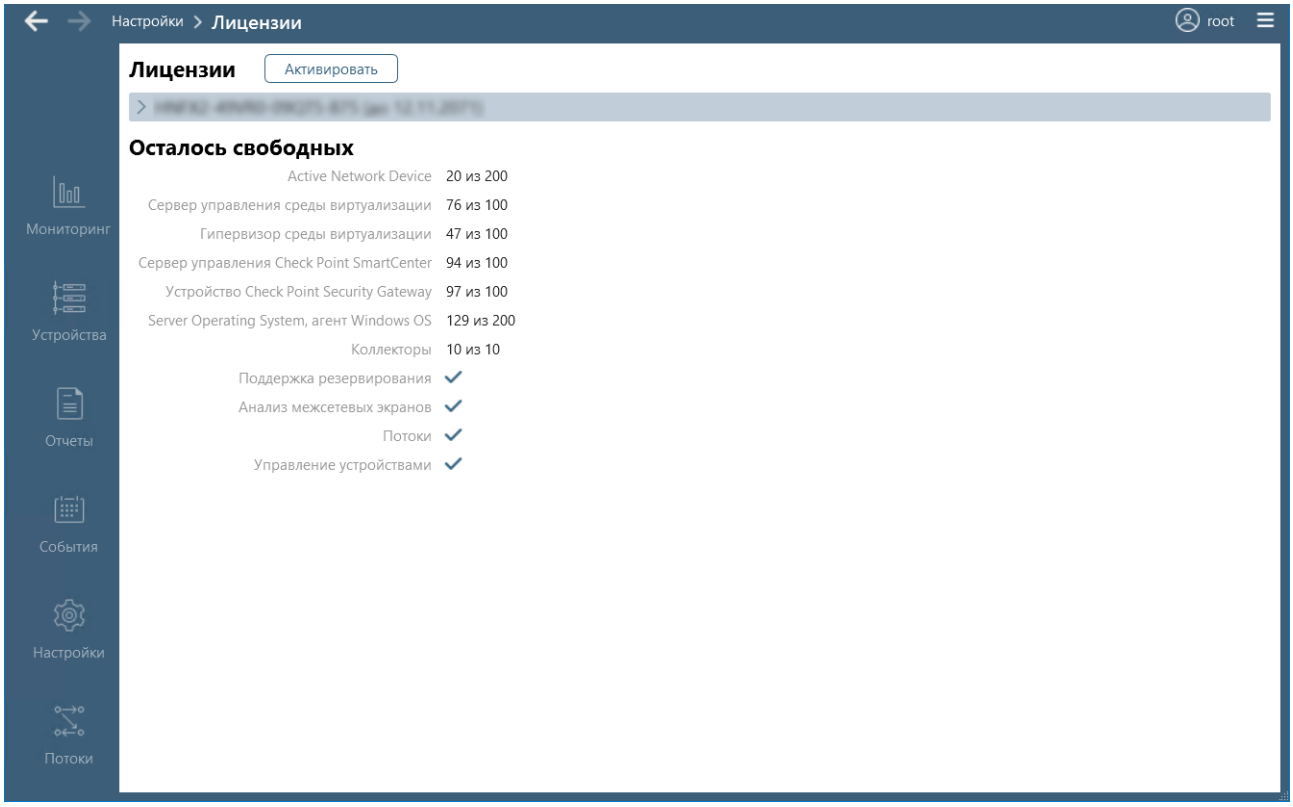


Рисунок 20 – Форма управления лицензиями комплекса

Блоки индивидуальных параметров лицензий по умолчанию свернуты. Для просмотра подробных сведений необходимо выбрать с помощью «мыши» заголовок требуемой лицензии (рис. 21). В блоке отображаются данные: тип лицензии, номер лицензии, данные владельца лицензии, срок действия лицензии, максимальное количество устройств по типам, которое можно будет контролировать на сервере ПК с использованием этой лицензии, включенные в лицензию дополнительные модули (например, *Потоки*, *Управление устройствами*)

Блок **Осталось свободных** всегда отображается в развернутом виде и содержит данные об общем количестве устройств по типам, которое можно контролировать на сервере ПК с использованием всех активных лицензий, и количестве доступных для подключения в текущий момент устройств соответствующих типов, а также перечень дополнительных модулей, включенных во все активные лицензии.

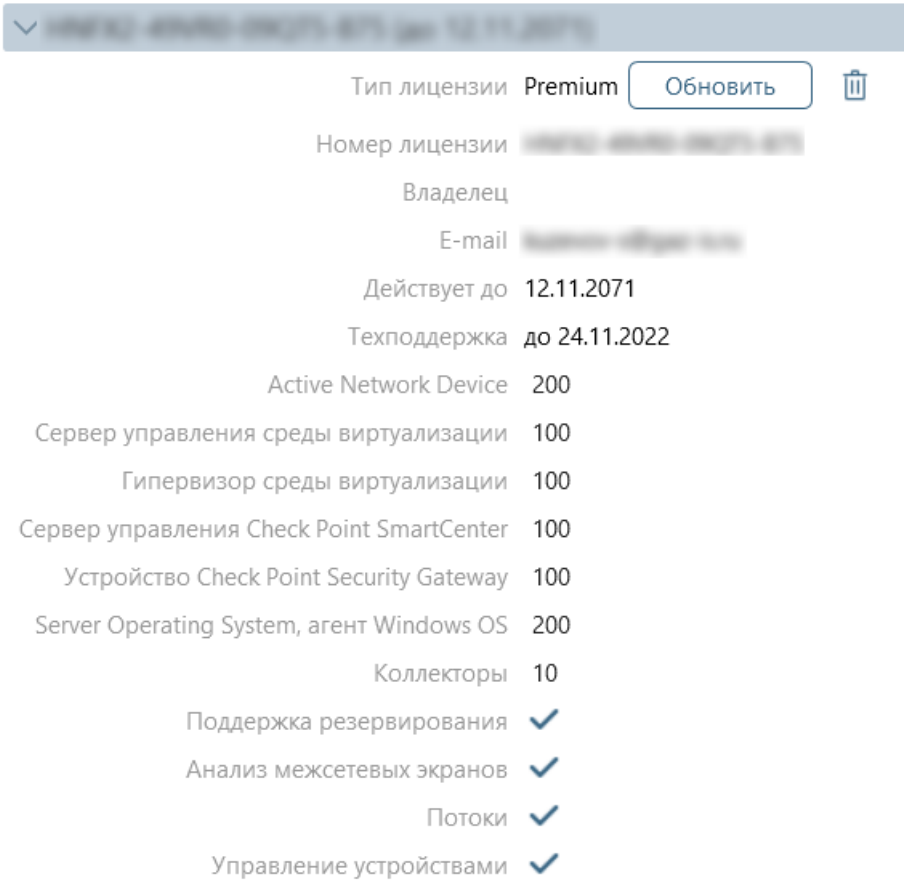


Рисунок 21 – Блок просмотра индивидуальных параметров лицензии

2.2.5. Удаление лицензии

Для удаления лицензии администратору комплекса необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, нажав на соответствующую кнопку в панели выбора раздела консоли.
2) В области *Администрирование* нажать кнопку ***Лицензии***.
3) В открывшейся форме управления лицензиями комплекса нажать кнопку ***Удалить лицензию*** (🗑), расположенную справа от удаляемой лицензии.

4) Подтвердить операцию удаления выбранной лицензии с сервера ПК, нажав кнопку ***Удалить*** в открывшемся окне.

5) Произойдет возврат в форму управления лицензиями, в которой изменится информация о максимальном количестве контролируемого текущим сервером ПК оборудования. Дальнейшая работа в консоли комплекса будет невозможна. Также в консоли появится незакрываемый баннер с надписью о необходимости ввода лицензии.

2.2.6. Обновление лицензии

Для обновления лицензии администратору комплекса необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки,** нажав соответствующую кнопку в панели выбора раздела консоли.

2) В области *Администрирование* нажать кнопку ***Лицензии***.

3) В открывшейся форме управления лицензиями комплекса нажать кнопку ***Обновить***, расположенную справа от лицензии.

4) При наличии подключения к серверу лицензирования произойдет подключение к серверу и проверка наличия обновления лицензии. При наличии обновления будет выполнено обновление лицензии и выведено сообщение ***Лицензия обновлена.*** При отсутствии обновления будет выведено соответствующее сообщение.

При отсутствии подключения к серверу лицензирования выводится сообщение ***Ошибка подключения к серверу лицензирования,*** содержащее ссылку ***Офлайн обновление*** для перехода к процедуре офлайн обновления лицензии (см. п. 3 пункта 2.2.2 «Офлайн активация лицензии»).

2.3. Управление внешними модулями

2.3.1. Загрузка (установка) внешних модулей

В ПК «Efros Config Inspector» v.4 для взаимодействия с оборудованием и программным обеспечением различных производителей используются внешние модули. Некоторые модули устанавливаются автоматически, одновременно с установкой серверной части комплекса. Список доступных модулей можно увидеть, перейдя на вкладку ***Модули*** клиентской консоли комплекса (рис. 22) сразу после установки серверной части комплекса и клиентской консоли. Также на установочном диске ПК «Efros Config Inspector» v.4, в каталоге *Modules*, расположены дистрибутивы дополнительных внешних модулей – для возможности подключения к серверу ПК требуется их отдельная установка. Кроме того, пользователи с правами *Управление* категории *Администрирование* имеют возможность добавить пользовательские модули для подключения отдельных типов устройств.

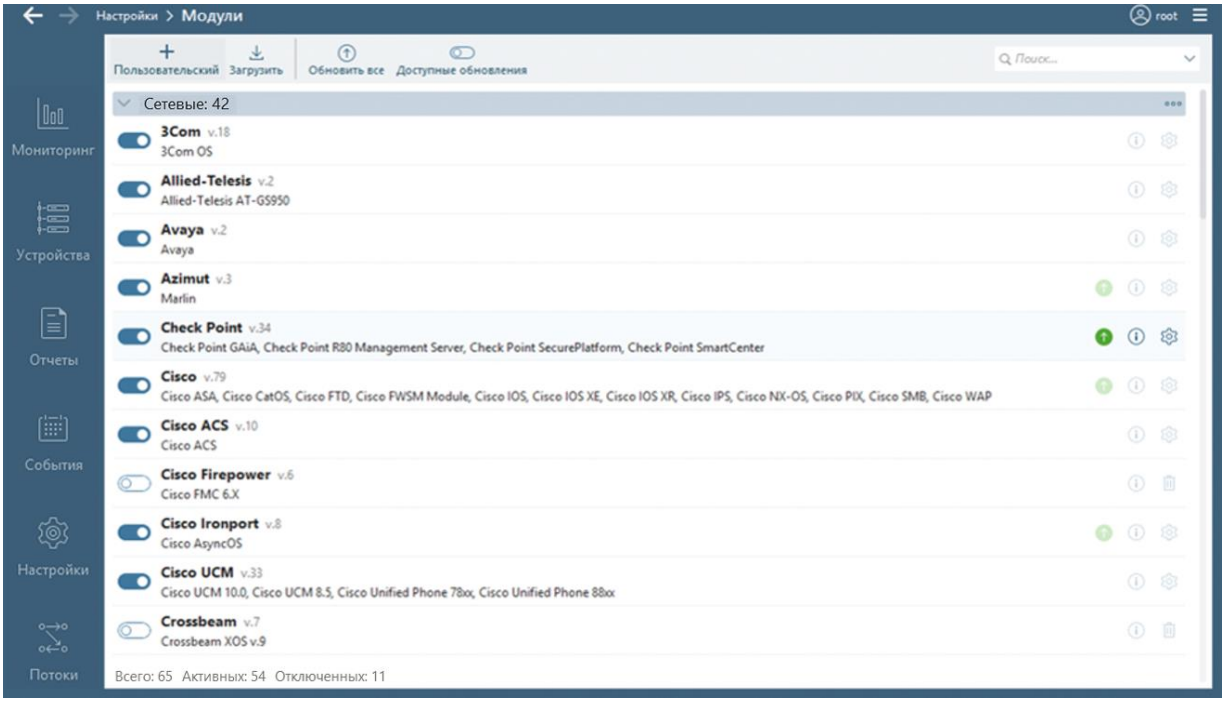


Рисунок 22 – Форма управления внешними модулями

Список установленных на сервере ПК модулей разделен на категории:

- ***Сетевые*** – модули поддержки сетевых устройств;
- ***Виртуализация*** – модули поддержки устройств виртуальной инфраструктуры;
- ***Операционные системы*** – модули поддержки устройств с указанными операционными системами;
- ***Прикладное программное обеспечение*** – модули поддержки АСУ ТП и другого прикладного программного обеспечения (ППО);
- ***Сервисные*** – модули, предназначенные для обработки событий, произошедших на сервере ПК, а также приема syslog-сообщений.

После добавления пользовательского модуля в списке модулей добавляется категория ***Пользовательские***.

В заголовке каждой категории указано количество активных (подключенных) в текущий момент модулей соответствующей категории. В нижней части страницы приведены данные об общем количестве внешних модулей, количестве активных и неактивных (отключенных)- на текущий момент времени.

Инсталляция, подключение, отключение, обновление, удаление и настройка внешних модулей выполняются во вкладке ***Модули***, доступной из раздела **Настройки**.

Примечание – Перед выполнением настроек модулей сервера ПК необходимо выбрать настраиваемый сервер в поле ***Сервер*** раздела **Настройки**

Для установки дополнительного внешнего модуля на сервер ПК необходимо:

1) В окне клиентской консоли перейти на вкладку ***Модули***, для чего в области *Администрирование* раздела **Настройки** нажать кнопку ***Модули***.

2) В заголовке вкладки ***Модули*** нажать кнопку ***Загрузить*** (). Откроется стандартное окно MS Windows **Открыть**, в котором необходимо указать файл (при

помощи клавиш **<Ctrl>** или **<Shift>** можно выбрать сразу несколько файлов) дистрибутива устанавливаемого модуля и нажать кнопку ***Открыть***.

3) В открывшемся окне загрузки выбранных модулей откорректировать список устанавливаемых модулей, отметив или сняв отметку напротив имени модуля, и нажать кнопку ***Загрузить*** (рис. 23).

Если в системе уже установлен загружаемый модуль, то будет выведено соответствующее предупреждение. Переключатели ***Включить после загрузки*** и ***Обновить автоматически*** (если имеется обновление модуля) позволяют задать параметры, соответственно, включения или обновления загружаемых на сервер ПК внешних модулей:

- включенный (– положение по умолчанию) переключатель – выбранные для загрузки модули (или обновления их версии) будут включены сразу же после загрузки модулей на сервер;
- выключенный ( ) переключатель – для включения модуля или обновления его версии необходимо выполнить действия, указанные в соответствующих подпунктах данного пункта.

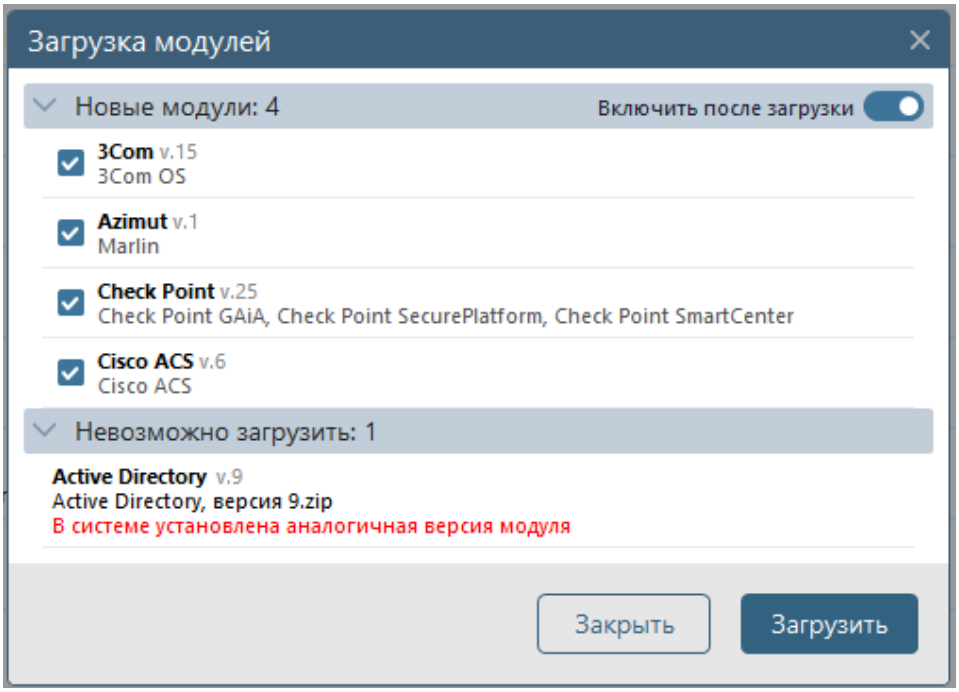


Рисунок 23 – Окно со списком устанавливаемых на сервер ПК модулей

4) Во время процесса установки выбранных модулей на сервер ПК в окне консоли будут появляться сообщения о загрузке на сервер ПК соответствующего внешнего модуля.

2.3.2. Подключение внешних модулей

После установки внешнего модуля необходимо произвести его подключение к серверной части комплекса.

В случае наличия загруженных на сервер ПК обновлений модулей, в форме управления модулями комплекса появляется кнопка ***Обновить все*** ( ) и переключатель ***Доступные обновления*** (/).

Отмеченный переключатель ***Доступные обновления*** позволит оставить в форме только список модулей, которые требуют обновления.

Нажатие на кнопку ***Обновить все*** запустит процесс обновления для всех внешних модулей, установленных на сервере ПК, новые версии которых были загружены на сервер.

В области *Обновления* окна загрузки модулей можно ознакомиться с информацией о внесенных в работу загружаемой версии модуля изменениях – для этого нажмите кнопку ***Сведения***, расположенную в строке с именем модуля. В результате откроется окно со списком внесенных в работу модуля изменений. Для закрытия информационного окна и возврата в окно загрузки модулей нажмите кнопку ***Закрыть***.

Слева от наименования внешнего модуля отображается переключатель включения/отключения модуля: «» – модуль выключен, «» – модуль включен. Справа от наименования внешнего модуля указан номер версии установленного модуля, а под наименованием модуля приведен краткий список поддерживаемых модулем типов устройств. При наведении на строку с именем модуля справа от имени становятся активными кнопки ***Сведения*** и ***Настройки***. Описание элементов управления, расположенных в форме управления внешними модулями, приведено в таблице 7.

Таблица 7 – Элементы управления в форме управления внешними модулями

Элемент	Обозначение	Назначение
Переключатель ***Подключить/ Отключить***	/	Подключение/отключение внешнего модуля. При включении модуля открывается окно настройки его параметров (например, настройки сервера для отправки писем, настройка режима хранения логов (включен/отключен) и т.д.)
Кнопка ***Подключить все/ Отключить все***		Подключение/отключение всех внешних модулей в категории. Отображается только в строке заголовка категории модулей
Кнопка ***Обновить***		Выполнение операции обновления установленного на сервере ПК внешнего модуля. Кнопка появляется после загрузки на сервер ПК обновленной версии модуля
Кнопка ***Сведения***		Переход в окно с информацией обо всех изменениях, которые произошли в работе модуля от версии к версии. Кнопка становится активной при наведении курсора мыши на строку с именем модуля
Кнопка ***Настройки***		Переход в окно настроек параметров внешнего модуля. Кнопка становится активной при наведении курсора «мыши» на строку с именем модуля. Кнопка становится активной только для подключенного модуля, у которого есть параметры для настройки

Элемент	Обозначение	Назначение
Кнопка ***Удалить***		Выполнение операции удаления внешнего модуля с сервера ПК. Кнопка присутствует только у отключенных модулей

Для каждого внешнего модуля комплекса в форме управления модулями клиентской консоли администратору доступны операции установки, подключения, отключения, обновления, изменения настроек подключенных внешних модулей и удаления модулей с сервера ПК.

Для подключения внешнего модуля:

– в форме управления модулями комплекса (см. рис. 22) выполните щелчок левой кнопкой «мыши» по переключателю  , расположенному слева от имени требуемого модуля. В некоторых случаях перед включением модуля откроется окно настройки параметров работы модуля. На рис. 24 приведен пример окна для модуля ***Экспорт событий***;

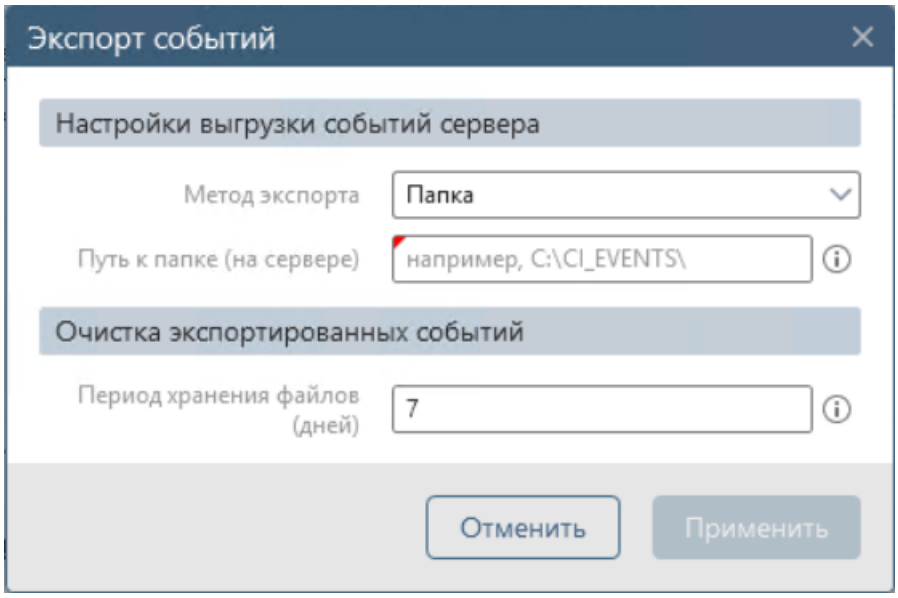


Рисунок 24 – Окно настройки параметров внешнего модуля ***Экспорт событий***

– внесите требуемые изменения в параметры работы модуля (подробное описание настраиваемых параметров внешних модулей приведено в файле *Описание модулей.chm*, поставляемом на дистрибутивном диске);

– нажмите кнопку ***Применить***. По окончании процесса подключения в форме управления внешними модулями появится сообщение о подключении модуля к серверной части комплекса, переключатель слева от наименования модуля окрасится в синий цвет, в строке подключенного модуля вместо кнопки ***Удалить*** () отобразится кнопка ***Настройки*** ().

Для модуля **Управление устройствами** при настройке вводятся параметры подключения к серверу, после ввода параметров и нажатия кнопки ***Применить*** под названием модуля отображается ссылка ***Проверка подключения к серверу***. По нажатию ссылки запускается выполнение проверки подключения, открывается окно просмотра результатов выполнения операции. По завершении проверки в поле

Состояние операции окна отображается результат выполнения (успешно, неуспешно). Пользователь имеет возможность, при необходимости, внести изменения в настройки подключения и повторить проверку подключения.

Подключать установленные внешние модули к комплексу можно и в процессе установки на сервер других модулей.

После подключения внешнего модуля, обеспечивающего взаимодействие комплекса с устройствами конкретного типа, станет доступна функция добавления соответствующих устройств в список контролируемого оборудования.

В клиентской консоли ПК «Efros Config Inspector v.4» реализована возможность группового подключения модулей, которые не содержат индивидуальные параметры настройки работы. В строке с именем категории модулей нажмите кнопку (…) и в открывшемся меню выберите пункт ***Подключить все***. По окончании процесса подключения модулей в форме управления внешними модулями будут появляться сообщения о подключении модулей к комплексу.

2.3.3. Добавление пользовательского модуля

Для добавления пользовательского модуля для подключения к комплексу отдельных типов устройств пользователю необходимо:

1) В окне клиентской консоли перейти на вкладку ***Модули***, для чего в области ***Администрирование*** раздела **Настройки** нажать кнопку ***Модули***.

2) В заголовке вкладки ***Модули*** нажать кнопку ***Пользовательский*** (+). Откроется окно **Новый тип сетевого устройства** (рис. 25, таблица 8), в котором необходимо указать параметры взаимодействия ПК «Efros Config Inspector» v.4 с новым типом устройств.

3) Для проверки подключения устройства, заполнить поля блока *Тестирование* и нажать кнопку ***Проверить подключение***. Для просмотра результатов проверки – нажать текст-ссылку в поле *Результат проверки*.

4) Нажать кнопку ***Применить***. Окно закроется, в списке модулей в категории ***Пользовательские*** добавится строка с новым модулем. Пользовательский модуль доступен, как и другие модули, для редактирования настроек, отключения/подключения и удаления.

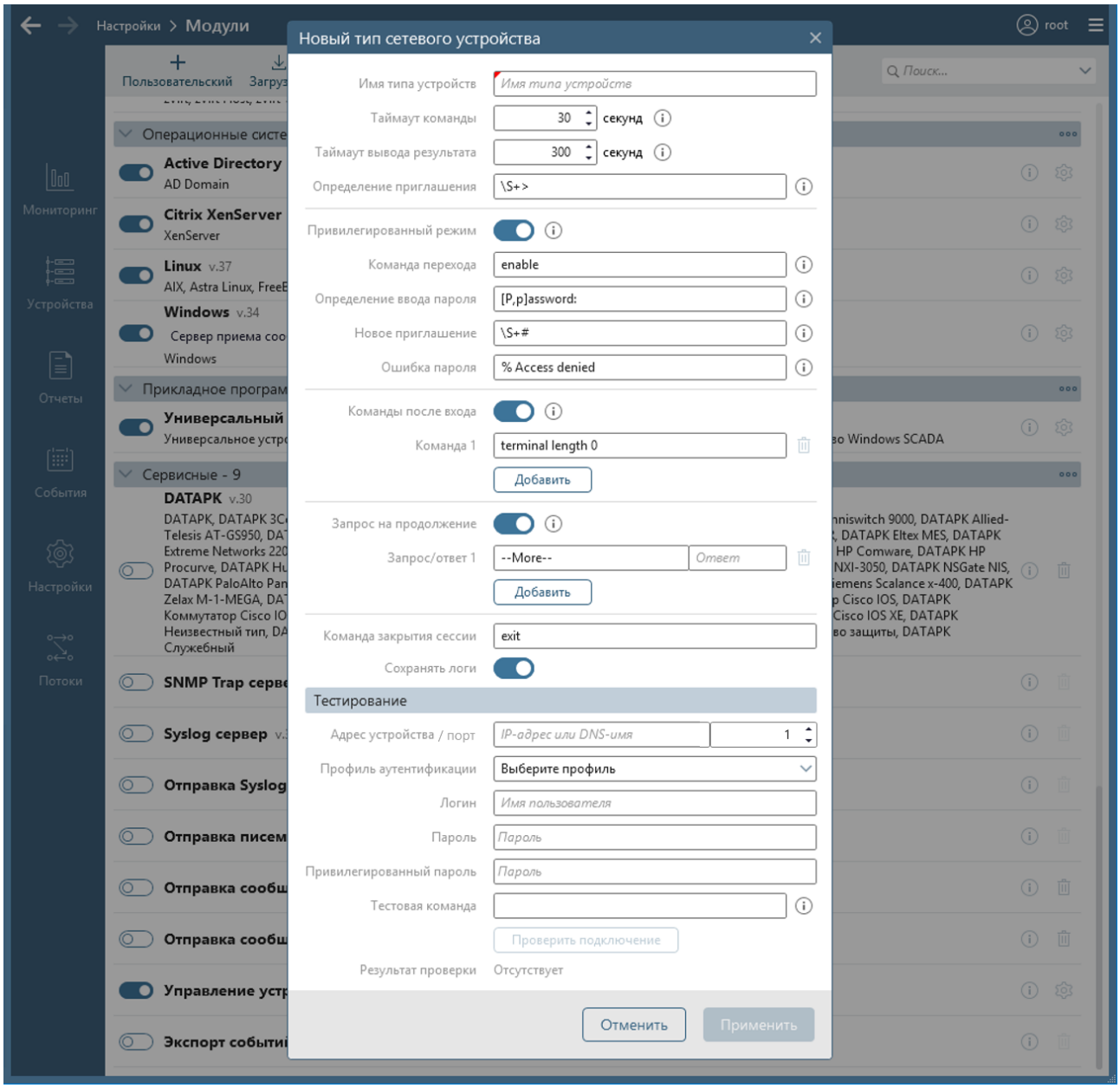


Рисунок 25 – Окно ***Новый тип сетевого устройства***

Таблица 8 – Состав и описание полей окна добавления нового модуля

Поле	Описание/Назначение
Группа параметров модуля	
Имя типа устройств	Имя нового типа устройств
Таймаут команды	Время ожидания ответа при выполнении команд на устройстве
Таймаут вывода результата	Время ожидания вывода результата при запросе конфигурации устройства
Определение приглашения	Регулярное выражение для определения вида приглашения. По умолчанию соответствует приглашению вида «Text>»
Привилегированный режим	Переключатель. Устанавливает необходимость перехода в привилегированный режим для выполнения команд на устройстве. По умолчанию переключатель установлен в положение *Включен* и

Поле	Описание/Назначение
	поля для ввода параметров работы в привилегированном режиме (см. ниже) отображаются в окне
Поля для ввода параметров работы в привилегированном режиме	
Команда перехода	Команда перехода в привилегированный режим. Значение по умолчанию: *enable*
Определение ввода пароля	Регулярное выражение для определения приглашения ввода пароля при переходе в привилегированный режим
Новое приглашение	Регулярное выражение для определения вида приглашения в привилегированном режиме. Если приглашение не меняется, то поле оставляется пустым
Ошибка пароля	Регулярное выражение для определения ошибки пароля
Команды после входа	Переключатель. Устанавливает наличие дополнительных команд для настройки устройства. По умолчанию переключатель установлен в положение *Включен* и поля для ввода команд *Команда 1..N* (см. ниже) отображаются в окне
Команда 1..N	Поля для ввода дополнительных команд для настройки устройства. Справа от поля расположена кнопка удаления поля (🗑)
Кнопка Добавить	По нажатию кнопки добавляется новое поле для дополнительной команды
Запрос на продолжение	Переключатель. Устанавливает наличие запроса на продолжение вывода ответа на выполнение команды. По умолчанию переключатель установлен в положение *Включен* и поля для ввода запросов/ответов *Запрос/ответ 1..N* (см. ниже) отображаются в окне
Запрос/ответ 1…N	Поля для ввода регулярных выражений запросов и соответствующих ответов. По умолчанию, если поле на заполнено, то будет отправляться «пробел». Справа от поля расположена кнопка удаления поля (🗑)
*Кнопка **Добавить***	По нажатию кнопки добавляется новое поле для дополнительного запроса/ответа
Команда закрытия сессии	Команда закрытия сессии
Сохранять логи	Переключатель. Устанавливает необходимость сохранения логов сессии
Группа ***Тестирование***	
Адрес устройства/порт	IP-адрес или доменное имя устройства и п подключения
Профиль аутентификации	Раскрывающийся список поля содержит наименования профилей аутентификации, имеющихся на сервере ПК. Профиль аутентификации содержит в себе имя учетной записи (логин) и

Поле	Описание/Назначение
	пароль, которые будут использоваться при аутентификации на контролируемом устройстве
Логин	Логин пользователя для аутентификации на устройстве
Пароль	Пароль пользователя для аутентификации на устройстве
Привилегированный пароль	Пароль пользователя для осуществления входа на устройство в привилегированном режиме. Поле отображается во вкладке только при наличии включенном переключателе *Привилегированный режим* (см. выше)
Тестовая команда	Команда для тестирования загрузки конфигурации с устройства. Например, «show version» – отображение текущей версии для устройств типа Cisco IOS. Поле обязательно для заполнения
*Кнопка **Проверить подключение***	По нажатию кнопки выполняется проверка подключения и выполнения заданной команды
Результат проверки	После завершения проверки в поле отображается ее результат: *Успешно* или *Ошибка.* Текст результата является ссылкой, при выборе которой открывается окно с логом выполнения команды (рис. 26)

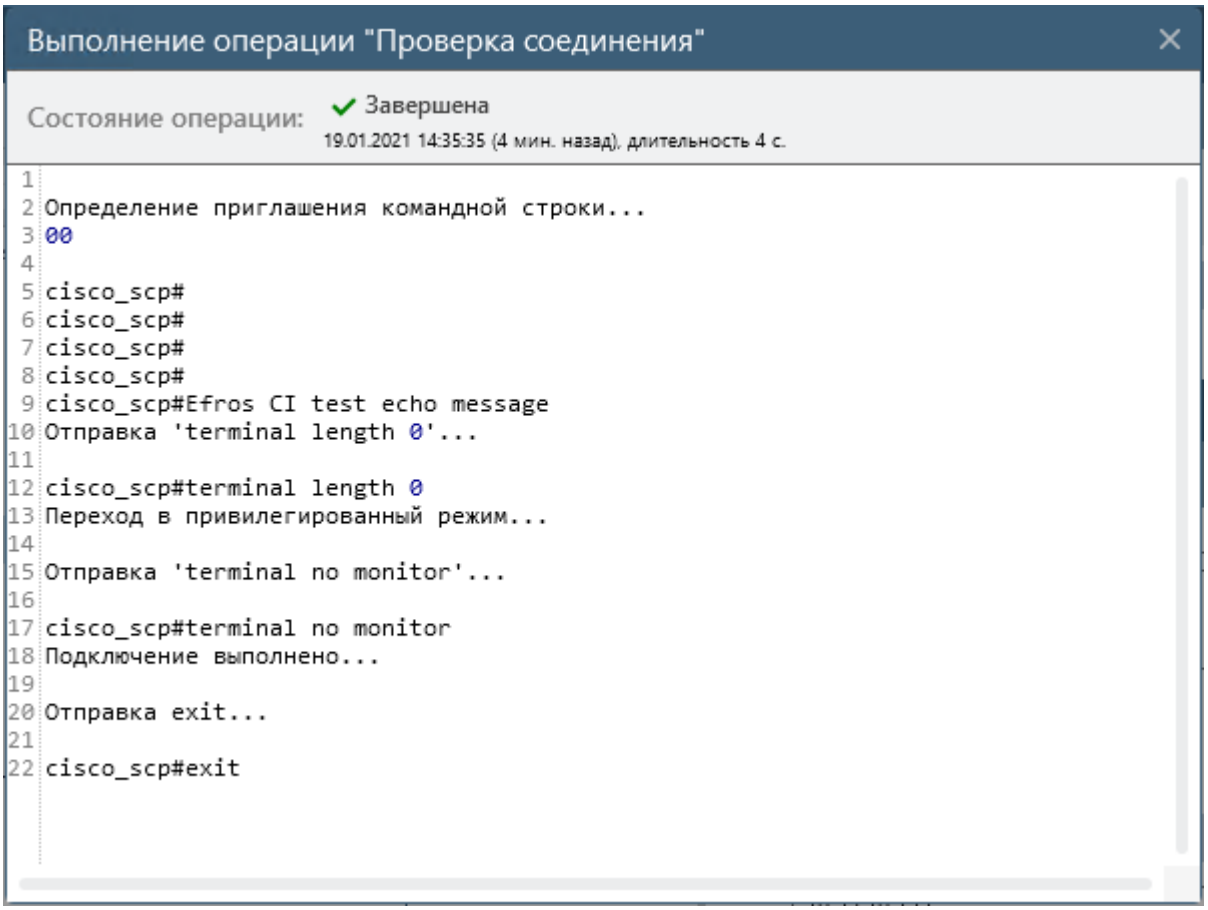


Рисунок 26 – Лог выполнения проверки подключения устройства

2.3.4. Внесение изменений в параметры работы внешнего модуля

Для внесения изменений в параметры работы внешнего модуля – в строке с именем требуемого модуля нажмите кнопку ***Настройки*** (). Откроется окно настройки параметров внешнего модуля. На рис. 27 приведен пример окна для модуля ***Windows***.

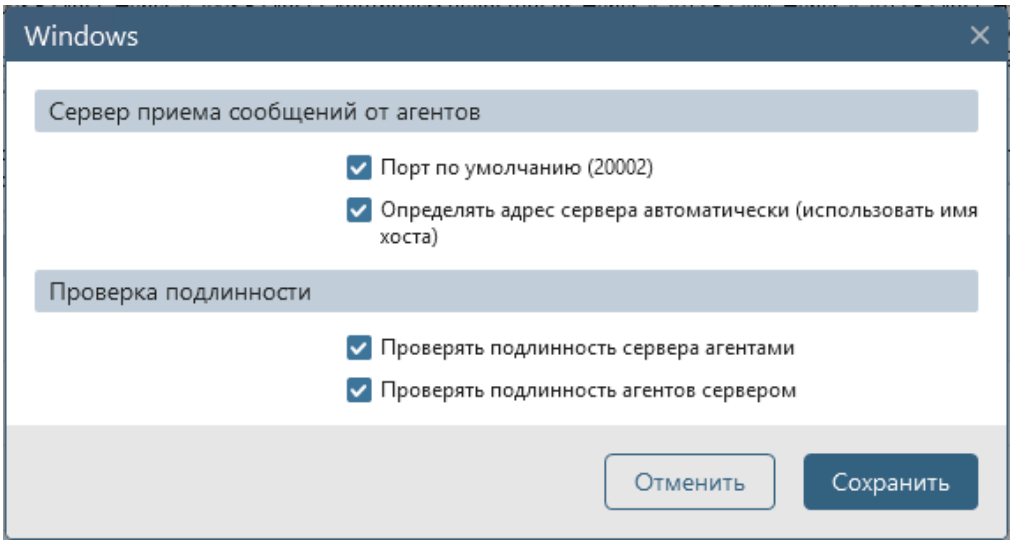


Рисунок 27 – Окно настройки параметров внешнего модуля ***Windows***

Внесите требуемые изменения в параметры работы модуля (подробное описание настраиваемых параметров внешних модулей приведено в файле *Описание модулей.chm*, поставляемом на дистрибутивном диске). Например, для модуля ***Windows*** можно изменить:

- порт подключения сервера приема сообщений от windows-агентов (используется либо значение по умолчанию (20002) или задается вручную после снятия флага в поле);
- адрес, используемый windows-агентами для подключения (определяется либо автоматически (используется имя хоста) или задается вручную после снятия флага в поле);
- настройки режимов проверки подлинности (включена/отключена).

Нажмите кнопку ***Сохранить***. Внесенные изменения будут сохранены.

Для модуля ***Управление устройствами***, чтобы убедиться в правильности внесенных в настройки изменений, – выполнить проверку подключения к OpenSSH серверу, нажав ссылку ***Проверка подключения к серверу***.

2.3.5. Обновление подключенного к комплексу внешнего модуля

Перед обновлением внешнего модуля можно ознакомиться с информацией о внесенных в работу модуля изменениях – для этого нажмите кнопку ***Сведения*** (), расположенную в строке с именем модуля, справа от кнопки ***Обновить*** ().

В результате откроется окно со списком внесенных в работу модуля изменений (рис. 28). Для закрытия информационного окна и возврата в консоль нажмите кнопку ***Закрыть окно*** ().

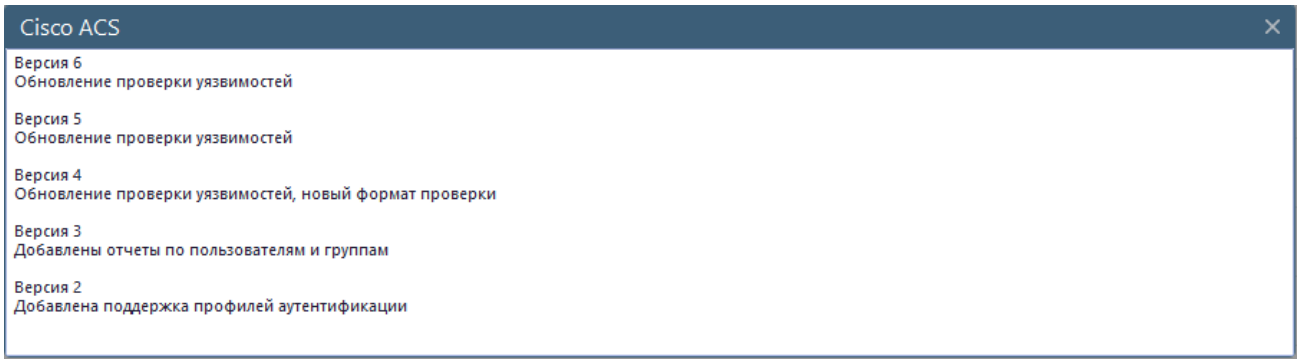


Рисунок 28 – Окно со списком внесенных в работу модуля изменений

Для обновления подключенного к комплексу внешнего модуля в строке с именем требуемого модуля нажмите кнопку ***Обновить*** () (при наличии обновления).

После чего будет выполнена проверка наличия в комплексе пользовательских проверок безопасности, сделанных по шаблону из обновляемого модуля. При обнаружении таких проверок откроется окно с предупреждением о необходимости удаления связанных с шаблоном проверок и списком проверок безопасности (требований), которые необходимо удалить. Пользователь имеет возможность подтвердить удаление проверок и продолжить обновление модуля или отменить обновление модуля.

При отсутствии связанных с шаблонами модуля проверок или после подтверждения обновления с удалением связанных проверок пользователем начнется процесс обновления модуля. После окончания обновления изменится информация о номере версии установленного модуля.

ВНИМАНИЕ: При обновлении модулей, использующих при подключении к устройствам библиотеку libssh, выполняется обновление библиотеки до актуальной версии STABLE с потерей возможности подключения к устройствам по SSH v.1. В процессе обновления такого модуля открывается окно в соответствии с рис. 29. Пользователь должен принять решение об обновлении модуля (с потерей подключения по SSH v.1), нажав кнопку ***Обновить*****,** или отмене обновления (оставить возможность подключения по SSH v.1), нажав кнопку ***Отменить***!.

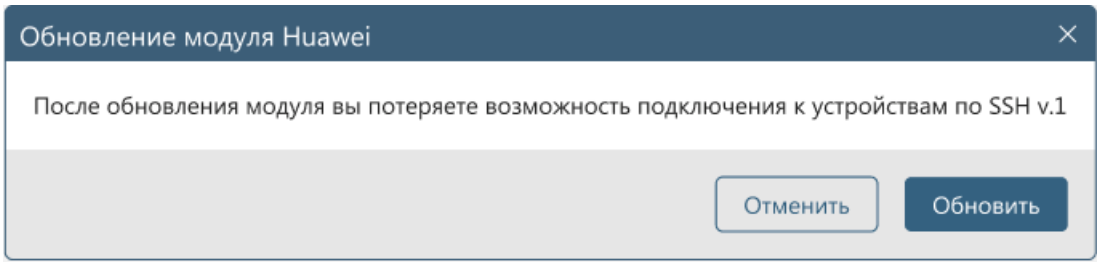


Рисунок 29 – Окно с предупреждением о потере возможности подключения по SSH v.1

Установленный, но не подключенный к комплексу внешний модуль, будет автоматически обновлен при загрузке его новой версии на сервер ПК.

2.3.6. Отключение внешних модулей

Для отключения внешнего модуля выполните щелчок левой кнопкой мыши по переключателю (), расположенному слева от имени требуемого модуля (см. пример на рис. 22). По окончании процесса отключения модуля появится всплывающее сообщение о результате отключения модуля, переключатель слева от наименования модуля окрасится в белый цвет, а в строке отключенного модуля кнопка ***Настройки*** () заменится на кнопку ***Удалить*** ().

При отключении внешнего модуля выполняется проверка на наличие устройств, контролируемых на сервере ПК с использованием модуля, а также наличия пользовательских отчетов и проверок безопасности, сделанных по шаблону из отключаемого модуля. При обнаружении таких устройств, отчетов или проверок безопасности произойдет ошибка отключения модуля. В открывшемся окне **Ошибка отключения модуля** (рис. 30) будет выведен список зависимых от модуля устройств, отчетов и проверок безопасности.

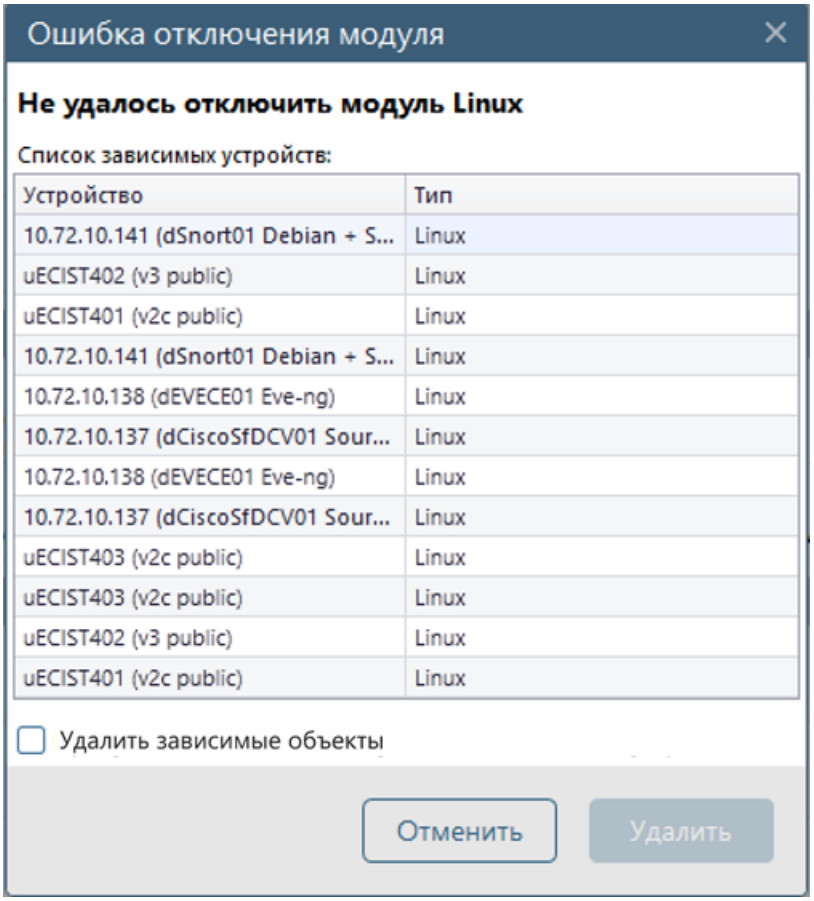


Рисунок 30 – Окно **Ошибка отключения модуля**

Пользователь имеет возможность подтвердить отключение модуля с удалением зависимых устройств, отчетов и проверок безопасности, для чего отметить параметр ***Удалить зависимые объекты*** и нажать кнопку ***Удалить***, либо отменить отключение, нажав кнопку ***Отменить***. После подтверждения отключения модуль будет отключен, а все зависимые от него устройства, отчеты и проверки безопасности удалены из соответствующих списков комплекса.

В клиентской консоли ПК «Efros Config Inspector v.4» реализована возможность группового отключения модулей. Для реализации этой возможности в строке с именем категории модулей нажмите кнопку (⋯) и в открывшемся меню выберите пункт ***Отключить все***. По окончании процесса отключения модулей в форме управления внешними модулями будут появляться сообщения об отключении модулей от комплекса.

Примечание – Если в группе отключаемых модулей имеются модули с зависимыми устройствами, пользовательскими отчетами или проверками безопасности, то такие модули не будут отключены, вместо сообщения об успешном отключении отобразится сообщение *Не удалось отключить модуль <наименование модуля>*.

2.3.7. Удаление внешних модулей

Для удаления внешнего модуля с сервера ПК в строке с именем удаляемого модуля нажмите кнопку ***Удалить*** (🗑). Подтвердите операцию удаления модуля с сервера ПК, нажав кнопку ***Удалить*** в открывшемся окне. В результате выбранный модуль будет удален с сервера ПК.

Удалить с сервера ПК можно только отключенный модуль.

ВНИМАНИЕ: Для удаление не доступны следующие базовые модули: *Отправка Syslog, Отправка писем по протоколу SMTP, Syslog сервер, SNMP Trap сервер, Экспорт событий, Windows*!

2.3.8. Модуль SNMP Trap сервер (особенности)

В ПК «Efros Config Inspector» v.4 реализован SNMP-trap сервер, позволяющий принимать сообщения событий от устройств по протоколу SNMP. Для этого на устройстве необходимо настроить отправку сообщений по SNMP протоколу, и настроить модуль **SNMP Trap сервер** в ПК «Efros Config Inspector» v.4.

Для включения этого модуля в ПК «Efros Config Inspector» v.4 необходимо выполнить следующие действия:

1) В области ***Администрирование*** раздела **Настройки** нажать кнопку ***Модули***.

2) В открывшемся окне включить переключатель в строке модуля **SNMP Trap сервер** (рис. 31). Откроется окно настроек модуля **SNMP Trap сервер** (рис. 32).

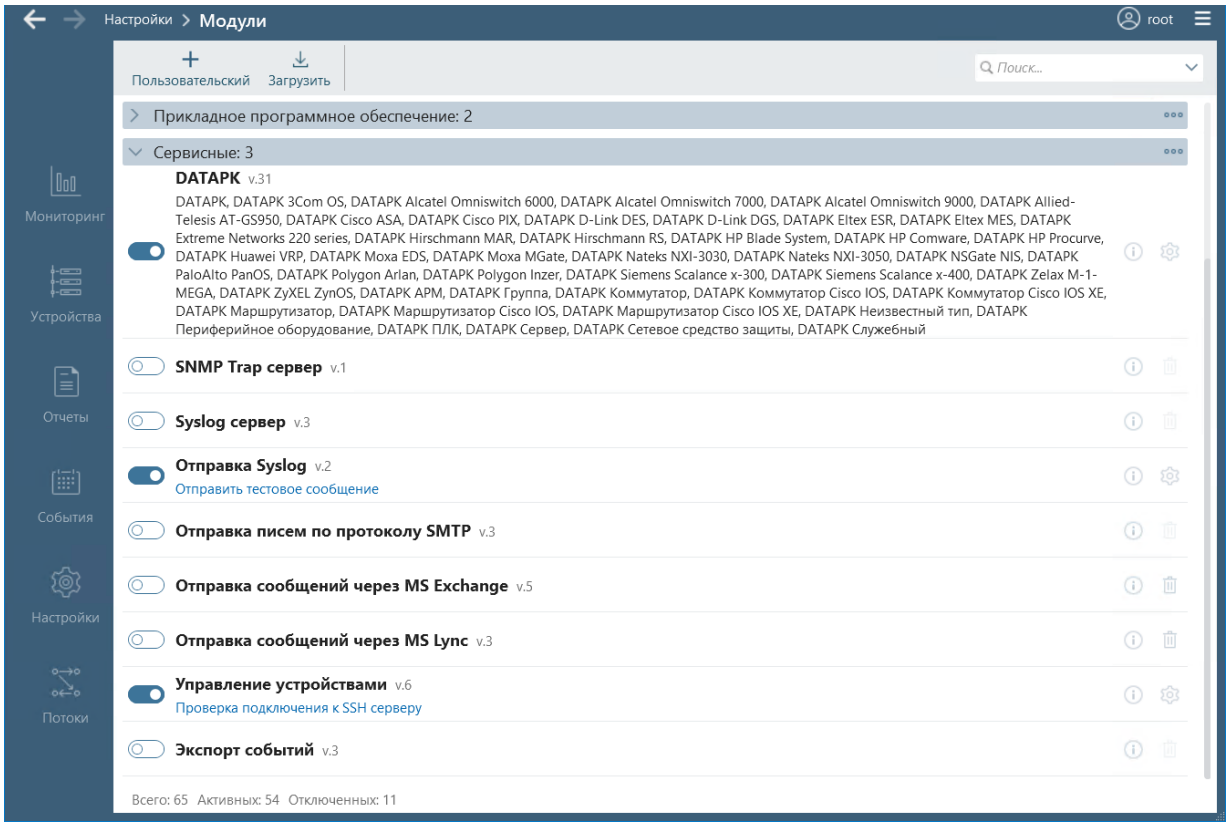


Рисунок 31 – Подключение модуля **SNMP Trap сервер**

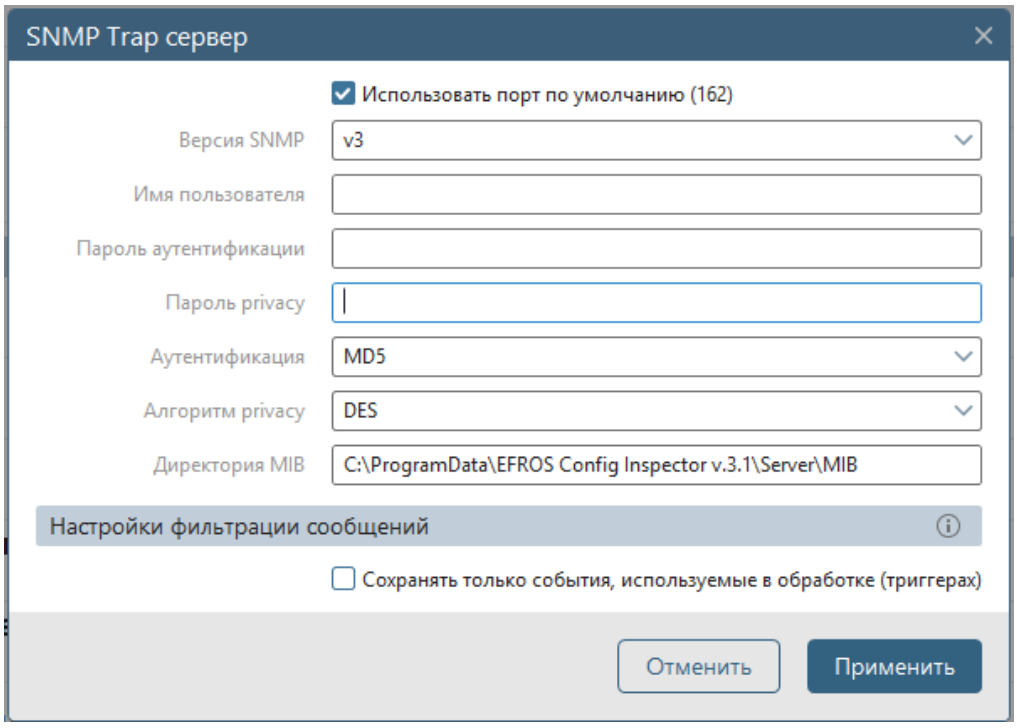


Рисунок 32 – Окно настроек модуля **SNMP Trap сервер**

3) В открывшемся окне настроить следующие параметры, для успешной работы модуля.

- ***Использовать порт по умолчанию (162).*** При включении данного параметра используется порт по умолчанию – 162. Если параметр не включен, то в окне настройки модуля становится доступно поле **Порт**, в котором можно указать порт для связи устройств (рис. 33).

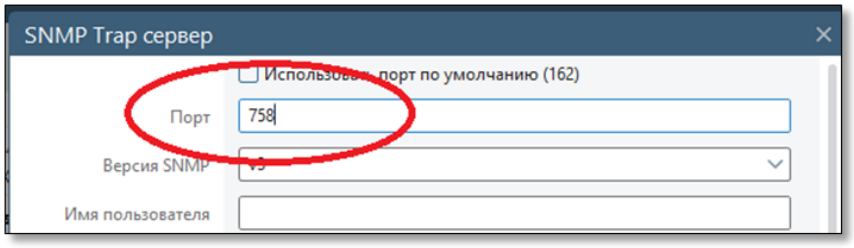
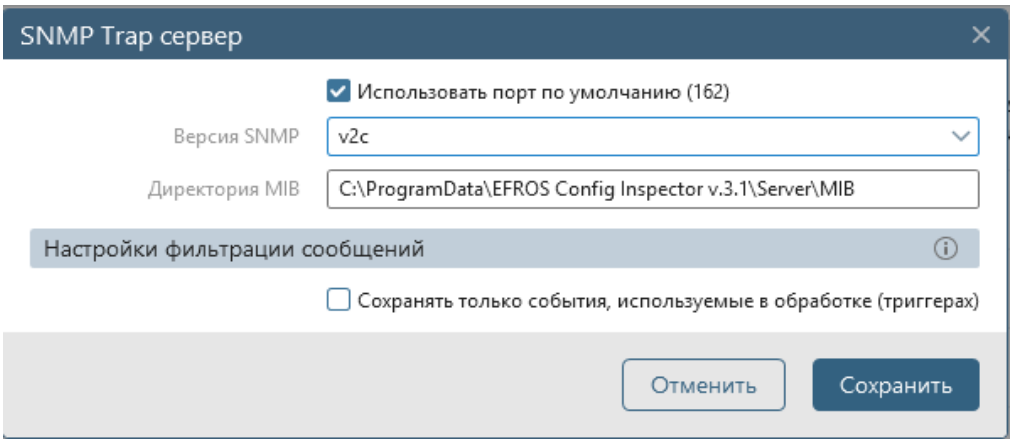


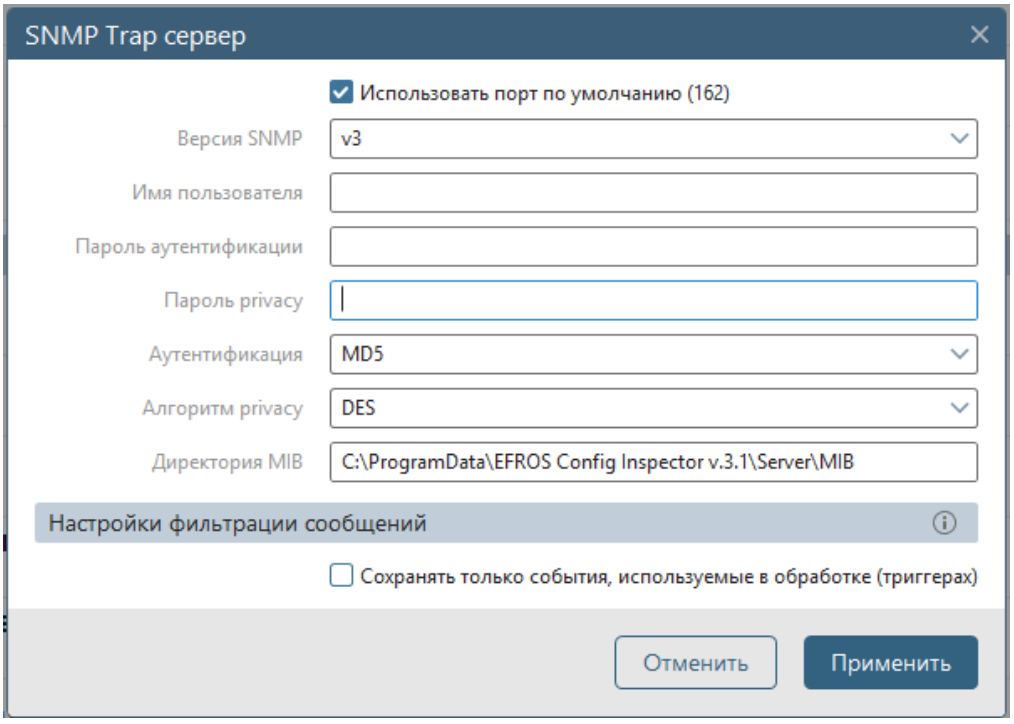
Рисунок 33 – Поле Порт

- ***Версия SNMP*** – выпадающий список, позволяющий выбрать версию протокола SNMP. Доступны два протокола: v2c и v3. (рис. 34 а, б).

Примечание – При выборе протокола SNMP v3, окно настроек модуля дополнительно включает следующие поля: **Имя пользователя, Пароль аутентификации, Пароль privacy, Аутентификация** (доступно: отсутствует, MD5, SHA), **Алгоритм privacy** (доступно: отсутствует, DES, AES-128).



а)



б)

Рисунок 34 – Версия протокола SNMP

– ***Директория MIB*** – директория, в которой находятся MIB[4]-файлы устройств.

Примечание – ПК «Efros Config Inspector» v.4 поддерживает расшифровку стандартных событий MIB для любых устройств. Для расшифровки нестандартных MIB событий устройства, необходимо поместить MIB файл устройства в данный каталог. Существуют стандартные события MIB, установленные различными международными стандартами, которые одинаковы для всех устройств. Также, каждому устройству соответствует свой набор событий MIB, определяемый производителями оборудования, который дополняет стандартные. Перечень стандартных событий MIB приведен в таблице 9.

– Параметр ***Сохранять только события, используемые в обработке (триггерах)*** отвечает за то, чтобы события, для которых не настроена обработка (триггеры), игнорировались и не регистрировались в ПК «Efros Config Inspector» v.4. В противном случае все принятые события от устройств будут отображены в разделе ***События***.

4) Нажать кнопку ***Применить***.

Таблица 9 – Стандартные события MIB

SNMP Trap	Описание	OID	Object
Cold Start (Холодный старт)	Данное сообщение означает, что коммутатор был включен и инициализирован так, что все программные настройки были восстановлены, а аппаратные компоненты были перезагружены. "Холодный" старт отличается от сброса коммутатора к заводским установкам тем, что настройки сохраняются в энергонезависимой памяти, используемой для восстановления конфигурации коммутатора	1.3.6.1.6.3.1.1.5.1	coldStart
Warm Start (Горячий старт)	Данное сообщение означает, что коммутатор был перезагружен (только программно), но тест по самодиагностике при включении питания (Power-On Self-Test - POST) был пропущен	1.3.6.1.6.3.1.1.5.2	warmStart
Authentication Failure (Ошибка аутентификации)	Данное сообщение означает, что кто-то пытается подключиться к коммутатору, используя неверную "строку сообщества" SNMP - Community string. Коммутатор автоматически запоминает IP-адрес неавторизированного пользователя	1.3.6.1.6.3.1.1.5.5	authenticationFailure
Topology Change	Данное сообщение посылается	1.3.6.1.2.1.17.2	topologyChange

[4] MIB - Managment Information Base - база данных информации управления, хранящая информацию обо всех объектах (параметрах и настройках) устройства

SNMP Trap	Описание	OID	Object
(Изменение топологии)	коммутатором, когда любой из его сконфигурированных портов переходит из состояния Learning в Forwarding, или из состояния Forwarding в Blocking. Данный trap не генерируется, если при том же изменении состояния порта был послан new root trap		
Link Change Event (Изменение статуса соединения)	Данное сообщение посылается каждый раз, когда состояние порта меняется с link up на link down или с link down на link up	1.3.6.1.2.1.31.1.1.1.14 1.3.6.1.6.3.1.1.5.3 1.3.6.1.6.3.1.1.5.4	ifLinkUpDownTrapEnable linkDown linkup
Broadcast/Multicast Storm (Широковещательный шторм)	Данное сообщение посылается каждый раз, когда на порту преодолевается пороговое значение пакетов широковещательной/ групповой рассылки. (количество пакетов в секунду), установленное глобально для коммутатора. На каждом порту поддерживаются раздельные счетчики для широковещательных пакетов и для пакетов групповой рассылки. Пороговое значение по умолчанию равно 128 тысяч пакетов/с как для широковещательной рассылки, и так и для групповой рассылки	1.3.6.1.2.1.31.1.1.1.2 1.3.6.1.2.1.31.1.1.1.3 1.3.6.1.2.1.31.1.1.1.4 1.3.6.1.2.1.31.1.1.1.5	ifOutBroadcastPkts ifOutMulticastPkts ifInBroadcastPkts ifInMulticastPkts

В результате выполнения всех необходимых настроек, ПК «Efros Config Inspector» v.4 будет регистрировать события устройств по протоколу SNMP (рис. 35).

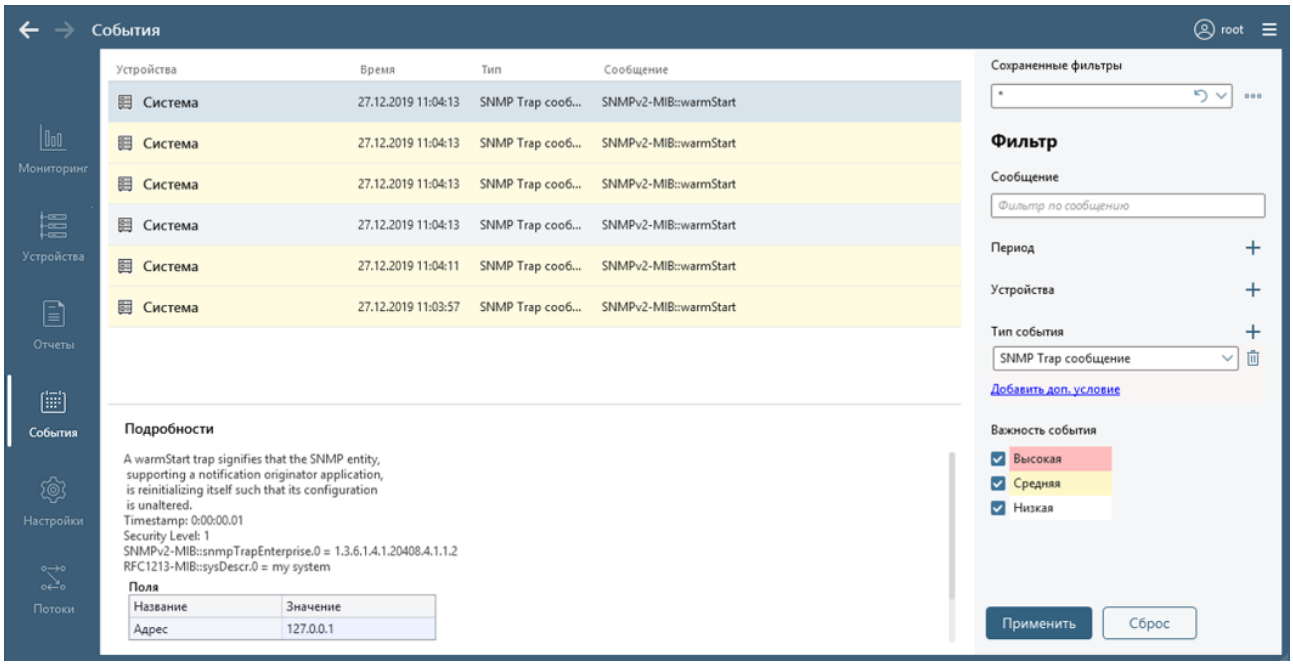


Рисунок 35 – Регистрация событий устройств по протоколу SNMP

2.4. Управление пользователями комплекса и их правами

Управление пользователями комплекса и настройка их прав выполняется во вкладке **Пользователи** (форма управления пользователями и их правами), приведенной на рис. 36 (описание элементов управления и полей приведено в таблице 10). Вкладка открывается при переходе из раздела **Настройки** по ссылке ***Пользователи и группы***.

Для работы с ПК «Efros Config Inspector» v.4 существует два типа учетных записей пользователей комплекса: учетные записи, создаваемые и существующие только в списке пользователей комплекса (далее – локальные пользователи комплекса), и добавляемые в список пользователей комплекса учетные записи пользователей домена (далее – доменные пользователи комплекса).

Пользователи могут быть объединены в группы на основе ролей пользователей (доступа к настройкам контроля и администрированию комплекса) и прав доступа к корневой группе устройств. Группы также могут быть двух типов – локальные и доменные.

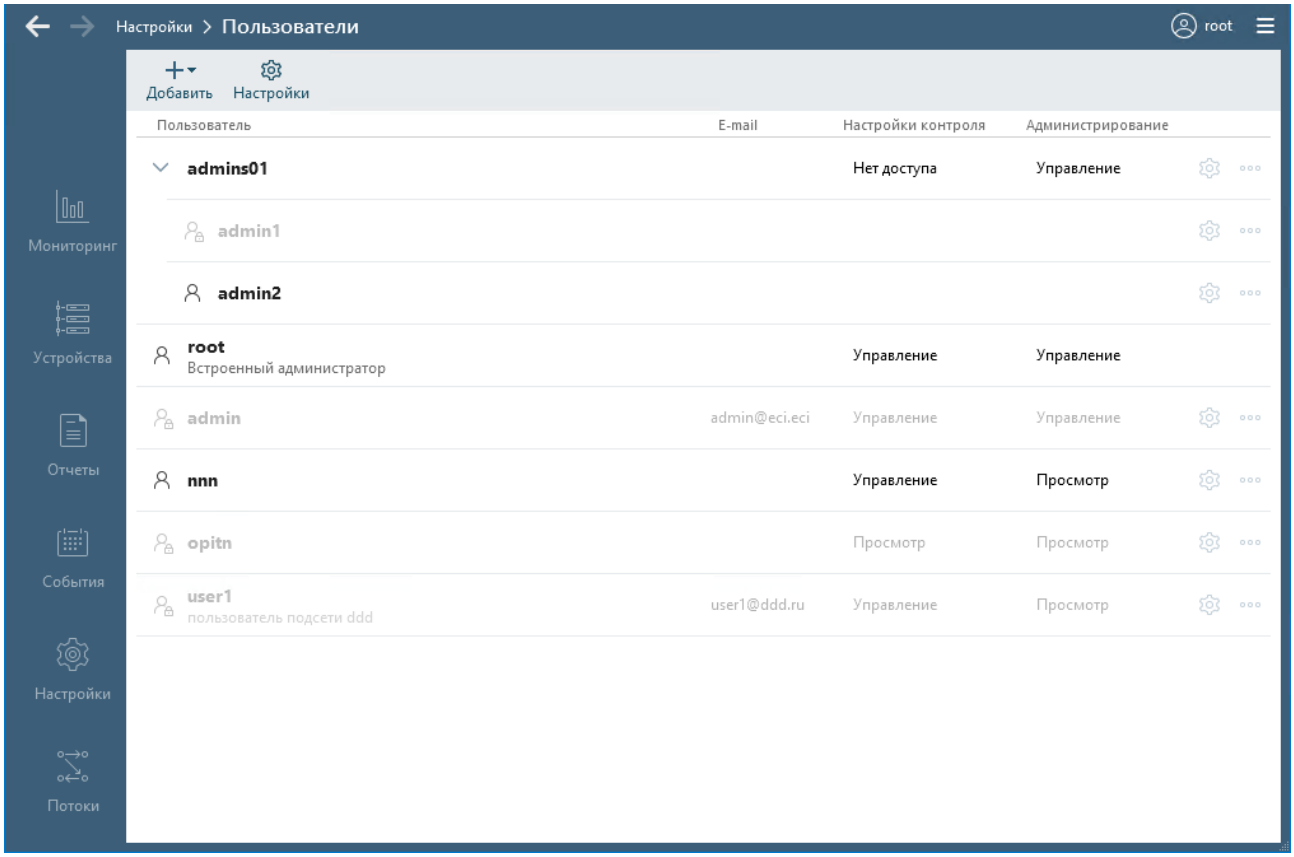


Рисунок 36 – Форма управления пользователями и их правами

Таблица 10 – Форма управления пользователями и их правами

Элемент	Назначение
Меню вкладки ***Пользователи***	
Кнопка ***Добавить***	Открытие окна добавления пользователя/группы пользователей. При нажатии на кнопку открывается дополнительное меню для выбора типа добавляемой учетной записи:

Элемент	Назначение
	– *Пользователь* – локальный пользователь; – *Группа* – локальная группа; – *Доменный пользователь* – доменный пользователь; – *Доменная группа* – доменная группа
Кнопка ***Настройки***	При нажатии кнопки открывается окно **Настройки пользователей,** в котором производится настройка параметров идентификации и аутентификации пользователей (подробнее см. п. 2.4.9 «Настройка параметров безопасности учетных записей пользователей »)
Рабочая область вкладки ***Пользователи***	
Список пользователей	Для каждого пользователя отображаются: логин, описание. Для каждой группы отображаются название, описание
E-mail	Отображается адрес электронной почты, если он указан в настройках пользователя
Настройки контроля	Возможные значения: *Нет доступа; Просмотр; Управление*
Администрирование	Возможные значения: *Нет доступа; Просмотр; Управление*
Кнопка ***Настройка***	Для перехода в окно редактирования параметров выбранного пользователя/группы. Открывается окно**,** в котором администратор: – для пользователя может изменить имя пользователя, указать адрес электронной почты, добавить описание (при необходимости), указать группу, в которую будет включен пользователь. Также возможно изменить доступ к настройкам контроля и администрирования для выбранного пользователя; – для группы может изменить название, описание, доступ к настройкам контроля и администрирования для пользователей группы. Примечание – Если пользователь или доменная группа включены в локальную группу, то для них изменение настроек контроля и администрирования не доступно
Кнопка ***Меню***	Раскрывает контекстное меню. Панель меню содержит пункты: 1. Для пользователя: – *Сменить пароль* – для перехода в форму смены пароля соответствующего пользователя (пункт отсутствует у доменных пользователей); – *Заблокировать/Разблокировать* – блокировка/разблокировка учетной записи соответствующего пользователя; – *Права на устройствах* – для перехода в окно настройки доступа пользователя к устройствам, подключенным к комплексу; – *Удалить* – для удаления выбранного пользователя (после подтверждения действия). 2. Для группы: – *Права на устройствах* – для перехода в окно настройки доступа группы пользователей к устройствам, подключенным к

Элемент	Назначение
	комплексу; – *Удалить* – для удаления выбранной группы (после подтверждения действия)

Примечания:

1) Пользователь может быть включен только в одну локальную группу, при этом привилегии и права доступа пользователя к устройствам определяются привилегиями и правами соответствующей группы.

2) При нахождении пользователя в нескольких доменных группах, пользователь будет обладать правами всех доменных групп, в которые он включен. Если пользователь добавлен в список пользователей ПК «Efros Config Inspector» v.4 отдельно (без группы) с индивидуальными привилегиями и правами, то привилегии и права пользователя и группы будут также суммироваться.

ВНИМАНИЕ: Добавление доменных пользователей и групп может быть выполнено только при соблюдении следующих условий:

- сервер ПК введен в домен AD;
- администратор, выполняющий добавление пользователя/группы, является доменным пользователем (консоль сервера ПК запущена под доменной учетной записью)!

Строки с учетными записями блокированных пользователей отображаются затененными (цвет текста данных пользователя – светло-серый).

Для просмотра информации об активных в текущий момент времени пользователях необходимо под ссылкой ***Пользователи и группы*** в разделе **Настройки** выбрать ссылку ***Активные пользователи.*** При выборе этой ссылки открывается форма ***Активные пользователи*** (рис. 37), на которой отображаются информация об активных пользователях (имя пользователя, права доступа, IP-адрес, время работы пользователя на сервере). На вкладке предоставляется возможность изменения настроек пользователя (доступ к настройкам пользователя – по кнопке ***Изменить*** ( ), отключение пользователя – по кнопке ***Отключить*** ( )).

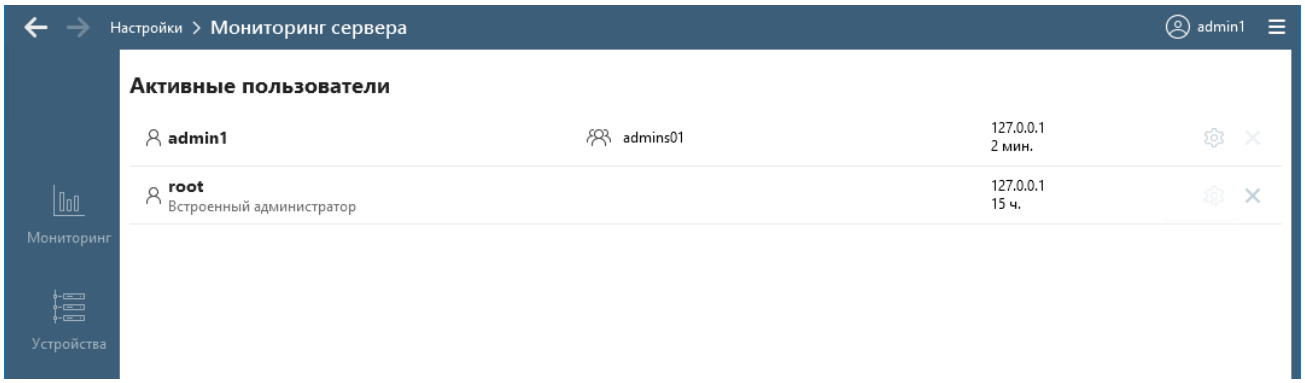


Рисунок 37 – Вкладка ***Активные пользователи***

2.4.1. Ведение списка групп пользователей

2.4.1.1. Добавление локальной группы пользователей

Для добавления новой локальной группы необходимо выполнить следующие действия:

1) Нажать в форме управления пользователями системы и их правами кнопку ***Добавить*** (+) (см. рис. 36). В раскрывшемся списке выбрать значение ***Группа.*** Откроется окне добавления новой локальной группы (рис. 38, таблица 11).

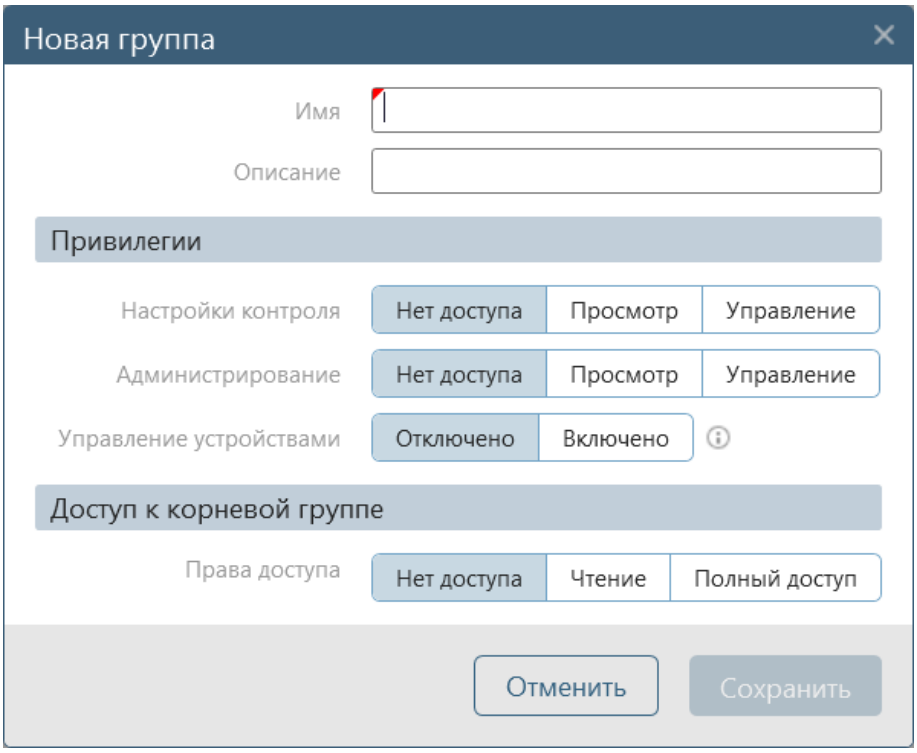


Рисунок 38 – Окно ***Новая группа***

Таблица 11 – Состав и описание полей окна добавления локальной группы

Поле	Описание/Назначение
Имя	Название группы
Описание	Текстовое поле, в которое можно ввести понятное описание группы
Блок *Привилегии*	
Настройки контроля и Администрирование	Выбор доступа к настройкам контроля и администрирования комплекса для пользователей группы (в соответствии с п. 1.3 «Пользователи ПК «Efros Config Inspector» v.4»)
Управление устройствами	Включение/отключение доступности пользователям группы функций управления устройствами. Поле *Управление устройствами* отображается в окне только в том случае, если в состав ПК «Efros Config Inspector» v.4 входит модуль ***Управление устройствами*** и он включен. ВНИМАНИЕ: Привилегия на управление выдается всем пользователям группы и действует только на устройствах с полным доступом!

Поле	Описание/Назначение
Блок *Доступ к корневой группе*	
Права доступа	Назначение пользователям группы прав доступа к корневой группе устройств. Возможные значения: – *Нет доступа* – полностью не доступны все функции по работе с устройствами; – *Чтение* – просмотр, загрузка отчетов; – *Полный доступ* – чтение, запись и выполнение операций, которые не требуют прав *Управление устройствами*

2) Ввести параметры группы:

- в поле ***Имя*** ввести наименование новой группы;
- при необходимости, ввести описание создаваемой группы комплекса в соответствующее поле;
- указать доступ к настройкам контроля и администрирования комплекса для пользователей добавляемой группы, выбрав необходимое значение в полях соответственно *Настройки контроля* и *Администрирование* блока ***Привилегии***;
- включить или отключить доступ к функциям управления устройствами, выбрав необходимое значение в поле *Управление устройствами* блока ***Привилегии***;
- определить права доступа пользователей добавляемой группы к корневой группе, выбрав необходимый параметр в одноименной области (описание возможных значений приведено в таблице 11).

Примечание – При назначении прав доступа группы пользователей к настройкам контроля и администрирования комплекса, а также к корневой группе необходимо учитывать, что при выборе:

- в блоке ***Привилегии*** в поле *Настройки контроля* значения *Просмотр* или *Управление* автоматически в блоке ***Доступ к корневой группе*** в поле *Права доступа* будет установлено значение *Чтение*;
- в блоке ***Привилегии*** в поле *Администрирование* значения *Просмотр* автоматически в блоке ***Доступ к корневой группе*** в поле *Права доступа* будет установлено значение *Чтение*;
- в блоке ***Привилегии*** в поле *Администрирование* значения *Управление* автоматически в блоке ***Доступ к корневой группе*** в поле *Права доступа* будет установлено значение *Полный доступ*;
- в блоке ***Доступ к корневой группе*** в поле *Права доступа* значения *Нет доступа* автоматически в блоке ***Привилегии*** в полях *Настройки контроля* и *Администрирование* будет установлено значение *Нет доступа*.

3) Нажать кнопку ***Сохранить***. Произойдет возврат в форму управления пользователями программного комплекса, в которой отобразится строка с данными добавленной группы.

Для доступа к вложенным устройствам у пользователей группы всегда должен быть доступ на чтение к устройству верхнего уровня. Таким образом, для доступа к устройствам группа пользователей обязательно должна иметь доступ на чтение к корневой группе устройств. В дальнейшем администратор имеет возможность настроить права доступа пользователей группы к устройствам в соответствии с п. 2.4.3 «Настройка прав доступа пользователей/групп пользователей к устройствам».

2.4.1.2. Добавление доменной группы пользователей

Для добавления доменной группы необходимо выполнить следующие действия:

1) Нажать в форме управления пользователями системы и их правами кнопку ***Добавить*** (+). В раскрывшемся меню выбрать пункт ***Доменная группа***.

Примечание – Если сервер ПК не введен в домен AD, то откроется окно с сообщением об ошибке.

2) Выбрать необходимую группу пользователей в открывшемся стандартном окне используемой ОС **Выбор: Группа** (рис. 39). Откроется окно добавления нового пользователя (рис. 40), в котором поля ***Логин*** и ***Описание*** будут автоматически заполнены данными выбранной на контроллере домена группы.

Примечание – Доменная группа добавляется в список пользователей ПК «Efros Config Inspector» v.4 в качестве пользователя, и, в отличие от локальных групп, может быть заблокирована/разблокирована (см. п. 2.4.7) и добавлена в локальную группу пользователей. При этом в доменную группу нельзя добавить пользователей и другие группы пользователей средствами ПК «Efros Config Inspector» v.4.

3) Заблокировать, при необходимости, группу, для чего перевести переключатель ***Активность*** в положение *Отключен* ( ).

4) Выбрать в поле ***Группа***, при необходимости, локальную группу пользователей в которую должна входить доменная группа.

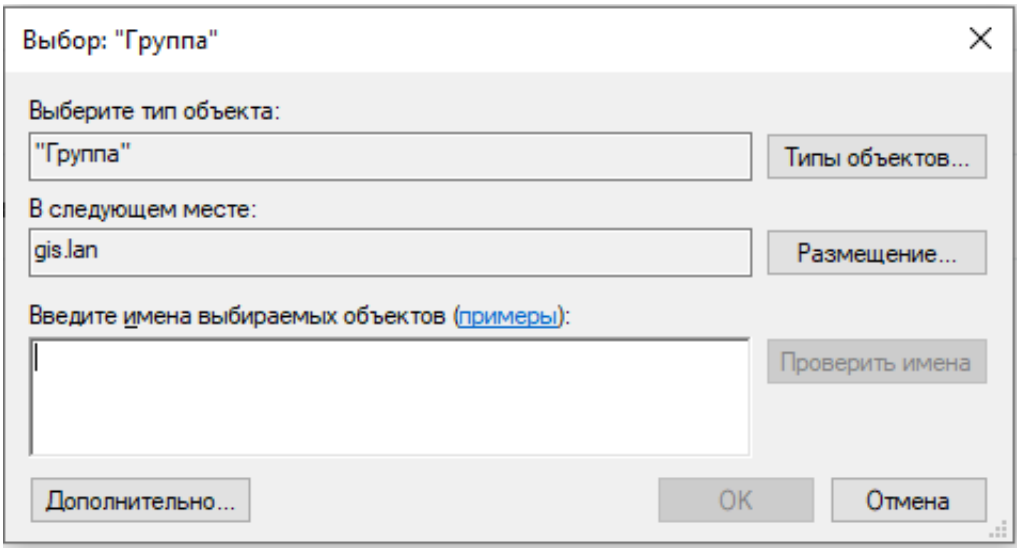


Рисунок 39 – Окно выбора группы пользователей домена

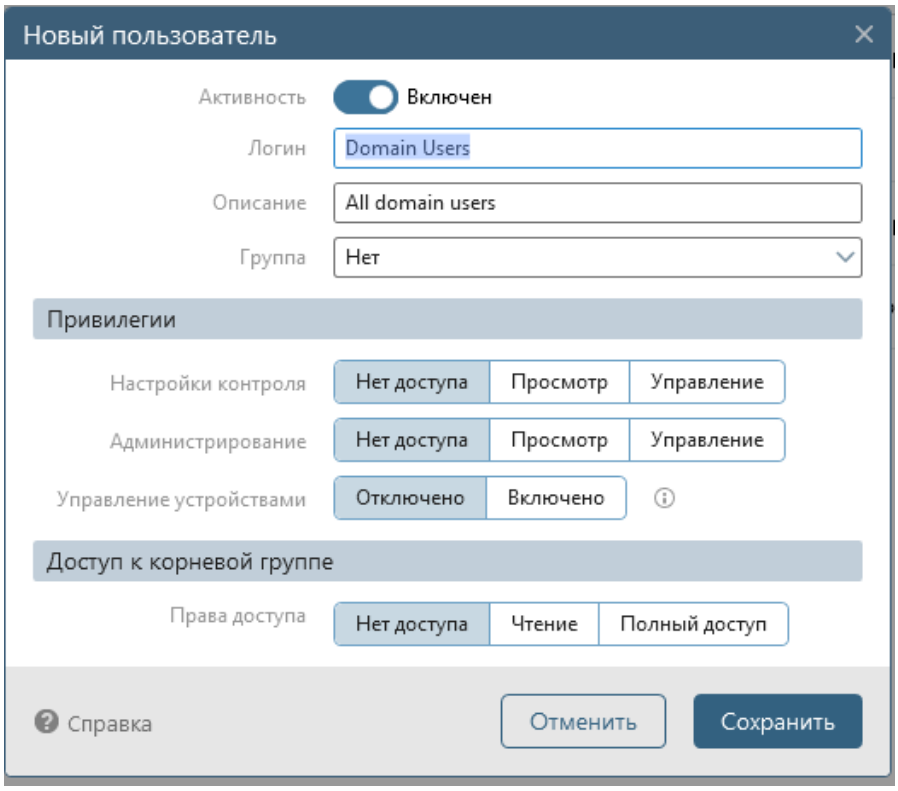


Рисунок 40 – Окно добавления нового пользователя с параметрами доменной группы

ВНИМАНИЕ: При добавлении в локальную группу пользователям доменной группы автоматически назначаются привилегии выбранной локальной группы и при редактировании учетной записи доменной группы в дальнейшем привилегии не доступны для внесения изменений!

5) Если поле ***Группа*** оставлено незаполненным – указать права доступа к настройкам и администрированию, назначить права доступа к корневой группе (описание полей приведено в таблице 11).

6) Нажать кнопку ***Сохранить***. Произойдет возврат в форму управления пользователями программного комплекса, в которой отобразится строка с данными добавленной группы.

Примечание – Если администратор не является доменным пользователем, то откроется окно с сообщением об ошибке.

Администратор имеет возможность настроить права доступа группы пользователей к устройствам в соответствии с п. 2.4.4 «Настройка прав доступа пользователей/групп пользователей к устройствам».

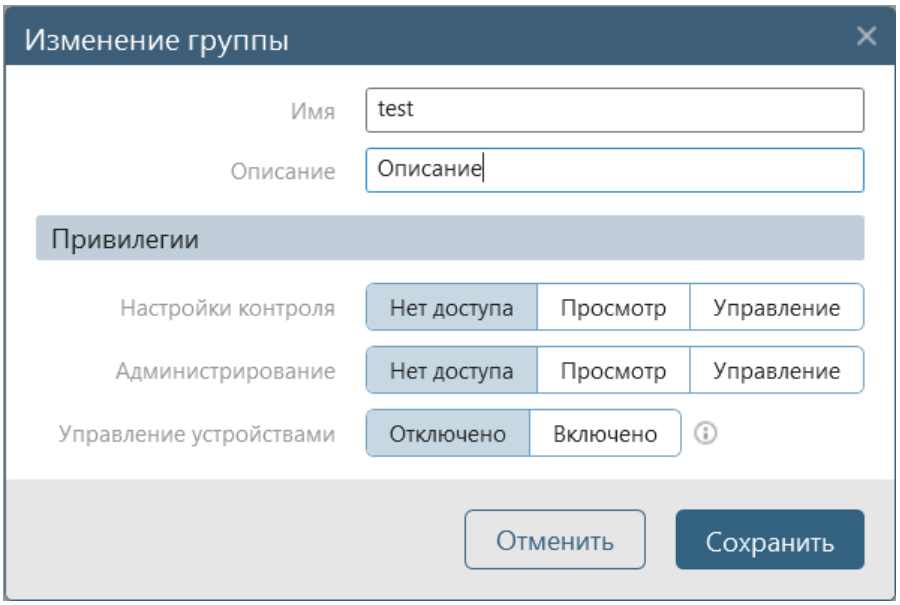
2.4.1.3. Изменение параметров групп пользователей

Для изменения параметров локальной или доменной группы пользователей комплекса необходимо выполнить следующие действия:

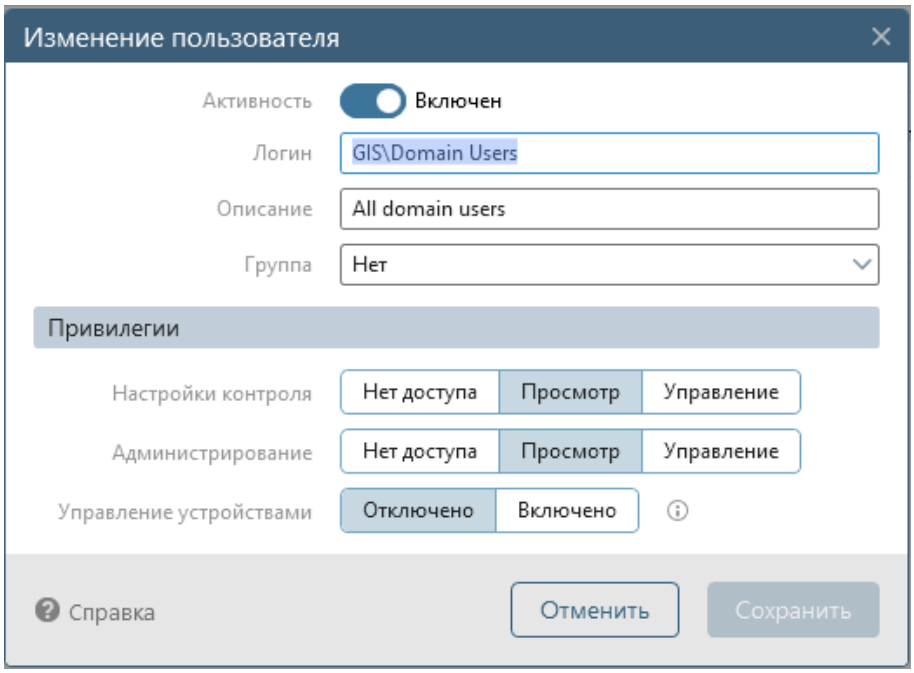
1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.

2) В области *Администрирование* нажать ссылку ***Пользователи и группы.*** Откроется форма управления пользователями системы и их правами.

3) Нажать в строке требуемой группы кнопку ***Изменить*** (⚙). Откроется окно изменения данных группы (рис. 41, а – для локальной группы, б – для доменной группы).



а) для локальной группы пользователей



б) для доменной группы пользователей

Рисунок 41 – Окно изменения параметров

4) Изменить требуемые параметры группы (имя, описание, группу (только для доменной группы), доступ к настройкам контроля и администрированию комплекса, доступ к функциям управления устройствами).

Примечание – Для доменной группы пользователей не доступны для внесения изменений логин и описание, а также, если доменная группа включена в другую группу пользователей – привилегии.

5) Для доменной группы – блокировать/разблокировать группу, при необходимости, выбрав требуемое положение переключателя ***Активность***.

6) Нажать кнопку ***Сохранить***. Произойдет возврат в форму управления пользователями программного комплекса, внесенные изменения будут сохранены.

Изменение прав доступа пользователей группы к устройствам, подключенным к комплексу, выполняется в соответствии с п. 2.4.4 «Настройка прав доступа пользователей/групп пользователей к устройствам» и при добавлении и изменении устройств (подробнее см. раздел «Формирование списка контролируемых устройств» документа «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»).

2.4.1.4. Удаление групп пользователей

Для удаления учетной записи группы пользователей необходимо выполнить следующие действия:

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

2) В области *Администрирование* нажать ссылку ***Пользователи и группы***. Откроется форма управления пользователями системы и их правами.

3) Нажать кнопку ***Меню*** (▫▫▫) в строке требуемой группы.

4) Выбрать в раскрывшемся меню пункт ***Удалить***. Откроется окно подтверждения удаления группы (рис. 42).

5) Нажать кнопку ***Удалить***.

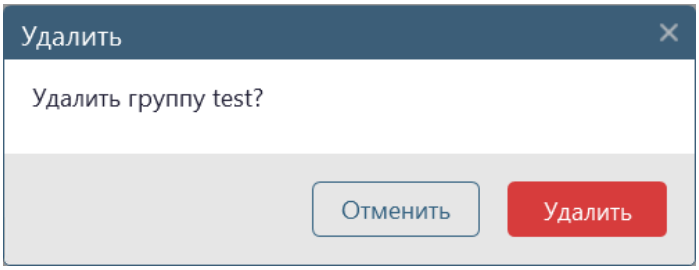


Рисунок 42 – Окно подтверждения удаления группы пользователей

Группа будет удалена из списка пользователей комплекса и списков пользователей, имеющих доступ к устройствам.

Пользователи, включенные в локальную группу, не удаляются – отображаются в списке на первом уровне группировки списка.

Удаление доменной группы из списка пользователей комплекса не влечет за собой удаление этой группы с контроллера домена. Пользователи доменной группы, если их учетная запись не добавлена в список пользователей отдельно, теряют возможность доступа к ПК «Efros Config Inspector» v.4.

2.4.2. Создание локального пользователя комплекса

Для создания локальной учетной записи пользователя комплекса необходимо выполнить следующие действия:

1) Нажать в форме управления пользователями системы и их правами кнопку ***Добавить*** () (см. рис. 36). В раскрывшемся списке выбрать значение ***Пользователь.*** Откроется окно добавления нового пользователя (рис. 43, таблица 12).

2) Заблокировать, при необходимости, учетную запись пользователя, для чего перевести переключатель ***Активность*** в положение *Отключен* ().

3) Ввести параметры пользователя:

- в поле ***Логин*** ввести имя нового пользователя;
- ввести пароль нового пользователя комплекса и его подтверждение в соответствующие поля (при вводе пароля необходимо учитывать требования к его сложности – подробнее см. п. 2.4.9 «Настройка параметров безопасности учетных записей пользователей комплекса»);
- в поле ***E-mail*** ввести адрес электронной почты нового пользователя комплекса, на который будут отправляться уведомления;
- при необходимости, ввести описание создаваемого пользователя комплекса в соответствующее поле;
- в выпадающем списке поля ***Группа,*** при необходимости, выбрать группу для включения в нее добавляемого пользователя;
- указать доступ к настройкам контроля и администрирования комплекса для добавляемого пользователя, отметив необходимое значение в полях соответственно *Настройки контроля* и *Администрирование* блока ***Привилегии*** (см. п. 1.3 «Пользователи ПК «Efros Config Inspector» v.4»);
- включить или отключить доступ к функциям управления устройствами, отметив необходимое значение в поле *Управление устройствами* блока ***Привилегии;***
- определить права доступа добавляемого пользователя к корневой группе, отметив необходимые параметры в одноименной области (описание возможных значений приведено в таблице 12).

Примечание – При назначении прав доступа пользователей к настройкам контроля и администрирования комплекса, а также к корневой группе необходимо учитывать, что при выборе:

- в блоке ***Привилегии*** в поле *Настройки контроля* значения *Просмотр* или *Управление* автоматически в блоке ***Доступ к корневой группе*** в поле *Права доступа* будет установлено значение *Чтение*;
- в блоке ***Привилегии*** в поле *Администрирование* значения *Просмотр* автоматически в блоке ***Доступ к корневой группе*** в поле *Права доступа* будет установлено значение *Чтение*;
- в блоке ***Привилегии*** в поле *Администрирование* значения *Управление* автоматически в блоке ***Доступ к корневой группе*** в поле *Права доступа* будет установлено значение *Полный доступ*;
- в блоке ***Доступ к корневой группе*** в поле *Права доступа* значения *Нет доступа* автоматически в блоке ***Привилегии*** в полях *Настройки*

контроля и *Администрирование* будет установлено значение *Нет доступа*.

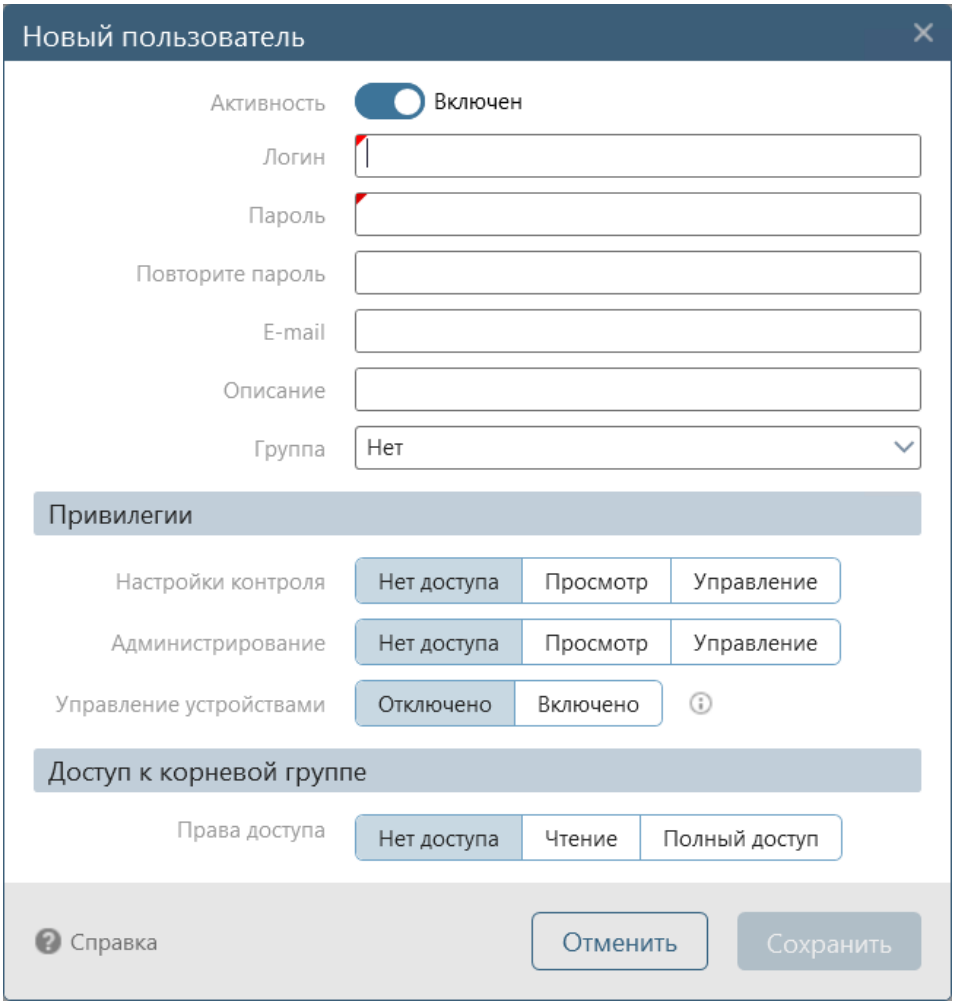


Рисунок 43 – Окно добавления пользователя

Таблица 12 – Состав и описание полей окна добавления пользователя

Поле	Описание/Назначение
Активность	Переключатель с двумя положениями: – *Включен* () – учетная запись пользователя разблокирована; – *Отключен* () – учетная запись пользователя заблокирована
Логин	Имя нового пользователя (или учетная запись доменного пользователя)
Пароль	Пароль нового пользователя (поле недоступно для ввода при добавлении доменного пользователя)
Повторите пароль	Подтверждение пароля пользователя (поле недоступно для ввода при добавлении доменного пользователя)
E-mail	Адрес электронной почты пользователя, на который будут отправляться уведомления (необходимость отправки уведомлений указывается при настройке триггеров)
Описание	Текстовое поле, в которое можно ввести понятное описание учетной записи пользователя

Поле	Описание/Назначение
Группа	Выпадающий список зарегистрированных групп пользователей, для добавления в них нового пользователя. В случае, если пользователь не включен в зарегистрированные группы, указать *Нет*
Блок *Привилегии*	
Настройки контроля и Администрирование	Выбор доступа к настройкам контроля и администрирования комплекса в соответствии с правами пользователя комплекса (см. п. 1.3 «Пользователи ПК «Efros Config Inspector» v.4»)
Управление устройствами	Включение/отключение доступности учетной записи пользователя функций управления устройствами. Поле *Управление устройствами* отображается в окне только в том случае, если в состав ПК «Efros Config Inspector» v.4 входит модуль ***Управление устройствами*** и он включен***.*** ВНИМАНИЕ: Привилегия на управление выдается конкретному пользователю, и действует только на устройствах с полным доступом!
Блок *Доступ к корневой группе*	
Права доступа	Назначение учетной записи пользователя прав доступа к корневой группе устройств. Возможные значения: – *Нет доступа* – пользователю полностью недоступны все функции по работе с устройствами*;* – *Чтение* – просмотр, загрузка отчетов; – *Полный доступ* – чтение, запись и выполнение операций, которые не требуют прав Управление устройствами

4) Нажать кнопку ***Сохранить***. Произойдет возврат в форму управления пользователями программного комплекса, в которой отобразится строка с данными добавленного пользователя.

Для доступа к вложенным устройствам у пользователя комплекса всегда должен быть доступ на чтение к устройству верхнего уровня. Таким образом, для доступа к устройствам пользователи обязательно должны иметь доступ на чтение к корневой группе. В дальнейшем администратор имеет возможность настроить права доступа пользователя к устройствам в соответствии с п. 2.4.4 «Настройка прав доступа пользователей/групп пользователей к устройствам».

2.4.3. Добавление доменного пользователя комплекса

ВНИМАНИЕ: Добавление доменных пользователей может быть выполнено только при соблюдении следующих условий:

- сервер ПК введен в домен AD;
- администратор, выполняющий добавление пользователя, является доменным пользователем (консоль сервера ПК запущена под доменной учетной записью)!

Для добавления учетной записи пользователя домена в список пользователей комплекса выполните следующие действия:

1) Нажать в форме управления пользователями системы и их правами кнопку ***Добавить*** (+). В раскрывшемся меню выбрать пункт ***Доменный пользователь***.

Примечание – Если сервер ПК не введен в домен AD, то откроется окно с сообщением об ошибке.

2) Выбрать необходимую учетную запись в открывшемся стандартном окне используемой ОС **Выбор: Пользователь** (рис. 44). Откроется окно **Новый пользователь**, в котором поля ***E-mail*** и ***Описание*** будут автоматически заполнены данными выбранной на контроллере домена учетной записи.

Примечание – В некоторых ОС (например, в ОС Windows Server 2016), после выполнения шага 1 откроется окно с предложением ввести имя пользователя и найти его. А далее при нажатии кнопки ***Дополнительно*** откроется окно в соответствии с рисунком 42.

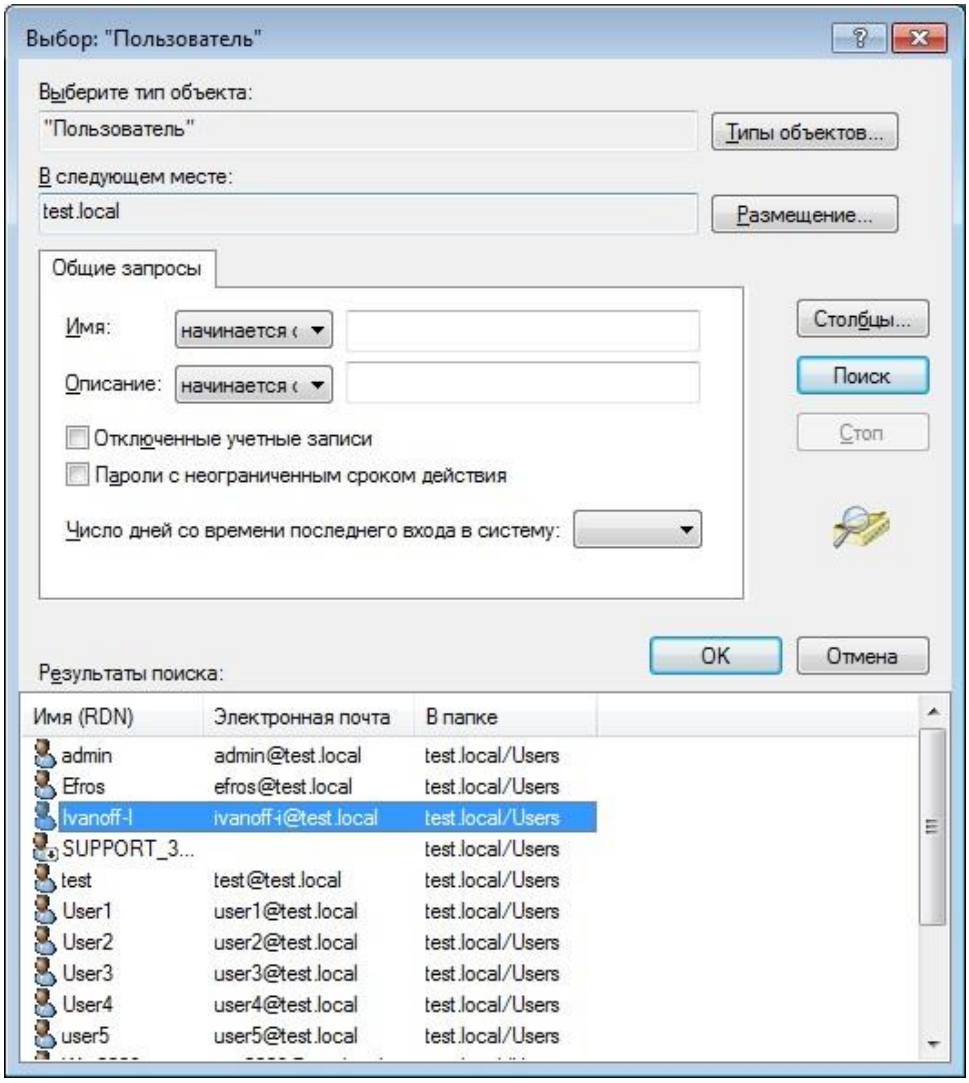


Рисунок 44 – Окно выбора учетной записи пользователя домена

3) Заполнить остальные поля окна добавления нового пользователя, указать его права доступа к настройкам и администрированию, назначить права доступа к корневой группе (описание полей приведено в таблице 12).

ВНИМАНИЕ: Если доменный пользователь добавлен в список пользователей ПК «Efros Config Inspector» v.4 и доменная группа, в которую он включен, также есть в списке, то пользователь будет иметь привилегии, назначенные как ему лично, так и группе пользователей (привилегии суммируются)!

4) Нажать кнопку ***Сохранить***. Произойдет возврат в форму управления пользователями программного комплекса, в которой отобразится строка с данными добавленного пользователя.

Примечание – Если администратор не является доменным пользователем, то откроется окно с сообщением об ошибке.

Администратор имеет возможность настроить права доступа пользователя к устройствам в соответствии с п. 2.4.4 «Настройка прав доступа пользователей/групп пользователей к устройствам».

2.4.4. Настройка прав доступа пользователей/групп пользователей к устройствам

Для настройки прав доступа пользователей к устройствам (нет доступа, чтение, полный доступ) администратору необходимо выполнить следующие действия:

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

2) В области *Администрирование* нажать ссылку ***Пользователи и группы***. Откроется форма управления пользователями системы и их правами.

3) Нажать кнопку ***Меню*** ( ) в строке требуемой группы пользователей/ пользователя.

4) Выбрать в раскрывшемся меню пункт ***Права на устройствах***. Откроется окно настройки прав доступа группы пользователей/пользователя к устройствам (рис. 45). В заголовке окна расположены поле поиска устройств и переключатели:

- ***Скрыть без доступа*** – для выбора режима отображения в списке окна устройств, к которым у пользователя отсутствует доступ;
- ***Скрыть наследуемые*** – для выбора режима отображения в списке окна устройств, доступ к которым наследуется от устройства верхнего уровня

По умолчанию в окне отображаются все устройства, переключатели установлены в положение *Выключен* ( ).

5) При необходимости, выдать группе пользователей/пользователю права доступа к группе устройств/устройству, отличные от прав доступа к вышестоящей группе устройств, для чего:

- в строке настраиваемой группы устройств/устройства перевести переключатель ***Наследовать*** в положение *Выключено* ( );

– щелчком левой кнопки «мыши» включить/отключить права доступа группы пользователей/пользователя к группе устройств/устройству *Нет доступа*, *Чтение*, *Полный доступ*.

6) После выбора в окне настройки прав доступа пользователей к устройствам нажать кнопку ***Сохранить***. Окно закроется, внесенные изменения будут сохранены.

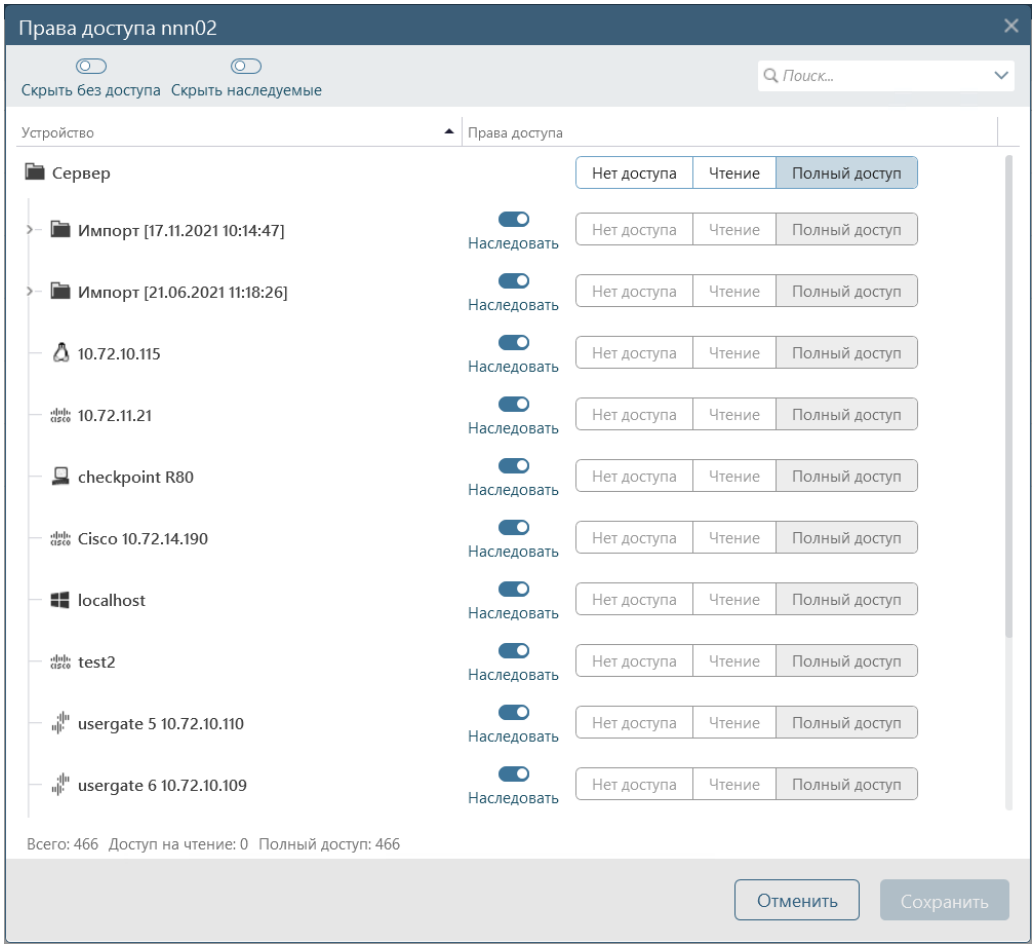


Рисунок 45 – Окно настройки прав доступа пользователей к устройствам

2.4.5. 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 может быть от 1 до 365 дней, настраивается в окне настройки параметров безопасности пользователей комплекса (см. пункт 2.4.9));
- 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. 46). Пользователю необходимо ввести дважды новый пароль и нажать кнопку ***Сохранить***. Окно смены пароля пользователя закроется, пароль пользователя будет изменен.

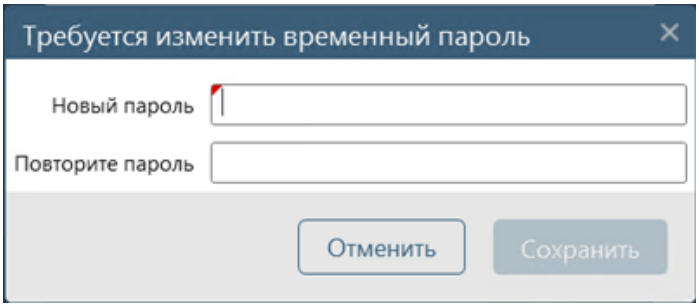


Рисунок 46 – Окно принудительной смены пароля пользователя

Для смены пароля ***текущего 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 (описание полей приведено в таблице 13).
4) Нажать кнопку ***Сохранить.*** Окно смены пароля пользователя закроется, пароль пользователя будет изменен.

Таблица 13 – Состав и описание полей окна смены пароля пользователя

Поле	Описание/Назначение
Текущий пароль	Действующий в текущий момент времени пароль пользователя
Новый пароль	Новый пароль пользователя
Повторите пароль	Подтверждение нового пароля пользователя

Для смены пароля ***пользователя из списка пользователей комплекса*** необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) В области *Администрирование* нажать ссылку ***Пользователи и группы***. Откроется форма управления пользователями системы и их правами.
3) Нажать кнопку ***Меню*** (▫▫▫) в строке требуемого пользователя.
4) Выбрать в раскрывшемся меню пункт ***Сменить пароль***. Откроется окно смены пароля пользователя, в котором необходимо вести новый пароль.

5) Нажать кнопку ***Сохранить.*** Окно смены пароля пользователя закроется, пароль пользователя будет изменен.

Примечание – При вводе нового пароля необходимо учитывать требования к его сложности (подробнее см. пункт 2.4.8. «Настройка параметров безопасности учетных записей пользователей комплекса»). При некорректно введенных данных могут возникать ошибки, перечень и правила исправления которых приведены в пункте 3.4.2.

2.4.6. Изменение параметров учетной записи пользователя комплекса

Для изменения параметров учетной записи пользователя комплекса необходимо выполнить следующие действия:

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

2) В области *Администрирование* нажать ссылку ***Пользователи и группы.*** Откроется форма управления пользователями системы и их правами.

3) Нажать в строке требуемого пользователя кнопку ***Изменить*** (). Откроется окно изменения данных пользователя (рис. 47).

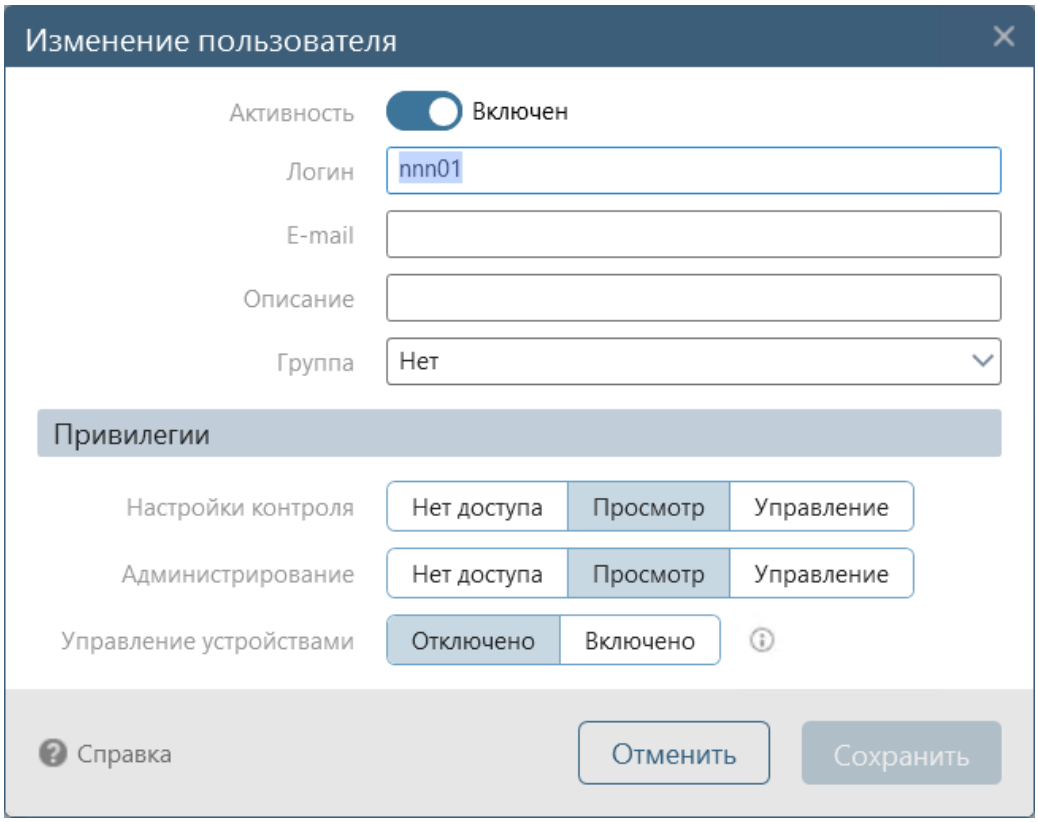


Рисунок 47 – Окно изменения параметров пользователя комплекса

4) Изменить требуемые параметры пользователя (логин, адрес электронной почты, описание, группу, доступ к настройкам контроля и администрированию комплекса, доступ к функциям управления устройствами). Нельзя изменить логин и описание доменного пользователя комплекса – поля не доступны для редактирования. Также, если пользователь (локальный или доменный) включен в группу, то не доступны для изменения его привилегии.

Примечание – Поле ***Управление устройствами*** отображается в форме только в том случае, если в состав ПК «Efros Config Inspector» v.4 входит модуль ***Управление устройствами*** и он включен.

5) Блокировать/разблокировать учетную запись пользователя, при необходимости, выбрав требуемое положение переключателя ***Активность***.

6) Нажать кнопку ***Сохранить***. Произойдет возврат в форму управления пользователями программного комплекса, внесенные изменения будут сохранены.

Изменение прав доступа пользователя к устройствам, подключенным к комплексу, выполняется в соответствии с п. 2.4.4 «Настройка прав доступа пользователей/групп пользователей к устройствам» и при добавлении и изменении устройств (подробнее см. раздел «Формирование списка контролируемых устройств» документа «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»).

2.4.7. Блокировка учетной записи пользователя комплекса

В ПК «Efros Config Inspector» v.4 существует возможность блокировки учетной записи пользователя (доменной группы пользователей в том числе) – в результате заблокированный пользователь не сможет авторизоваться для работы с комплексом из клиентской консоли.

Для того чтобы заблокировать учетную запись пользователя необходимо выполнить в клиентской консоли следующие действия:

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

2) В области *Администрирование* нажать ссылку ***Пользователи и группы***. Откроется вкладка **Пользователи**.

3) Нажать кнопку ***Меню*** (∘∘∘) в строке требуемого пользователя.

4) Выбрать в раскрывшемся меню пункт ***Заблокировать***. В результате выполненных действий имя пользователя окрасится в серый цвет.

Для того чтобы разблокировать учетную запись пользователя необходимо выполнить в локальной консоли следующие действия:

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

2) В области *Администрирование* нажать ссылку ***Пользователи и группы***. Откроется вкладка **Пользователи**.

3) Нажать кнопку ***Меню*** (∘∘∘) в строке требуемого пользователя.

4) Выбрать в раскрывшемся меню пункт ***Разблокировать***.

Примечание – Блокирование/разблокирование учетной записи пользователя может быть выполнено также при внесении изменений в карточке пользователя (см. п. 2.4.6 «Изменение параметров учетной записи пользователя комплекса») и, для доменной группы, в карточке доменной группы (см. п. 2.4.1.3 «Изменение параметров групп пользователей»).

2.4.8. Удаление учетной записи пользователя

Для удаления учетной записи пользователя необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) В области *Администрирование* нажать ссылку ***Пользователи и группы***. Откроется форма управления пользователями системы и их правами.
3) Нажать кнопку ***Меню*** (▫▫▫) в строке требуемого пользователя.
4) Выбрать в раскрывшемся меню пункт ***Удалить***. Откроется окно подтверждения удаления пользователя (рис. 48).

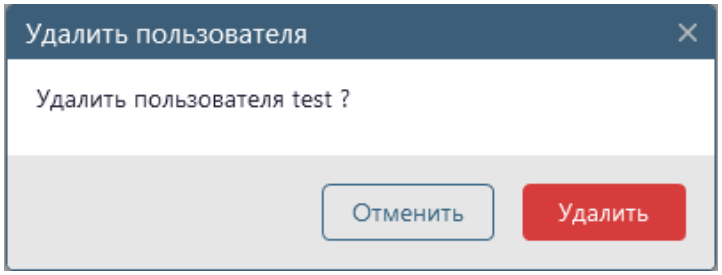


Рисунок 48 – Окно подтверждения удаления пользователя

5) Нажать кнопку ***Удалить***.

Пользователь будет удален из списка пользователей ПК и списков пользователей, имеющих доступ к устройствам.

В случае невозможности удаления пользователя откроется окно **Ошибка удаления пользователя.** В окне **Ошибка удаления пользователя** отображаются только те группы/устройства, в свойствах доступа к которым не установлен параметр ***Наследовать права доступа***.

Удаление учетной записи доменного пользователя из списка пользователей комплекса не влечет за собой удаление учетной записи этого пользователя с контроллера домена.

2.4.9. Настройка параметров безопасности учетных записей пользователей комплекса

В клиентской консоли ПК «Efros Config Inspector» v.4 есть возможность настройки параметров безопасности учетных записей пользователей комплекса. Установленные параметры парольной политики распространяются только на локальные учетные записи пользователей, для доменных пользователей остаются требования, установленные на контроллере домена.

Для того чтобы перейти к настройке параметров локальных пользователей необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, для чего нажать соответствующую кнопку в панели выбора раздела консоли.
2) В области *Администрирование* нажать ссылку ***Пользователи и группы***. Откроется форма управления пользователями системы и их правами.

3) В открывшейся форме управления пользователями системы и их правами нажать кнопку ***Настройки*** (⚙) в верхнем меню формы. Откроется окно **Настройки пользователей** (рис. 49, таблица 14).

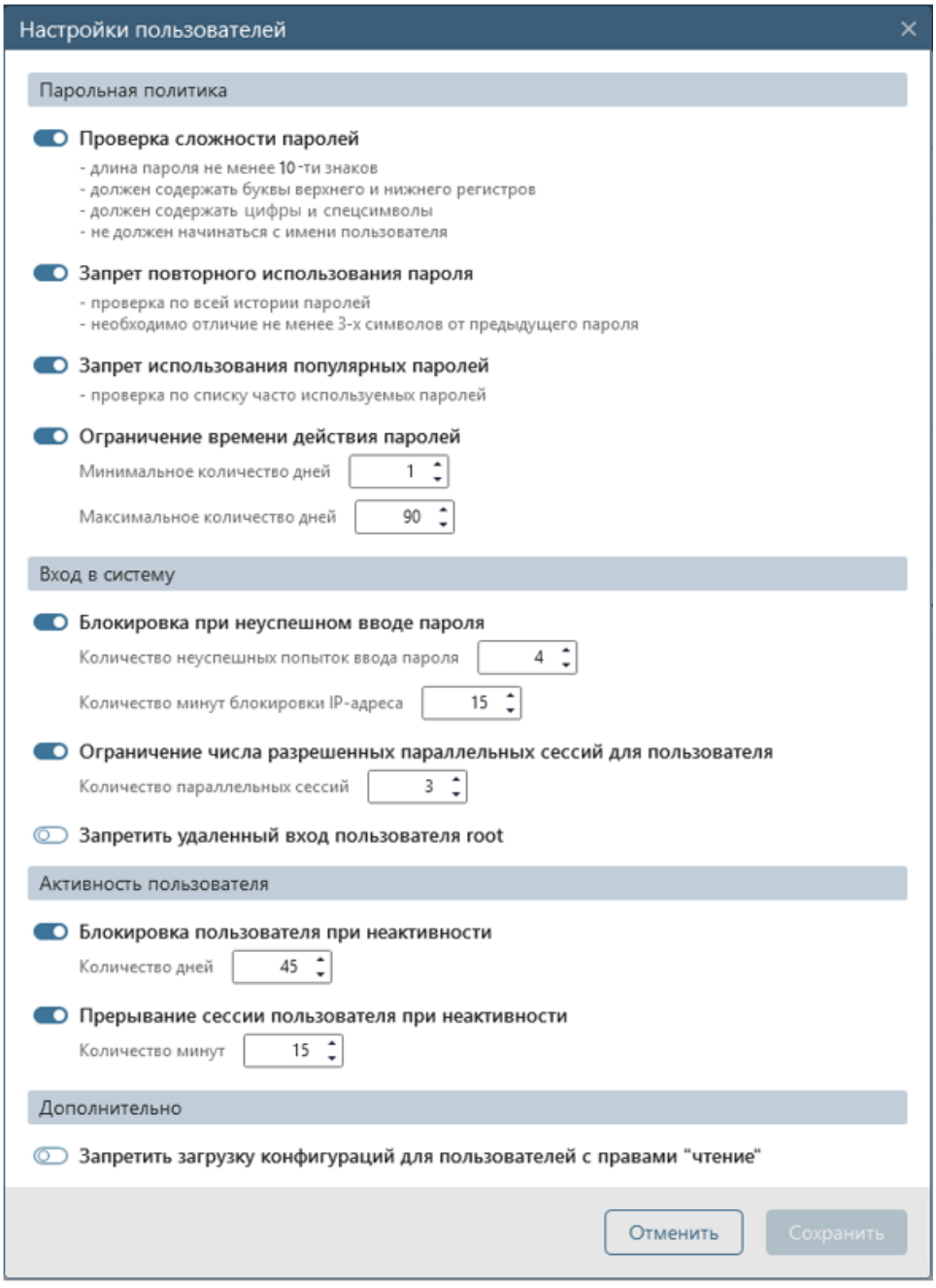


Рисунок 49 – Окно настройки параметров безопасности пользователей комплекса

Таблица 14 – Окно настройки параметров безопасности пользователей комплекса

Параметр	Описание/Значение по умолчанию
Проверка сложности паролей	При включенном переключателе (положение ⬤), осуществляется проверка сложности паролей пользователей комплекса: – минимальная длина пароля – 10 символов; – в пароле должны использоваться заглавные и строчные буквы; – в пароле должны использоваться цифры и спецсимволы; – пароль не может совпадать с именем пользователя (параметр

Параметр	Описание/Значение по умолчанию
	распространяется только на локальные учетные записи)
*Запрет повторного использования пароля**	При включенном переключателе (положение), средствами комплекса автоматически осуществляется проверка создаваемого пароля по истории паролей с запретом повторного использования пароля (отличие от используемого ранее пароля не менее чем на 3 символа)
*Запрет использования популярных паролей**	При включенном переключателе (положение), средствами комплекса автоматически осуществляется проверка создаваемого пароля на совпадение с популярными и общеизвестными паролями с запретом использования такого пароля
*Ограничение времени действия паролей**	При включенном переключателе (положение), устанавливаются минимальное (1 день) и максимальное (365 дней) время действия пароля
Блокировка при неуспешном вводе пароля	При включенном переключателе (положение), обеспечивается автоматическое блокирование на время от 10 до 60 минут программно-технического средства, с которого предпринимаются попытки доступа, при превышении пользователем ограничения количества неуспешных попыток входа в ПК «Efros Config Inspector» v.4 (возможность задания количества от 3 до 8 неуспешных попыток аутентификации)
Ограничение числа разрешенных параллельных сессий для пользователя	При включенном переключателе (положение), устанавливается ограничение на количество параллельных сеансов работы с серверной частью комплекса для учетной записи пользователя (минимальное значение – 1, максимальное – 32 сессии)
Запретить удаленный вход пользователя root	При включенном переключателе (положение), подключение встроенного пользователя (с логином root) с удаленной консоли запрещено
Блокировка пользователя при неактивности	При включенном переключателе (положение), осуществляется автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования не более 90 дней (возможность установки периода времени неиспользования от 1 до 90 дней)
Прерывание сессии пользователя при неактивности	При включенном переключателе (положение), осуществляется автоматическое блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя до 15 минут (возможность установки времени от 5 до 15 минут)
Запретить загрузку конфигураций для пользователей с правами «чтение»	При включенном переключателе (положение), осуществляется автоматическое блокирование загрузки конфигураций для пользователей с правами доступа к устройствам только «чтение (просмотр, загрузка отчетов)»
* - Параметр распространяется только на локальные учетные записи	

4) В открывшемся окне включить переключатели () необходимых параметров безопасности работы пользователей комплекса и задать требуемые количественные значения параметров (описание устанавливаемых параметров безопасности учетных записей пользователей комплекса приведено в таблице 14).

5) Нажать кнопку ***Сохранить***.

2.5. Настройка хранения данных в БД

Настройка хранения данных в БД программного комплекса выполняется в окне, приведенном на рисунке 50. Описание полей настройки базы данных комплекса приведено в таблице 15. Окно открывается при переходе из раздела **Настройки** по ссылке ***База данных***.

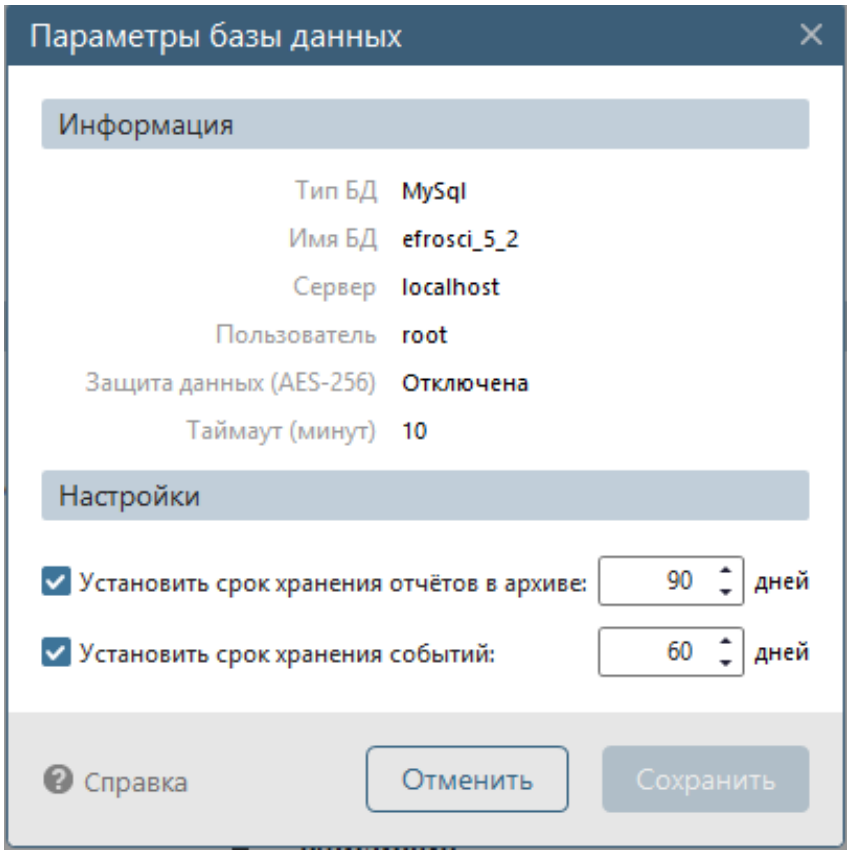


Рисунок 50 – Окно настройки параметров хранения данных в БД комплекса

Таблица 15 – Окно настройки параметров хранения данных в БД комплекса

Параметр	Назначение
Установить срок хранения отчетов в архиве	Определение срока хранения в БД отчетов, загруженных с устройств (в днях), по истечении которого отчеты будут автоматически удаляться.
Установить срок хранения событий	Определение срока хранения в БД записей о событиях (в днях), по истечении которого записи будут автоматически удаляться.

Настройки базы данных комплекса предназначены для экономии места на жестком диске и предотвращения значительного увеличения размера БД.

Для настройки сроков хранения данных в БД комплекса необходимо выполнить следующие действия:

1) В окне настройки параметров хранения данных в БД комплекса отметить параметры ***Установить срок хранения отчетов в архиве*** и ***Установить срок хранения событий*** и указать в соответствующих полях количество дней хранения в БД архивных отчетов и записей о событиях.

2) Нажать кнопку ***Сохранить.*** Окно настройки параметров хранения данных в БД комплекса закроется, внесенные изменения будут сохранены.

События и/или отчеты будут храниться в используемой БД постоянно, если в окне **Настройки базы данных** соответствующий параметр оставлен неотмеченным.

ВНИМАНИЕ: Вступление произведенных изменений параметров хранения данных в БД комплекса произойдет после перезапуска службы сервера программного комплекса (*EFROS CI Service 4*)!

2.6. Настройка использования коллекторов

Коллектор комплекса подключается к серверной части программного комплекса. При наличии большого количества задач серверной части (например, загрузка отчетов), часть задач передается на выполнение коллектору.

Для добавления коллектора администратору комплекса необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**, нажав соответствующую кнопку в панели выбора раздела консоли.

2) В области *Администрирование* нажать кнопку ***Коллекторы***.

3) В открывшейся форме управления коллекторами нажать кнопку ***Новый коллектор*** (рис. 51).

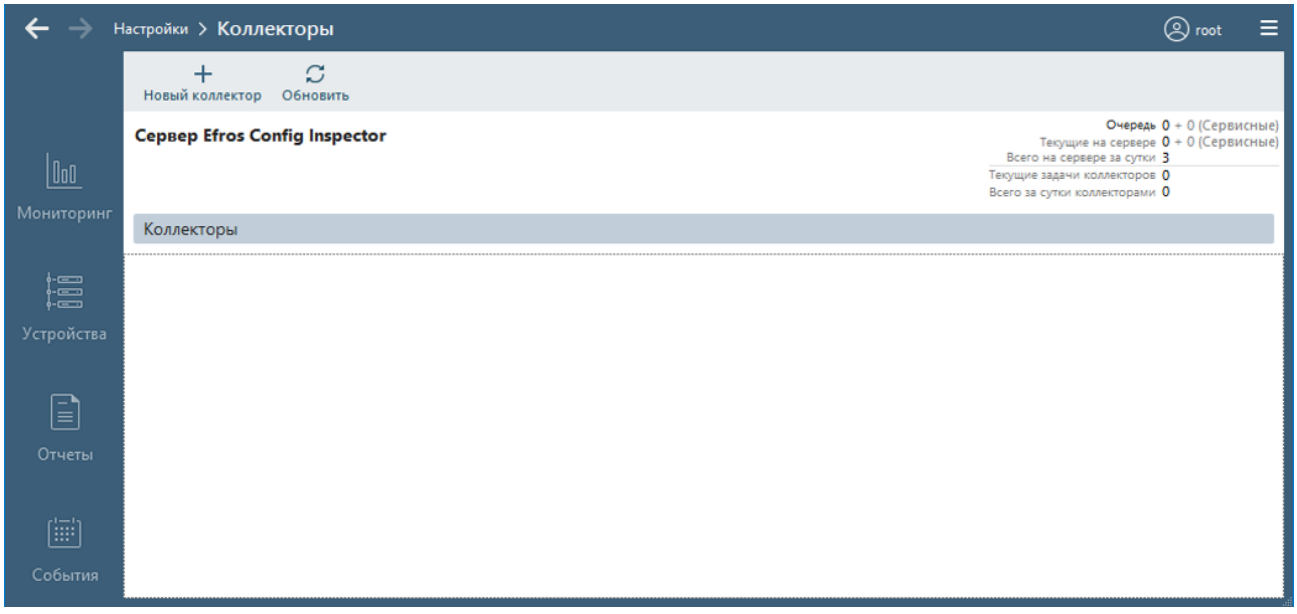


Рисунок 51 – Форма управления коллекторами задач

4) В открывшемся окне **Новый коллектор** (рис. 52) ввести IP-адрес добавляемого коллектора и порт подключения.

5) Подтвердить добавление коллектора задач, нажав кнопку ***Сохранить.***

Возможно подключение нескольких коллекторов задач. Число коллекторов ограничено приобретаемой лицензией.

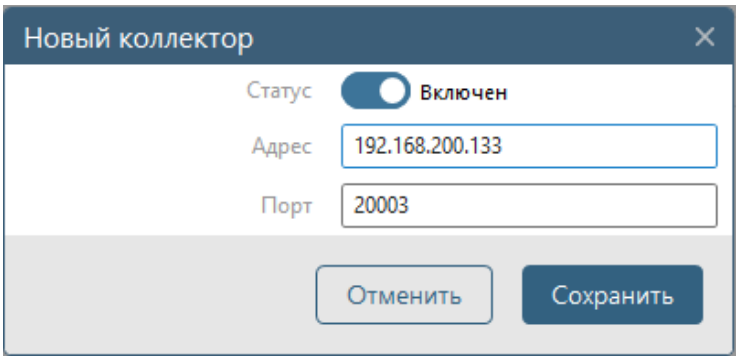


Рисунок 52 – Окно добавления нового коллектора задач

В окне управления будет выведен список коллекторов, где отображены (рис. 53):

- кнопка включения (отключения) использования коллектора задач ( );
- статус доступности коллектора (есть связь или нет связи). Если связь отсутствует из-за нарушения целостности ПО коллектора, то справа от статуса отобразится причина – «Нет связи (нарушена целостность)»;
- ***Текущие задачи*** – количество автоматически переданных задач серверной частью комплекса на выполнение коллектору задач;
- ***За сутки*** – параметр, отображающий количество выполненных коллектором за сутки задач;
- кнопка ***Настройки*** ( ) – открытие формы изменения параметров данного коллектора (IP-адрес и порт подключения). Данная форма практически совпадает с формой добавления нового коллектора (см. рис. 52);
- кнопка ***Удаление*** ( ) – удаление коллектора.

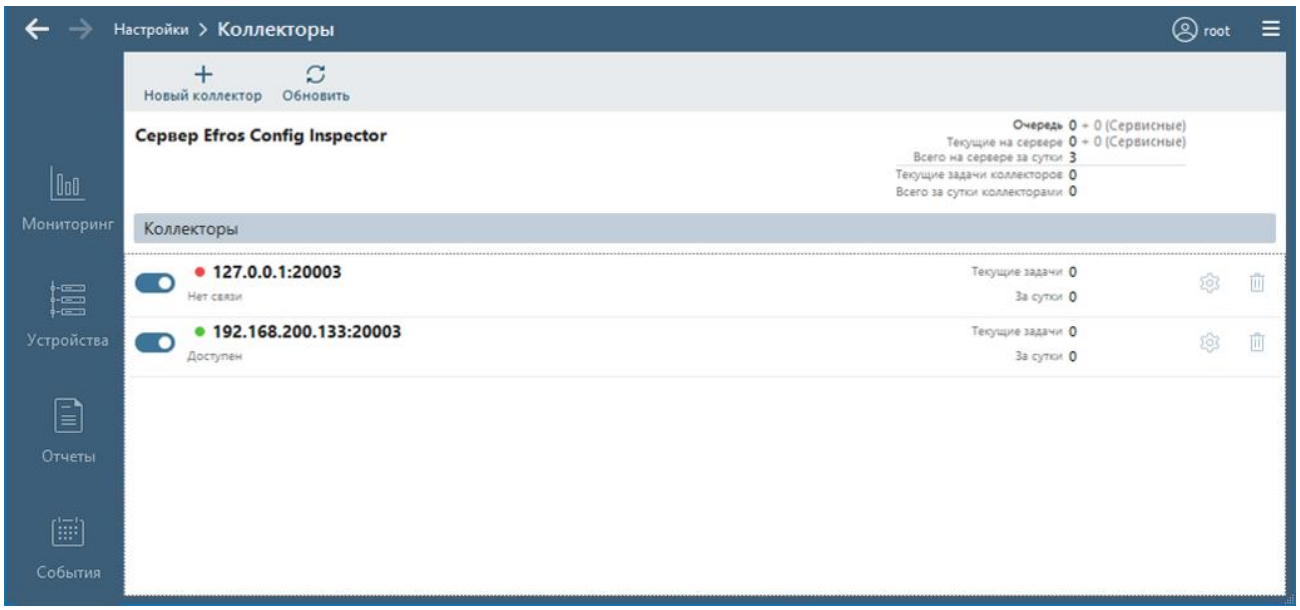


Рисунок 53 – Форма управления коллекторами задач с добавленными коллекторами

В верхней части окна управления коллекторами отображается общая статистика. В общей статистике отображены:

- ***Очередь*** – отображает количество задач в очереди на выполнение;
- ***Текущие на сервере*** – отображает количество текущих задач на сервере;
- ***Всего на сервере за сутки*** – отображает общее количество задач за сутки;
- ***Текущие задачи коллекторов*** – отображает количество текущих задач, переданных на выполнение всем коллекторам;
- ***Всего за сутки коллекторами*** – отображает общее количество задач, выполненных всеми коллекторами.

Установка коллектора возможна на резервный сервер. В случае перехода роли основного сервера к резервному, рекомендуется перенести коллектор на другой сервер.

2.7. Иерархия серверов

При наличии нескольких серверов ПК, а также необходимости централизованного управления, возможна настройка иерархии серверов.

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

Иерархия серверов представляет собой многоуровневую модель управления, в которой одному серверу, например, на уровне 1, 2 или 3 (управляющему) подчиняются управляемые сервера соответственно уровня 2, 3 или 4 (подчиненные).

Администратор комплекса определяет управляющий сервер из числа доступных серверов и осуществляет подключение управляемых им подчиненных серверов следующим образом:

- выполняет запуск клиентской консоли и ее подключение к управляющему серверу ПК;
- во вкладке **Настройки** в области ***Администрирование*** нажимает кнопку ***Иерархия***;
- в открывшейся форме **Иерархия** (рис. 54, состав элементов формы приведен в таблице 16) нажимает кнопку ***Добавить*** (+);

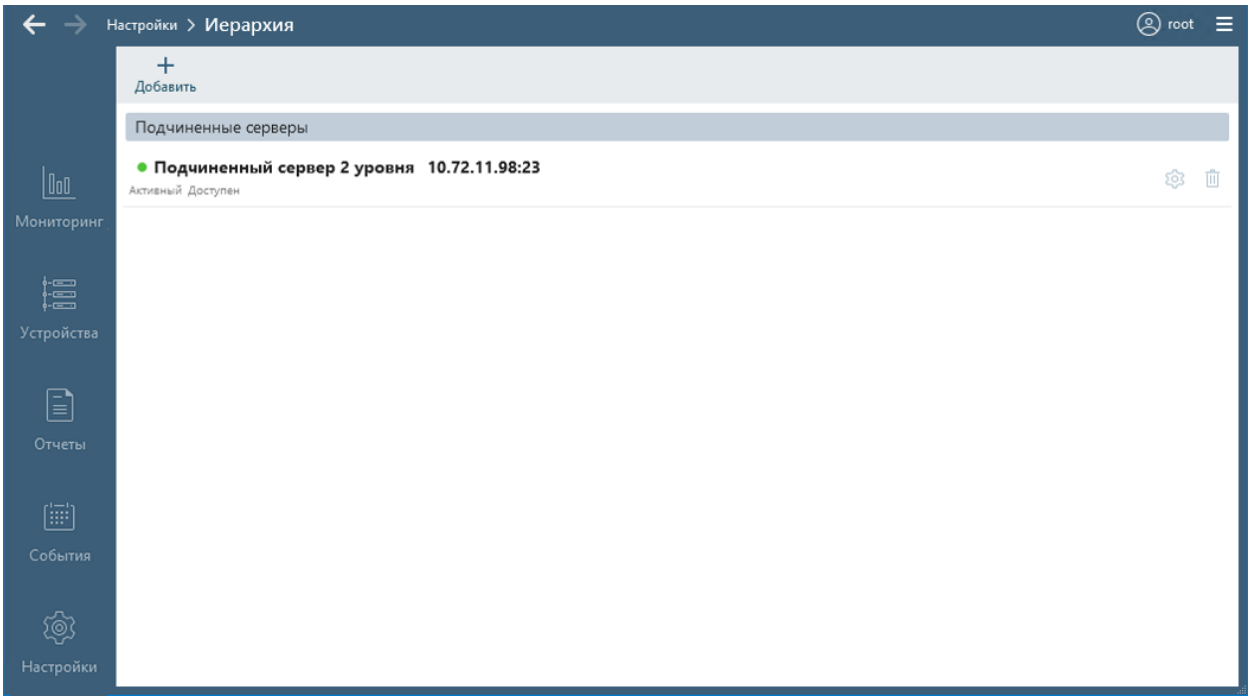


Рисунок 54 – Форма **Иерархия** для управляющего сервера 1 уровня (не имеет управляющий сервер), имеющего один подчиненный сервер

Таблица 16 – Элементы управления в форме настройки иерархии серверов

Элемент	Назначение
Кнопка ***Добавить*** (+)	Переход в окно добавления нового подчиненного сервера (рис. 55), где во вкладке ***Свойства*** необходимо указать параметры подключения управляемого сервера: – *Режим работы* – группа переключателей для выбора режима работы сервера (активный, пассивный, отключен); – *Имя* – название добавляемого сервера; – *Адрес* – IP-адрес добавляемого сервера; – *Порт* – порт подключения к добавляемому серверу; – *Логин и пароль* – учетные данные администратора сервера; – *Ограничение скорости* – переключатель для включения/отключения режима ограничения скорости при работе с подчиненными серверами (режим включен ()/отключен ())). А во вкладке ***Доступ*** – настроить доступ пользователей к добавляемому серверу (рис. 56).
Список серверов	Для каждого сервера отображаются: – *Имя сервера;* – *IP – адрес сервера и порт подключения* в формате *<IP-адрес> :<порт>;* – *статус сервера* – доступен или недоступен; – *режим работы сервера* – активный, пассивный, отключен; – *роль сервера* – управляющий или подчиненный. Примечание – После окончания срока действия лицензии на подчиненном сервере, статус сервера станет *Недоступен*, при наведении на статус курсора отобразится сообщение «*Текущая лицензия не поддерживает подключение к родительскому серверу*».

Элемент	Назначение
	Для каждого подчиненного сервера также отображаются кнопки: – *кнопка* Изменить ( ) – для перехода в форму изменения параметров сервера; – *кнопка* Удалить ( ) – для удаления сервера

- в окне **Новый сервер** на вкладках ***Свойства*** и ***Доступ*** (см. рис. 55, 56), вводит параметры подключения подчиненного сервера, описанные в таблице 16;
- нажимает кнопку ***Сохранить***.

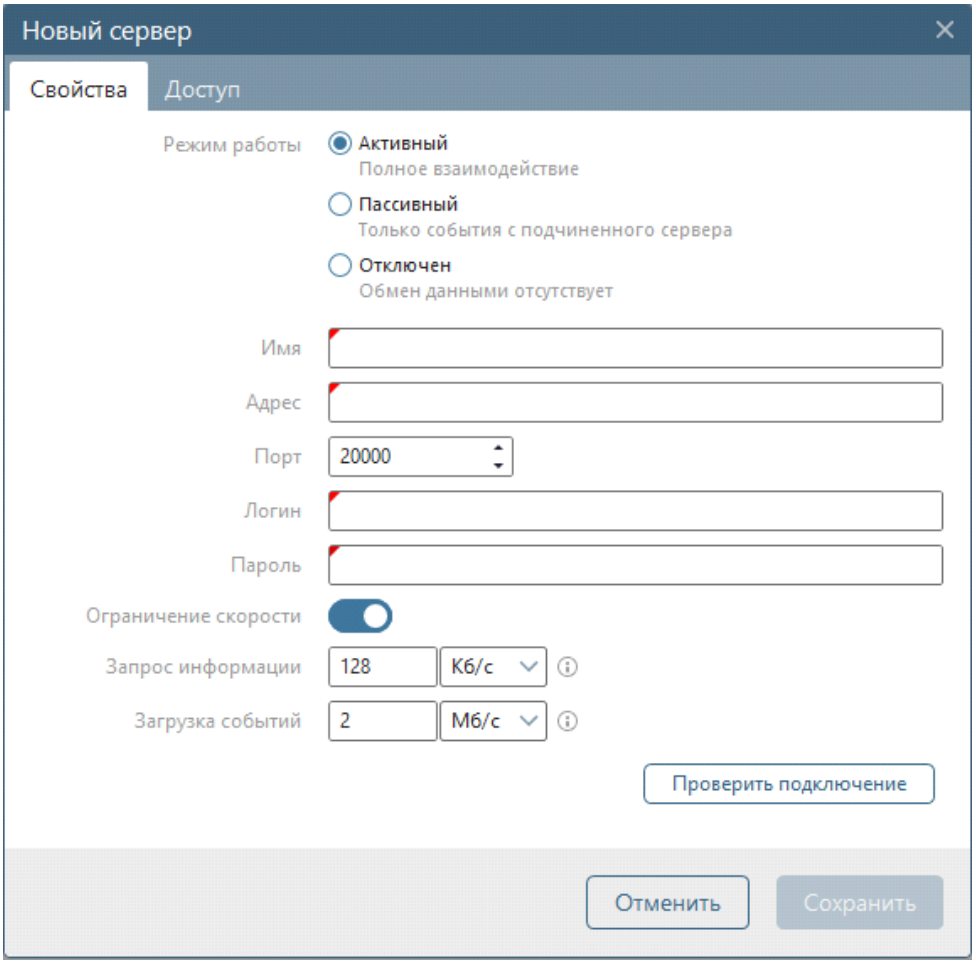


Рисунок 55 – Окно **Новый сервер**

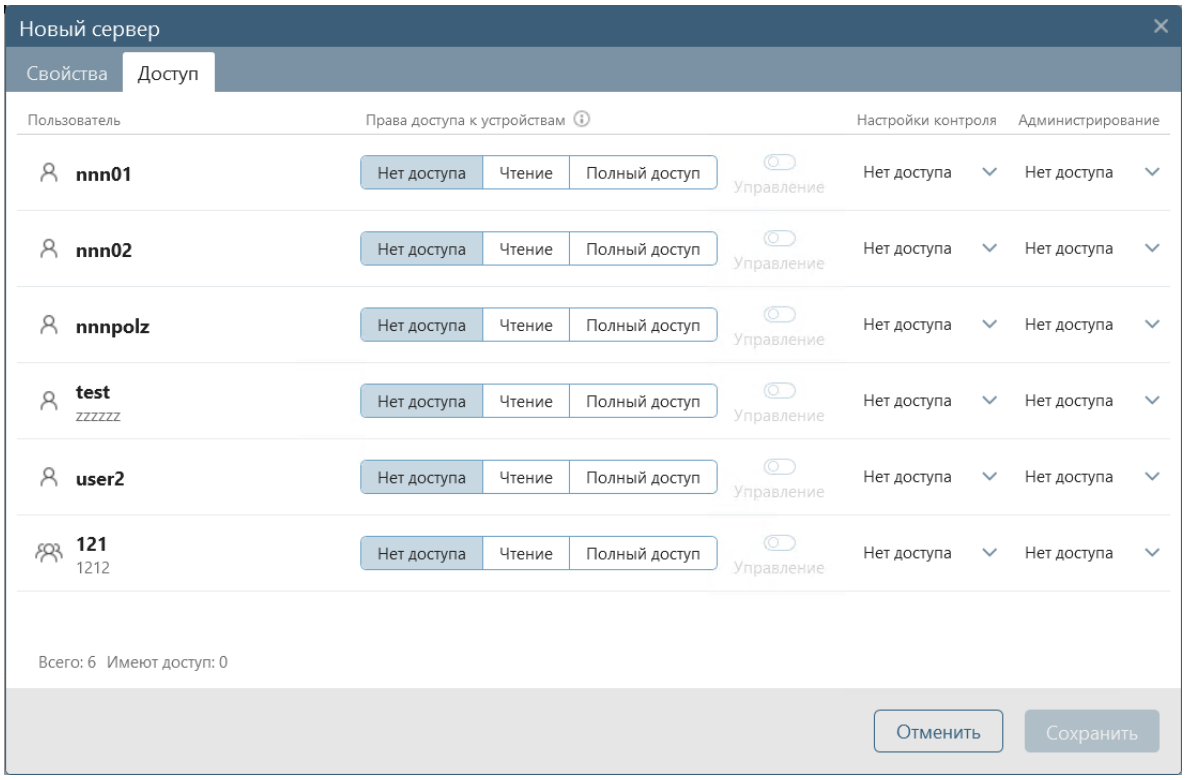


Рисунок 56 – Вкладка ***Доступ*** окна **Новый сервер**

После выполнения всех действий в области ***Подчиненные серверы*** будет отображен управляемый сервер и его статус (см. рис. 54).

При нажатии кнопки ***Настройки*** (⚙) открывается окно редактирования параметров подчиненного сервера. Кнопка ***Удалить*** (🗑) удаляет подчиненный сервер.

На управляемом сервере (сервер ПК, который добавлен на странице **Иерархия** для другого сервера в качестве подчиненного) в области ***Управляющий сервер*** будет отображен главный сервер, осуществляющий управление (рис. 57).

Рисунок 57 – Управляющий сервер

После настройки на управляющем сервере регистрируются события подчиненных серверов, где в столбце **Сообщение** также будет указан IP-адрес сервера, на котором произошло событие аудита.

В списке устройств раздела **Устройства** будут отображены наименования серверов, а также устройства, подключенные к ним (рис. 58).

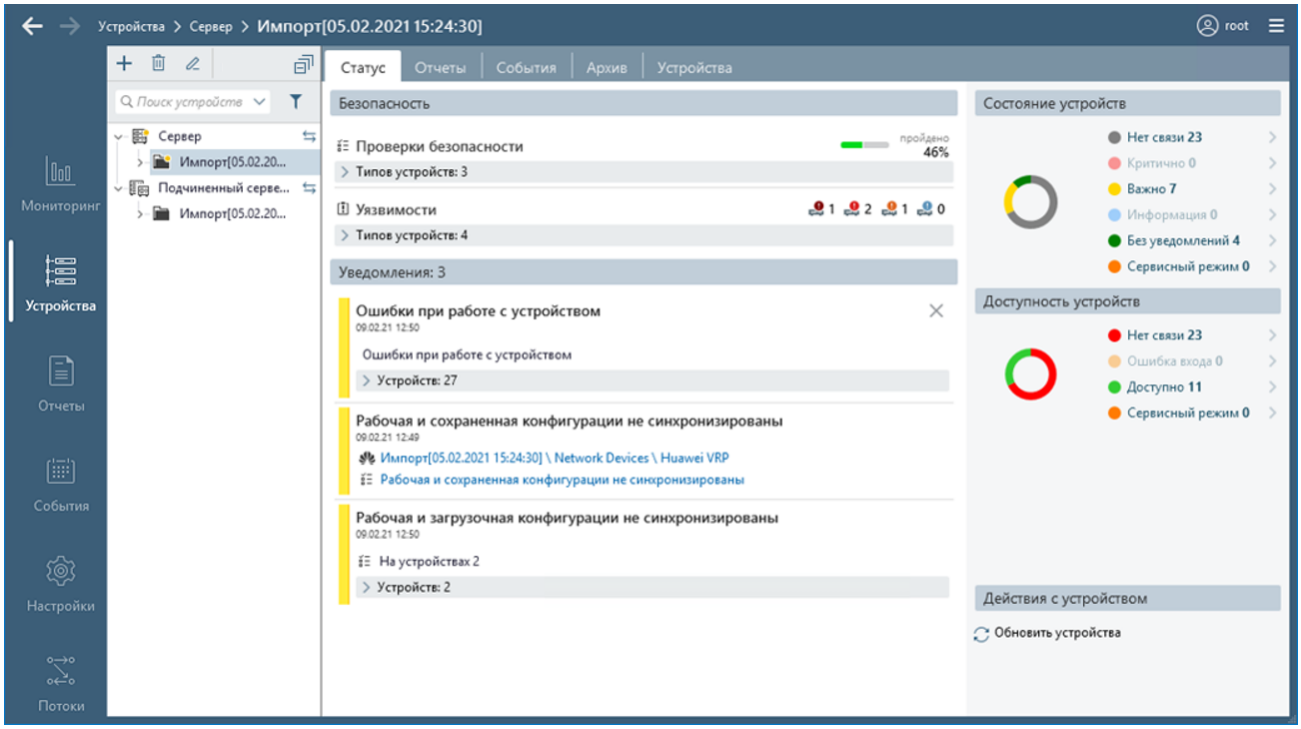


Рисунок 58 – Раздел **Устройства**

Одновременно в разделе **Устройства** отображаются данные не более чем с трех одновременно подключенных серверов (выбранных пользователем). Выбор серверов выполняется установкой флагов в окне **Выбор серверов** (рис. 59), которое открывается по нажатию кнопки «⇆» в строке любого отображаемого в текущий момент времени в списке устройств сервера.

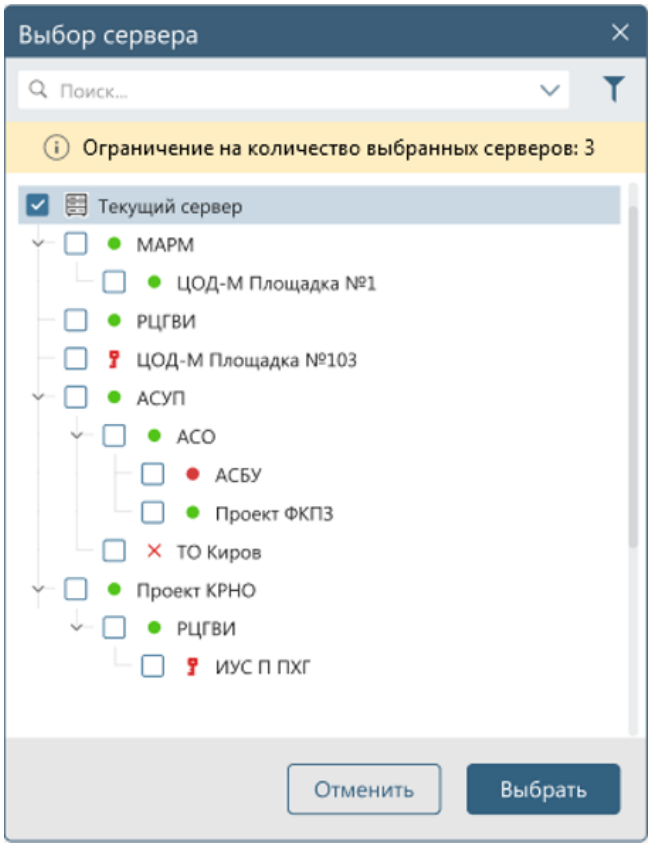


Рисунок 59 – Окно выбора серверов

Выбор применяется по нажатию кнопки ***Выбрать.*** Выбрано может быть одновременно не более трех серверов.

2.8. База уязвимостей

2.8.1. Настройка обновления базы уязвимостей

При переходе в раздел **Настройки** по ссылке ***База уязвимостей*** открывается форма **База уязвимостей** (рис. 60). Описание элементов управления, расположенных в форме, приведено в таблице 17.

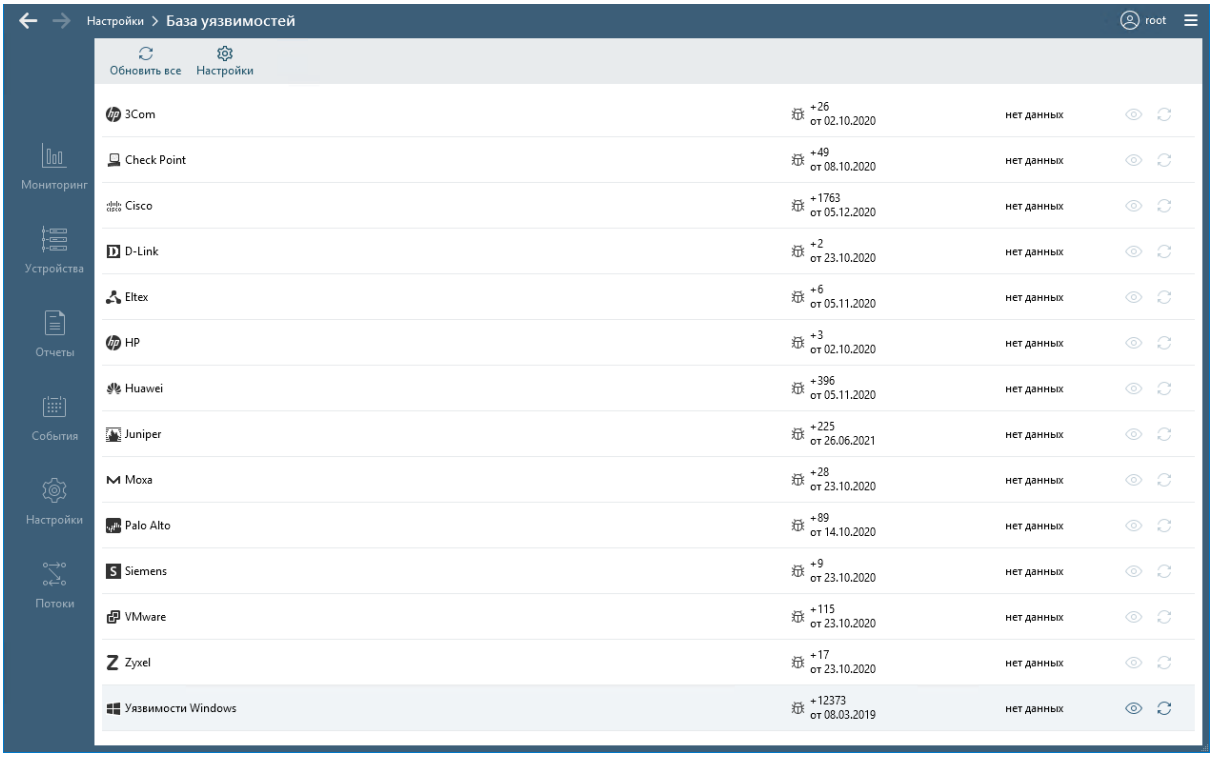


Рисунок 60 – Форма **База уязвимостей**

Таблица 17 – Элементы управления в форме **База уязвимостей**

Элемент	Назначение
Кнопка *Обновить все* ( )	Запускает процесс обновления баз уязвимостей для всех зарегистрированных модулей. Обновить БДУ для каждого зарегистрированного модуля отдельно можно, нажав кнопку ***Обновить***
Кнопка *Настройки* ( )	Переход в окно **Настройка сервера обновлений** (см. рис. 61, состав и описание значений полей окна приведено в таблице 18) для настройки и проверки подключения к БДУ

Для настройки сервера обновлений необходимо выполнить следующие действия:

1) Нажать кнопку ***Настройки*** ( ) в меню вкладки управления базой уязвимостей.

2) В открывшемся окне **Настройка сервера обновлений** выполнить настройку параметров подключения к базе данных (рис. 61).

3) Нажать кнопку ***Сохранить***.

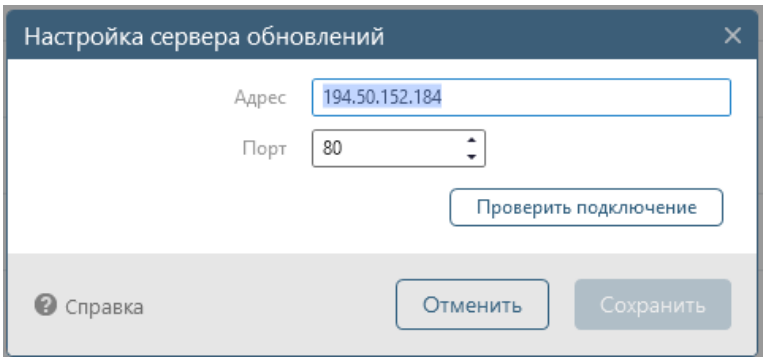


Рисунок 61 – Окно **Настройка сервера обновлений**

Таблица 18 – Состав и описание полей окна настройки обновления базы уязвимостей

Поле	Описание/Назначение
Адрес	Адрес сервера, на котором расположена база данных уязвимостей
Порт	Порт обмена данными с сервером, на котором распложена БДУ. После установки значений адреса и порта необходимо проверить подключение комплекса к серверу БДУ. Для чего нажать кнопку ***Проверить подключение***. В случае корректно установленных параметров рядом с кнопкой ***Проверить подключение*** (см. рис. 61) появится надпись ***Успешно***

2.8.2. Настройка расписания обновления БДУ

Для проведения обновления БДУ в ручном режиме необходимо:

1) Перейти в раздел **Настройки**.
2) В области *Администрирование* нажать кнопку ***База уязвимостей***.
3) В открывшейся форме нажать кнопку ***Обновить все*** ( ) (см. рис. 60) для обновления БДУ всех зарегистрированных в комплексе модулей. Для проведения обновления баз одного модуля, выбрать требуемый модуль и нажать в строке модуля кнопку ***Обновить*** ( ).

В результате выполненных операций БДУ зарегистрированных устройств будут обновлены. В форме будет указано время проведения проверки, количество уязвимостей в базе для каждого модуля и дата последнего обновления базы уязвимостей.

Для настройки периода обновления БДУ в автоматическом режиме необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**.
2) В области *Настройки контроля* нажать кнопку ***Расписания***.
3) В открывшейся форме **Расписания** выбрать расписание обновления базы уязвимостей и нажать кнопку ***Настройки*** ( ) в строке выбранного расписания.
4) В открывшемся окне **Свойства** (рис. 62) выполнить настройку параметра ***Запуск расписания***. При выборе в выпадающем списке ***Каждые***

параметров ***День, Неделя*** открываются дополнительно поля для настройки времени и дня старта выполнения операции обновления.

5) Нажать кнопку ***Сохранить.***

Установленные параметры настройки обновления БДУ будут применены для работы ПК «Efros Config Inspector» v.4.

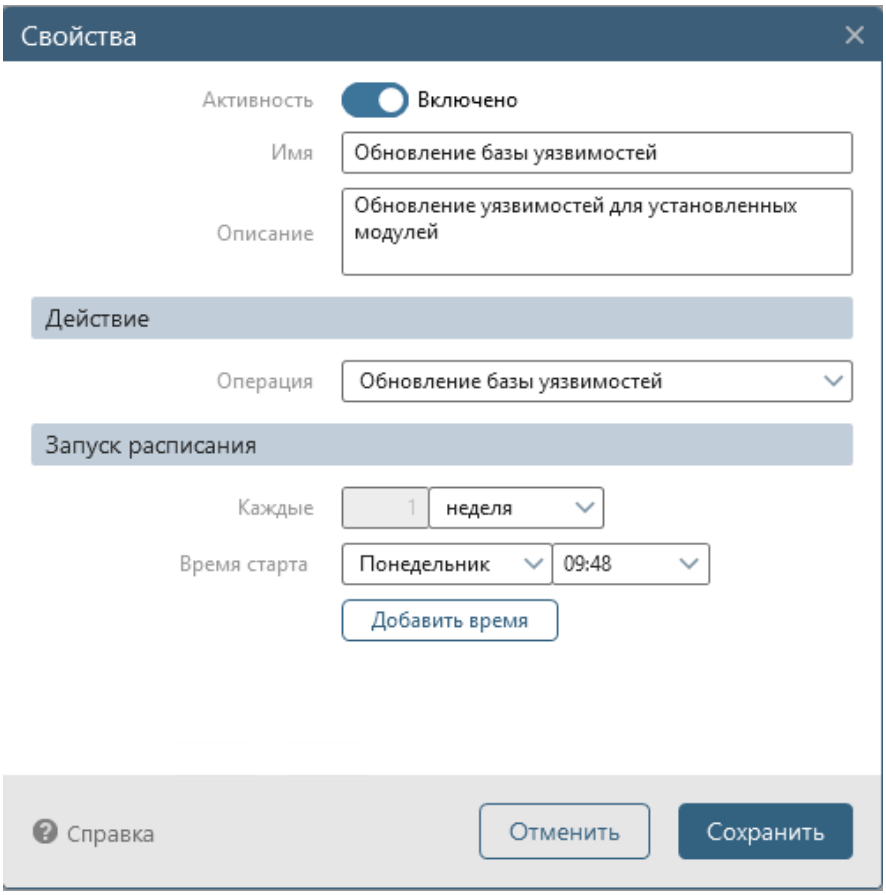


Рисунок 62 – Окно **Свойства** расписания обновления БДУ

2.8.3. Просмотр списка уязвимостей для внешнего модуля

Для просмотра списка уязвимостей одного из внешних модулей пользователю необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**.

2) В области *Администрирование* нажать кнопку ***База уязвимостей***. Откроется форма **База уязвимостей** (см. рис. 60). Форма содержит список подключенных к комплексу внешних модулей. В строке каждого модуля отображается наименование модуля, количество новых выявленных уязвимостей (при последнем обновлении), дата и время обновления БДУ.

3) В форме **База уязвимостей** нажать кнопку ***Просмотр*** () в строке требуемого модуля. Откроется форма просмотра списка уязвимостей для выбранного внешнего модуля (рис. 63). В заголовке формы содержатся данные: название модуля, дата и время последнего обновления словаря БДУ для модуля, количество уязвимостей в общем и по категориям: *Критический, Высокий, Средний* или *Низкий*. Форма содержит две вкладки:

- ***Отчет*** – со списком известных уязвимостей для модуля;

- ***История изменений*** – со списками новых (обнаруженных) и измененных уязвимостей, сгруппированных по датам обновления словаря модуля (загрузки из БДУ списка уязвимостей модуля). При их отсутствии во вкладке отображается сообщение ***Изменения отсутствуют***.

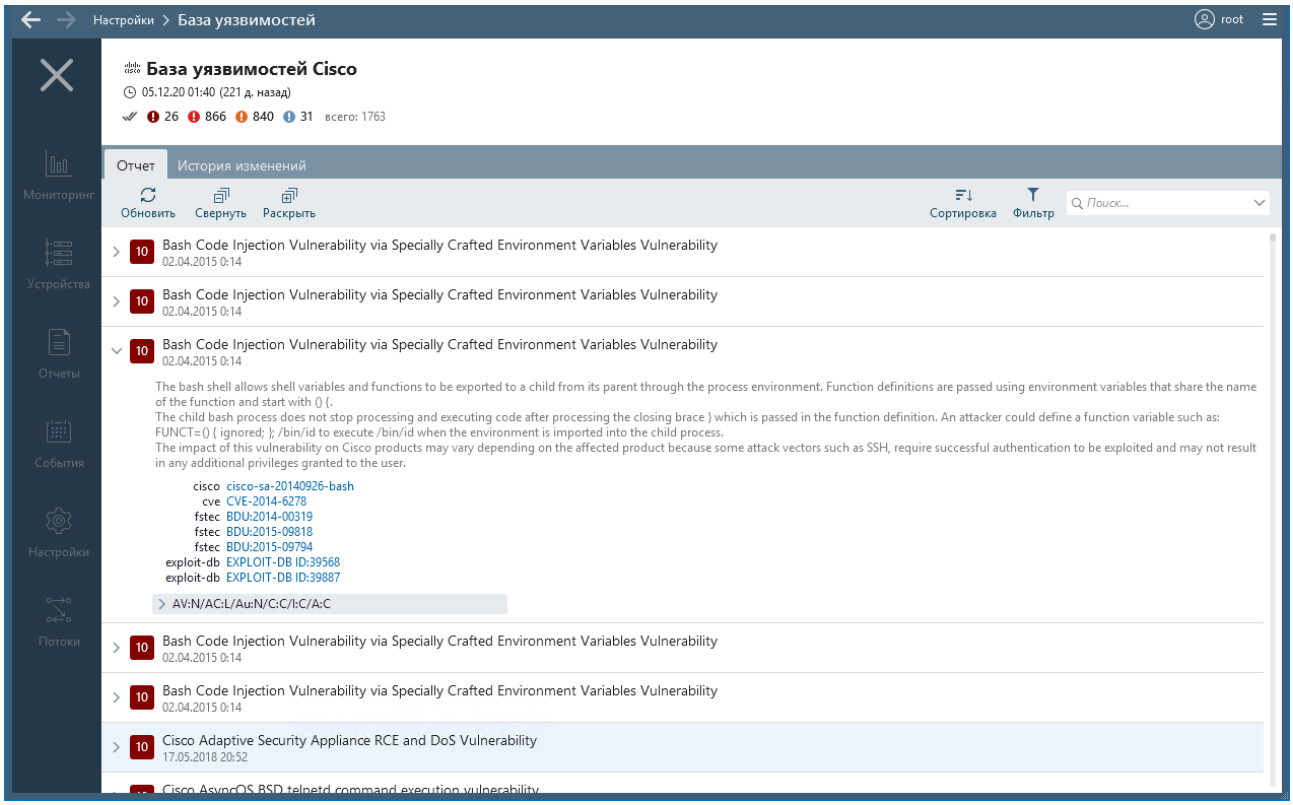


Рисунок 63 – Форма просмотра списка уязвимостей для внешнего модуля

Список уязвимостей вкладки ***Отчет*** по умолчанию отсортирован по критичности уязвимостей, начиная с высшего уровня критичности с наибольшей оценкой (10) до низкого уровня критичности. Для каждой уязвимости отображаются ее краткое описание и дата и время ее обнаружения и внесения в БДУ или обновления. В строках уязвимостей, актуальных для устройств комплекса, отображается пиктограмма и количество таких устройств. В развернутом состоянии для уязвимости отображаются ее полное описание, вектор и список устройств комплекса, для которых уязвимость актуальна.

В заголовке вкладки доступны кнопки:

- ***Обновить*** () – для обновления словаря модуля (загрузки из БДУ списка уязвимостей);
- ***Свернуть*** () и ***Раскрыть*** () – для сворачивания/разворачивания дерева уязвимостей;
- ***Сортировка*** () – для выбора критерия сортировки списка: *по оценке* (выбран по умолчанию), *по дате изменения, по количеству устройств*;
- ***Фильтр*** () – для фильтрации уязвимостей по наличию устройств комплекса, для которых уязвимость актуальна, по источнику (для

определения уязвимостей в базе ФСТЭК, mitre и других) и сброса настройки фильтра.

2.9. Настройка подключения к прокси-серверу БДУ

При необходимости подключения комплекса к БДУ через прокси-сервер администратору необходимо выполнить следующие действия:

1) Перейти в раздел **Настройки**.
2) В области *Администрирование* нажать кнопку ***Прокси-сервер***.

Откроется окно **Прокси-сервер** (рис. 64, таблица 19).

3) Установить переключатель ***Прокси-сервер*** в положение *Включен* (). Поля окна станут доступны для внесения изменений.
4) Ввести в поля окна настройки подключения IP-адрес/имя и номер порта прокси-сервера.
5) Установить, при необходимости, переключатель ***Авторизация*** в положение *Включен* () и указать учетные данные пользователя для подключения к прокси-серверу.
6) Нажать кнопку ***Сохранить***.

После сохранения внесенных данных подключение к БДУ будет выполняться через указанный в настройках прокси-сервер.

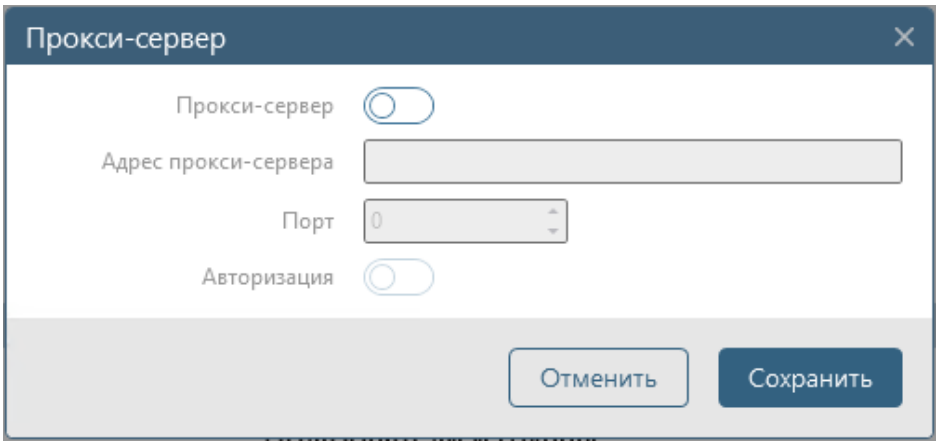


Рисунок 64 – Окно настройки подключения к прокси-серверу БДУ

Таблица 19 – Элементы управления в окне настройки подключения к прокси-серверу БДУ

Элемент	Назначение
Переключатель *Прокси-сервер*	Переключатель для включения/отключения режима подключения к БДУ через прокси-сервер (режим включен ()/отключен ()). По умолчанию переключатель отключен и все поля окна неактивны
Адрес прокси-сервера	IP-адрес или имя (FQDN) подключаемого прокси-сервера
Порт	Порт для подключения прокси-сервера

Элемент	Назначение
Переключатель ***Авторизация***	Переключатель для включения/отключения необходимости авторизации при подключении к прокси-серверу (авторизация требуется ( )/не требуется ( )). По умолчанию переключатель выключен. После включения переключателя в окне отображаются дополнительно поля для ввода данных пользователя для авторизации на прокси-сервере (рис. 65)
Логин	Логин пользователя для подключения к прокси-серверу
Пароль	Пароль пользователя для подключения к прокси-серверу

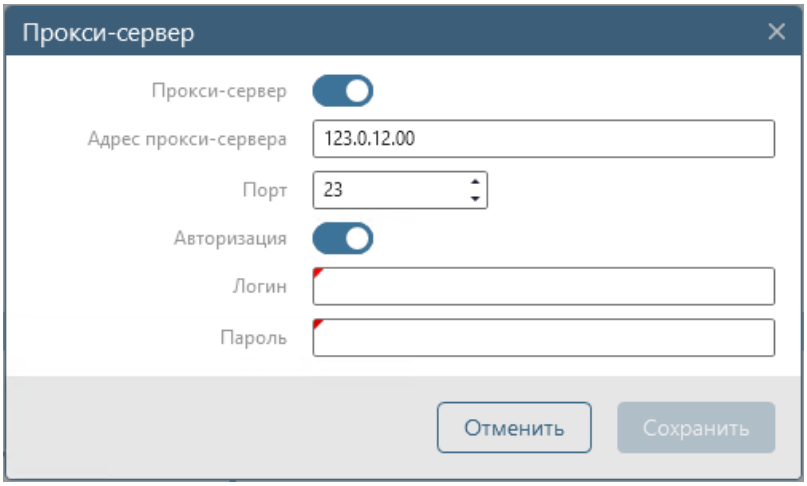


Рисунок 65 – Окно настройки подключения к прокси-серверу в режиме ввода данных пользователя для авторизации на прокси-сервере

2.10. Настройка подключения к серверу «Flow Server»

Программный компонент «Flow» доступен для использования только при его наличии в лицензии на ПК «Efros Config Inspector» v.4. Компонент предназначен для отображения статистики использования сетевого трафика по соединениям, поддерживает работу с устройствами типа Cisco IOS и Cisco ASA.

Программный компонент «Flow» устанавливается на ЭВМ установки серверной части комплекса и обеспечивает выполнение следующих функций:

- подключение к серверу «Flow Server» для получения собранной на сервере статистики использования сетевого трафика по соединениям;
- предоставление пользователям информации по соединениям, с параметрами скорости, длительности и принадлежности к адресам;
- отображение статистики на графике и формирование списков топ активности;
- формирование событий о зафиксированной активности в рамках параметров созданных триггеров;
- выгрузка информации в отчеты для предоставления заинтересованным лицам;
- возможность анализа активности благодаря фильтрам и просмотру событий.

После установки программного компонента «Flow» необходимо выполнить настройку подключения программного компонента «Flow» к серверу «Efros Flow», для чего выполнить следующие действия:

1) Перейти в раздел **Настройки**.
2) В области *Администрирование* нажать кнопку ***Потоки***. Откроется окно **Потоки** с параметрами настройки подключения к серверу «Flow Server» (рис. 66). Окно содержит поля для ввода IP-адреса и номера порта сервера «Flow Server»

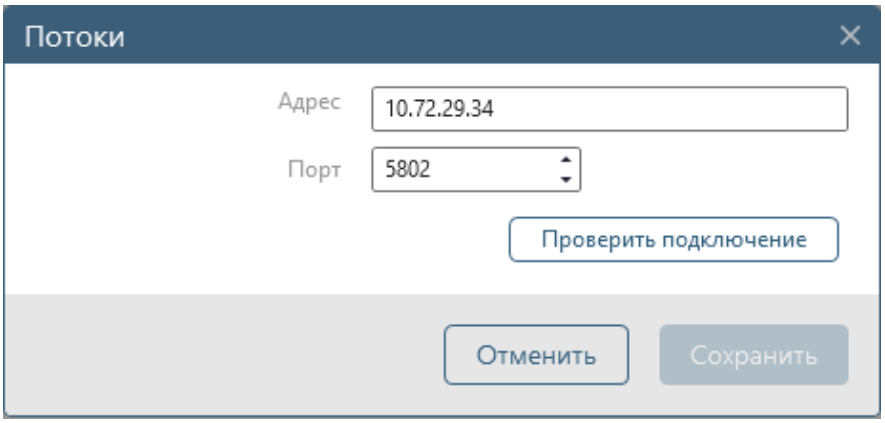


Рисунок 66 – Окно настройки подключения к серверу «Flow Server»

3) Ввести в поля окна настройки подключения IP-адрес и номера порта сервера «Flow Server».
4) Для проверки подключения и правильности ввода параметров нажать кнопку ***Проверить подключение***. В случае успешного подключения в окне настройки появится сообщение *Успешно* (рис. 67), в случае неуспешной проверки подключения к серверу «Flow Server» – сообщение *Ошибка*.
5) Нажать кнопку ***Сохранить***.

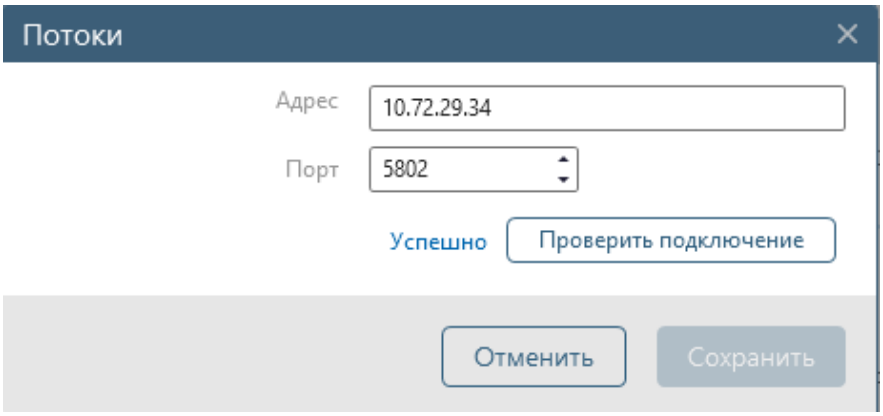


Рисунок 67 – Окно настройки подключения к серверу «Flow Server» после успешной проверки подключения

2.11. Просмотр списка задач комплекса

В ПК «Efros Config Inspector» v.4 администратор может просмотреть список текущих и выполненных задач комплекса.

Для просмотра пользователю необходимо перейти в раздел **Настройки** и в области *Администрирование* нажать кнопку ***Мониторинг задач***. Откроется страница **Мониторинг задач** (рис. 68). Страница содержит:

- кнопку ***Обновить*** (). По нажатию кнопки выполняется обновление списка, обновление состояния загруженных ранее в список заданий/задач выполняется в автоматическом режиме;
- кнопку ***Фильтр*** (). По нажатию кнопки открывается окно фильтрации, в котором возможно установить фильтр поиска, по признакам *Состояние*, *Тип задания* и *Тип задачи* или сбросить настройки фильтра;
- поле поиска. Позволяет выполнить поиск в списке задач по комбинации букв и символов из элементов заданий/задач раздела **Мониторинг задач.** В качестве результата выводятся все задачи и задания, соответствующие поисковому запросу;
- список задач сервера, выбранного в заголовке страницы раздела **Настройки**.

Список содержит последние 1000 задач, отсортированные в порядке убывания даты и времени старта их выполнения. Задачи сгруппированы по заданиям.

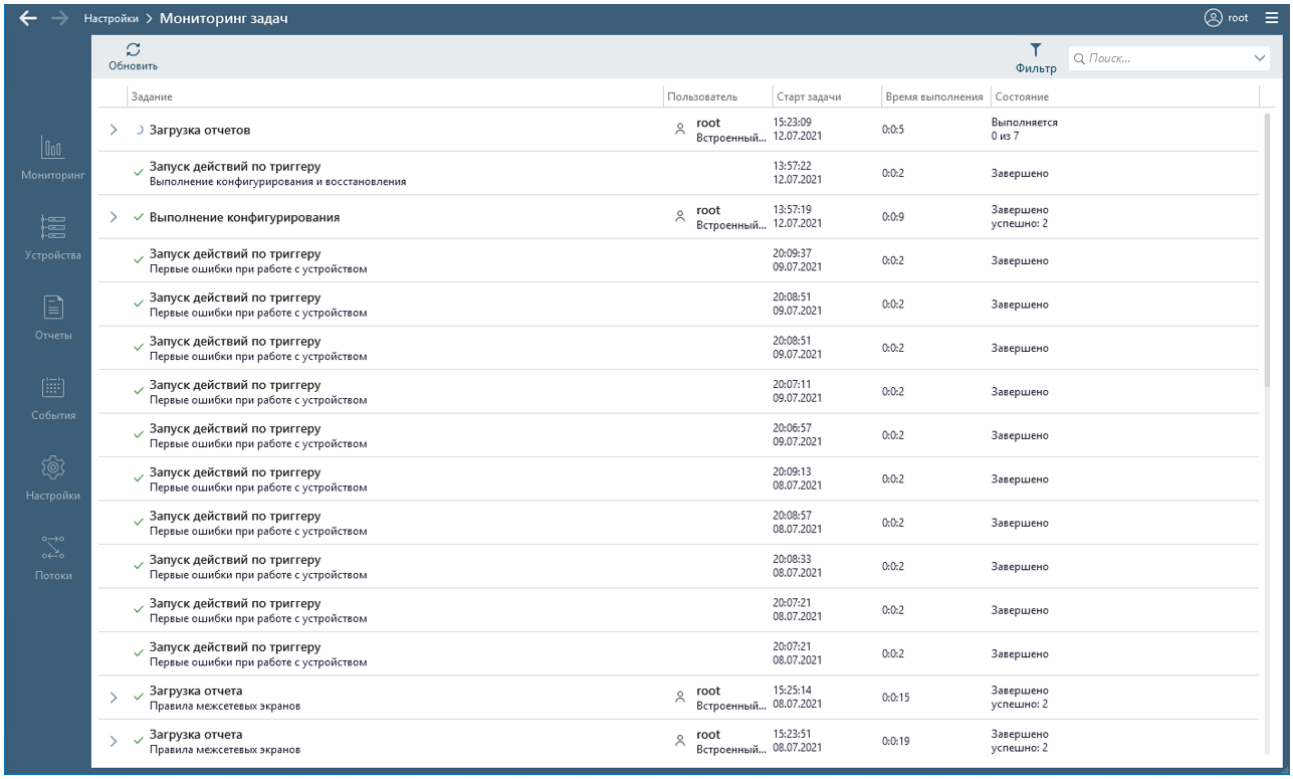


Рисунок 68 – Страница **Мониторинг задач**

В строке задания отображается пиктограмма статуса задания, наименование задания, его статус.

Возможные статусы заданий:

- – в текущий момент времени выполняется (статус *Выполняется XX из YY* либо *Выполняется XX из YY (ошибок ZZ)*);

- ● – все задачи задания завершены с ошибкой (статус *Завершено ошибок YY*);
- ✓ – все задачи задания завершены успешно (статус *Завершено успешно XX*);
- ●.– часть задач задания завершена успешно, часть – с ошибкой (статус *Завершено успешно NN, ошибок MM*).

Список задач задания раскрывается по нажатию кнопки «›» в строке задания (рис. 69). Для каждой задачи отображается информация:

1) Пиктограмма состояния задачи:
   - – в ожидании;
   - – в текущий момент времени выполняется;
   - ● – завершена с ошибкой;
   - ✓ – завершена успешно;
   - ✕ – отменена.

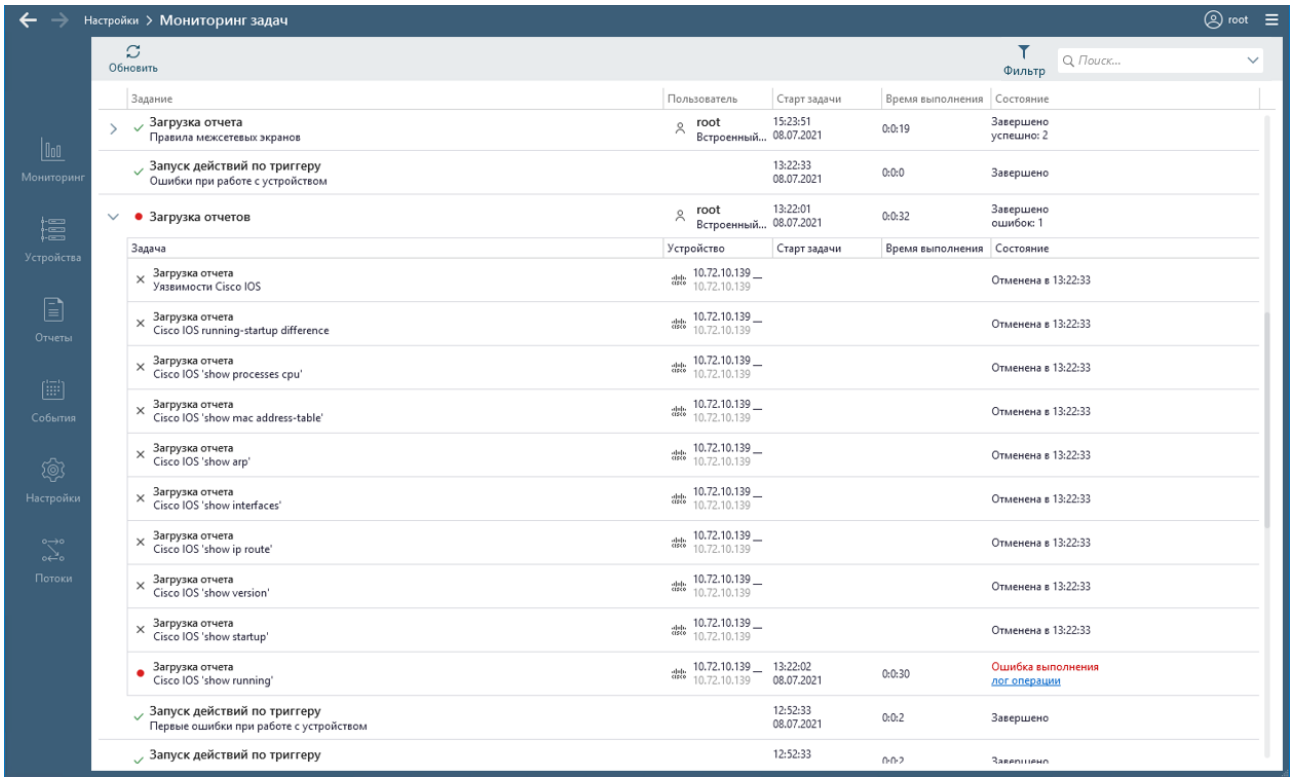


Рисунок 69 – Список задач задания

2) Тип задачи. Возможные значения:
   - загрузка отчёта;
   - восстановление конфигурации;
   - выполнение операции;
   - проверка соединения;
   - выполнение конфигурирования;
   - отправка сообщения;
   - проверка подключения с серверу обновления уязвимостей;
   - обновление словаря уязвимостей;
   - загрузка списка файлов;

- загрузка ключей реестра.

3) Наименование устройства.
4) Дата и время старта выполнения задачи.
5) Время выполнения задачи.
6) Состояние задачи. Возможные значения:
   - в ожидании;
   - выполняется;
   - ошибка выполнения;
   - завершена;
   - отменена.

Для задач, завершившихся с ошибкой, пользователь имеет возможность просмотреть лог выполнения задачи, для чего необходимо в строке задачи нажать ссылку ***Лог операции***.

2.12. Формирование списка и управление списком устройств

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

Раздел **Устройства** открывается при запуске клиентской консоли и при выборе кнопки ***Устройства*** в клиентской консоли.
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 более подробно изложены в п. 2.4 и 2.5 документа 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».

В разделе **Настройки** в области ***Настройки контроля*** пользователям с правами *Управление* в категории *Настройки контроля* доступны для выполнения действия с устройствами по нажатию кнопок:

- ***Экспорт настроек*** – позволяет экспортировать список устройств, а также профилей устройств, пользовательских отчетов и проверок, стандартов проверок межсетевых экранов в файл отчета;

- ***Импорт настроек*** – позволяет импортировать список устройств, а также профилей устройств, пользовательских отчетов и проверок, стандартов проверок межсетевых экранов из файла;
- ***Сканирование*** – задание параметров сканирования для поиска устройств в сети;
- и при выборе ссылок под кнопкой ***Устройства***:
  - ***Карта*** – отображает карту всех устройств сети и связи между ними;
  - ***Доступность устройств*** – установка параметров для проверки доступности устройств за определенный период.

Описание порядка и правил выполнения указанных действий подробно изложены в документе 643.72410666.00082-01 96 01-02 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 2. Настройки контроля».

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. 70. 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.

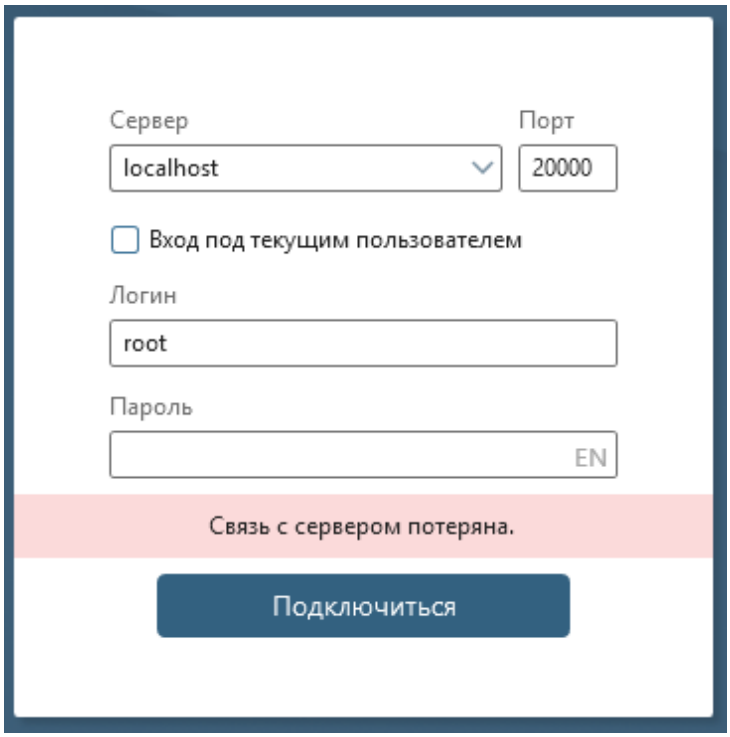


Рисунок 70 – Ошибка сетевого соединения между клиентской консолью и сервером ПК

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. 71). Запись об обнаружении нарушения будет также занесена в журнал событий раздела **События**.

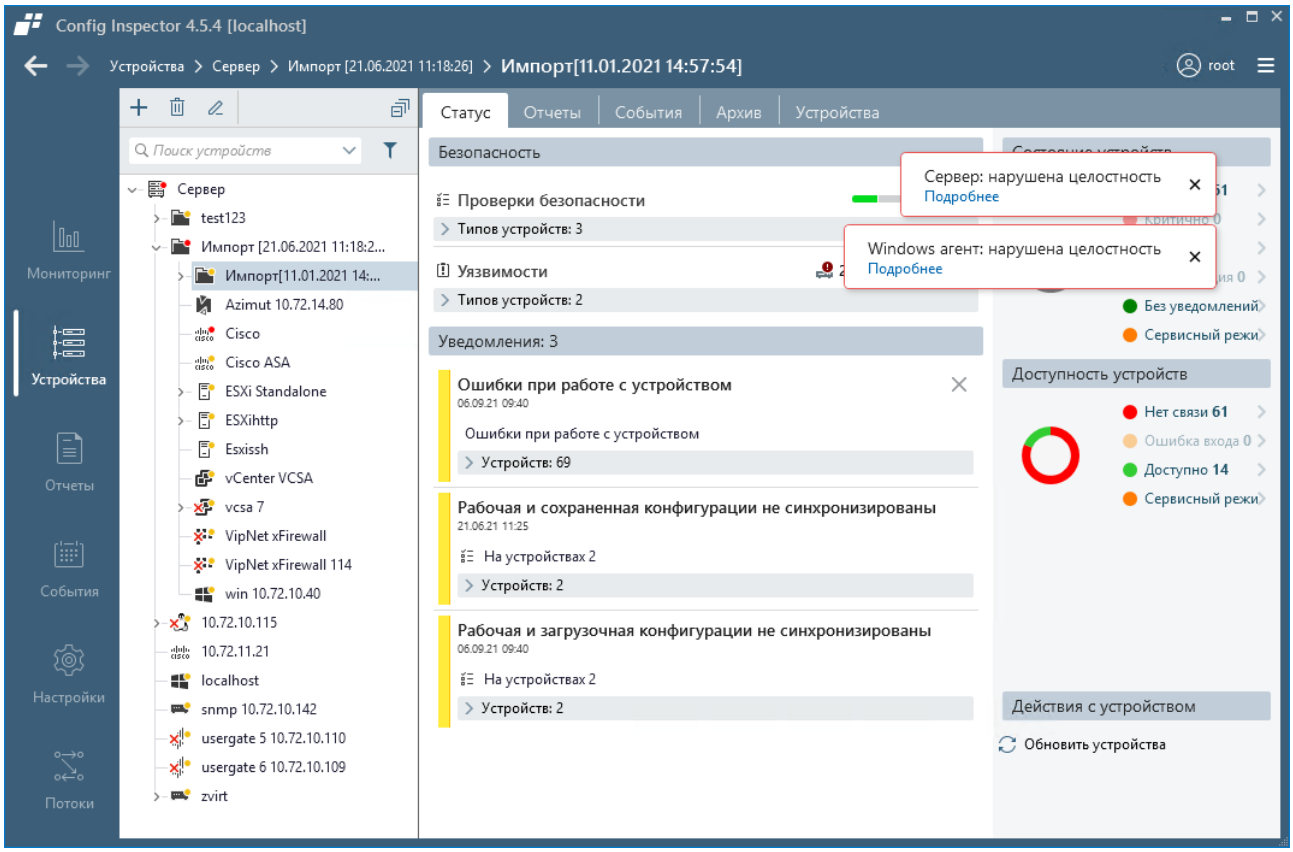


Рисунок 71 – Уведомления об обнаружении нарушения целостност компонентов комплекса

Пользователь имеет возможность просмотреть перечень обнаруженных нарушений, нажав ссылку *Подробнее* (рис. 72). 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.

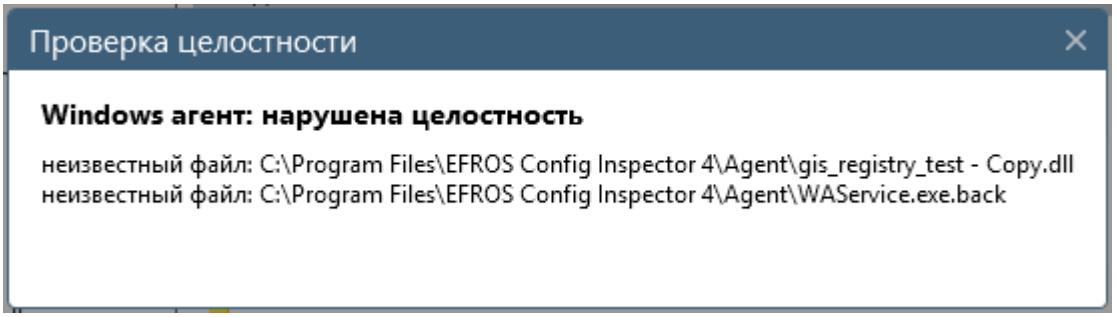


Рисунок 72 – Окно просмотра перечня обнаруженных нарушений при контроле целостности компонента комплекса

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

После этого пользователь приводит настройки ПК «Efros Config Inspector» v.4 в соответствие с настройками, указанными в эксплуатационной документации.

3.3. Сбой в работе сервера ПК «Efros Config Inspector» v.4 или СУБД

В случае сбоя работоспособности сервера ПК «Efros Config Inspector» v.4 или СУБД, пользователь не сможет выполнить запуск клиентской консоли, пользователю необходимо обратиться к администратору ПК «Efros Config Inspector» v.4.

Администратору «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 клиентской консоли 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. 73) 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***.

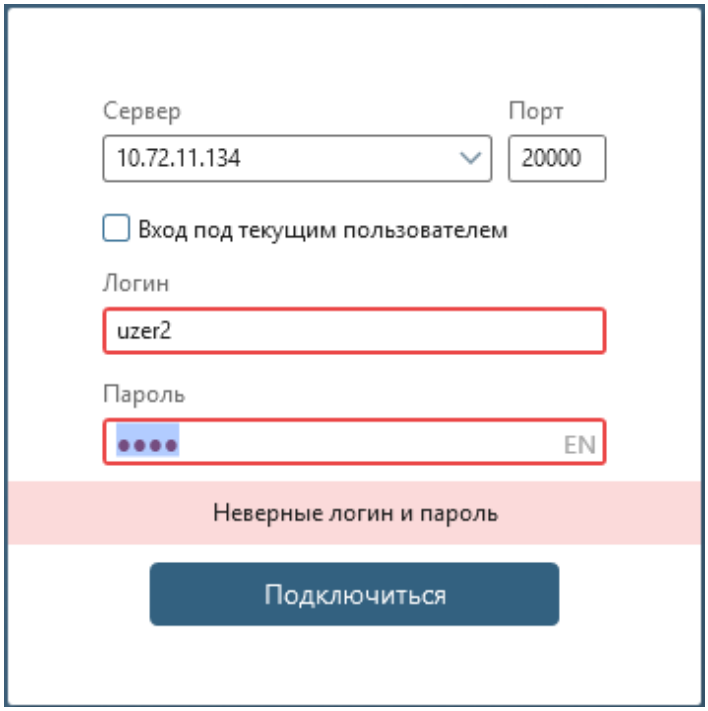


Рисунок 73 – Окно подключения к серверу ПК после ввода неверных данных пользователя

При получении сообщения о временной блокировке IP-адреса после нескольких подряд попытках (от 3 до 8) неверного ввода аутентификационных данных пользователя (рис. 74) 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 (см. п. 2.4.9 «Настройка параметров безопасности учетных записей пользователей комплекса»).

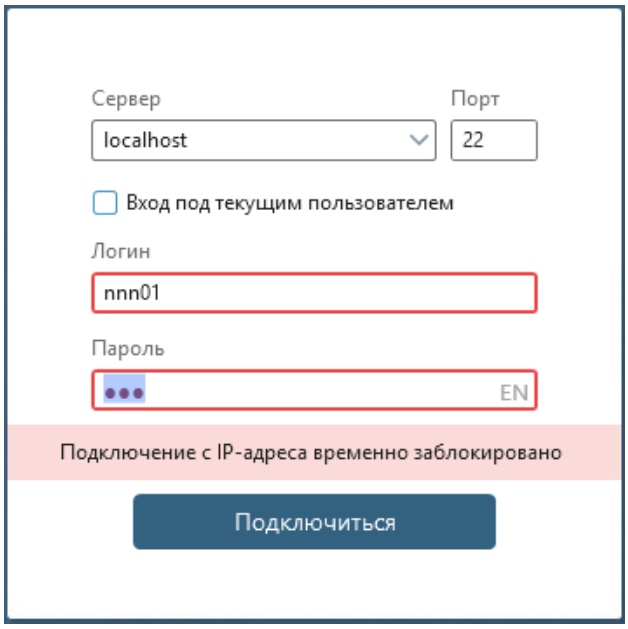


Рисунок 74 – Окно подключения к серверу ПК после превышения количества попыток неверного ввода аутентификационных данных пользователя

При получении сообщения о блокировке учетной записи пользователя (рис. 75) 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 (см. п. 2.4.8 «Настройка параметров безопасности учетных записей пользователей комплекса»).

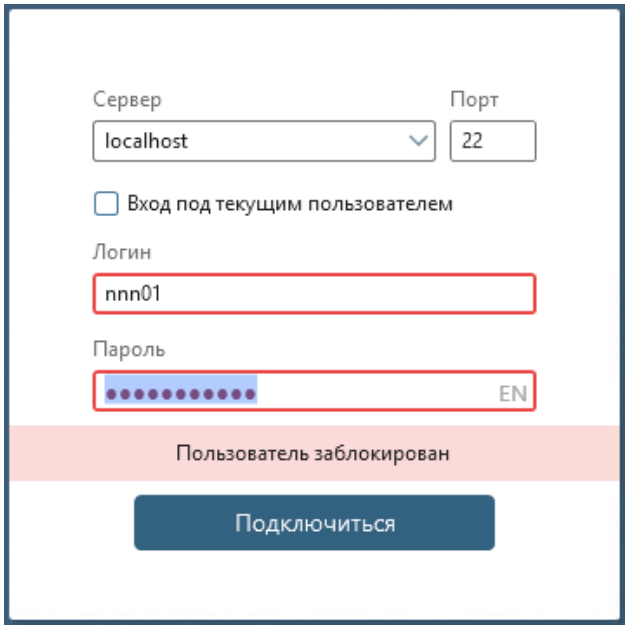


Рисунок 75 – Окно подключения к серверу ПК после ввода аутентификационных данных заблокированного пользователя

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 администрирования комплекса и настройки контроля устройств.

Информационные сообщения, связанные с действиями пользователя по настройке контроля устройств, со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступом и полномочий пользователей, 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, в качестве транспорта используется TCP, при этом все передаваемые данные шифруются
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
ОС	–	операционная система
ПК	–	программный комплекс
СУБД	–	система управления базами данных
ЭВМ	–	электронно-вычислительная машина

Термины и определения

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

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

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

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

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