

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

Руководство администратора

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 безопасной установке и настройке компонентов комплекса, а также действий по обновлению, удалению компонентов комплекса и резервированию данных комплекса.

Настоящее руководство предназначено для системных администраторов ПК «Efros Config Inspector» v.4.

Содержание

1. Общие сведения о программе	5
1.1. Назначение программы	5
1.2. Функции программы	5
1.3. Сведения о технических и программных средствах, обеспечивающих выполнение программы	17
2. Установка и настройка	23
2.1. Установка СУБД	25
2.1.1. Настройка СУБД Microsoft SQL Server для удаленного подключения	25
2.1.2. Настройка СУБД MySQL для удаленного подключения	26
2.2. Установка и настройка серверной части комплекса на ЭВМ под управлением ОС Windows	27
2.2.1. Установка серверной части комплекса	27
2.2.2. Настройка параметров подключения к серверу БД	30
2.2.3. Создание базы данных	31
2.2.4. Подключение к существующей базе данных	35
2.2.5. Настройка параметров службы сервера ПК	38
2.2.6. Настройка сервера ПК в серверной консоли	40
2.3. Установка и настройка серверной части комплекса на ЭВМ под управлением ОС Astra Linux, РЕД ОС	44
2.3.1. Установка серверной части комплекса	44
2.3.2. Настройка сервера ПК в серверной консоли	47
2.3.3. Создание БД комплекса	52
2.3.4. Подключение к существующей базе данных	55
2.4. Установка windows-агента комплекса	56
2.4.1. Установка windows-агента	56
2.4.2. Настройка параметров службы windows-агента	58
2.4.3. Подготовка flash накопителя для контроля Windows с использованием портативного Windows-агента	61
2.5. Установка и настройка коллектора задач	63
2.6. Установка клиентской консоли комплекса	66
3. Обновление компонентов комплекса	70
3.1. Обновление структуры базы данных	70
3.1.1. Обновление структуры базы данных при установке сервера ПК на ЭВМ под управлением ОС серии Windows	70
3.1.2. Обновление структуры базы данных при установке сервера ПК на ЭВМ под управлением ОС Astra Linux, РЕД ОС	70
3.2. Обновление внешних модулей	74
4. Удаление программы	75
5. Настройка регистрации и просмотра событий	76
5.1. Просмотр журнала приложений Windows	76
5.2. Просмотр лог-файлов	76

5.2.1. Просмотр лог-файлов при установке сервера ПК на ЭВМ под управлением ОС серии Windows	76
5.2.2. Просмотр лог-файлов при установке сервера ПК на ЭВМ под управлением ОС Astra Linux, РЕД ОС.....	77
5.3. Просмотр событий в клиентской консоли	77
6. Резервирование данных комплекса	83
6.1. Операции с БД	83
6.1.1. Создание резервной копии БД.....	83
6.1.2. Восстановление БД программного комплекса из резервной копии	85
6.1.3. Миграция БД программного комплекса	88
6.2. Сохранение и восстановление настроек серверной части комплекса	93
6.2.1. Сохранение и восстановление настроек сервера ПК на ЭВМ под управлением ОС серии Windows.....	93
6.2.2. Сохранение и восстановление настроек сервера ПК на ЭВМ под управлением ОС Astra Linux, РЕД ОС.....	94
6.3. Резервирование ключа защиты данных БД комплекса	95
6.3.1. Резервирование ключа защиты данных БД комплекса на ЭВМ под управлением ОС серии Windows.....	95
6.3.2. Резервирование ключа защиты данных БД комплекса на ЭВМ под управлением ОС Astra Linux, РЕД ОС.....	95
6.4. Перенос серверной части комплекса на другой компьютер.....	96
6.5. Настройка резервирования сервера комплекса.....	97
7. Реализация функций безопасности среды функционирования	100
8. Действия после сбоев и ошибок при эксплуатации	101
8.1. Сбой функционирования сетевых служб	101
8.2. Сбой после вмешательства посторонних лиц в ПК «Efros Config Inspector»	101
8.3. Сбой в работе сервера ПК «Efros Config Inspector» v.4	103
8.4. Сбой и ошибки в работе СУБД	105
8.5. Сбой клиентской консоли ПК «Efros Config Inspector» v.4	105
8.5.1. Ошибки идентификации	105
8.5.2. Ошибки управления доступом	107
8.5.3. Ошибки в работе консоли	108
Перечень сокращений	109
Термины и определения	110

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

Полные требования к техническим и программным средствам, обеспечивающим корректное выполнение функций компонентов ПК «Efros Config Inspector» v.4, приведены в подразделе 1.3.

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 иерархии¹.

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.

¹ К консоли одновременно могут быть подключены не более трех серверов ПК, входящих в иерархию.

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:

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

– администрирование комплекса:

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

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

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

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

1.2.5. Коллектор задач 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.

1.2.6. 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.

1.2.7. 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 данных СУБД. СУБД может быть установлена локально на ЭВМ установки сервера ПК, либо на удаленном компьютере (далее – сервере БД) и подключена к серверу ПК по сети.

1.2.8. ПК «Efros Config Inspector» v.4 обеспечивает активный контроль сетевого оборудования, серверных и клиентских ОС, АСУ ТП, виртуальных сред, а также анализ 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 Mera, 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);
- Муха, Inc (EDS, MGate, NPort 5100 Series);
- Huawei Technologies Co., Ltd (Quidway);
- Citrix Systems, Inc (XenServer);
- ОАО «ИнфоТекС» (VipNet Coordinator, VipNet xFirewall, VipNet Prime);
- НЗС Technologies (НЗС);
- 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 (SIMPLICITY, 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.

В таблице 1 приведен перечень оборудования, поддерживаемого серверной частью ПК «Efros Config inspector» v.4, установленной на разные платформы:

- 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 (x64)¹.

¹ ОС серии Windows (x64) в таблице 1 – перечень версий ОС MS Windows, под управлением которых допускается работа серверной части комплекса (64-разрядные ОС) (полный перечень см. в п. 1.3)).

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 серии 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
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
Мoxa (EDS, MGate, NPort 5100 Series)	ДА	ДА	ДА
MS SCVMM (Virtual Machine Manager 2008 R2, 2012 R2, 2016, 2019, SCVMM Group, Hyper-V 2008 (R2 VM, R2 хост, R2 хост с контролем целостности), Hyper-V 2012 (R2 VM, R2 хост, R2 хост с контролем целостности), Hyper-V 2016 (VM, хост, хост с контролем целостности), Hyper-V 2019 (VM, хост, хост с контролем целостности) Standalone Hyper-V (2008 R2, 2012 R2, 2016, 2019))	НЕТ	НЕТ	ДА
Альт Сервер Виртуализации 9.2 в PVE исполнении (PVE версия 6.3)	ДА	ДА	ДА
MS SQL 2000, 2005, 2008, 2012, 2016	ДА	ДА	ДА

Поддерживаемое оборудование	ОС «РЕД ОС»	ОС «Astra Linux SE»	ОС серии Windows (x64)
PostgreSQL	ДА	ДА	ДА
СУБД «Jatoba»	ДА	ДА	ДА
KVM (актуальные версии Linux)	ДА	ДА	ДА
Nateks (NX-3400, NX-5100, NXI-3030, NXI-3050)	ДА	ДА	ДА
КриптоПро TLS шлюз	ДА	ДА	ДА
NSGate NIS	ДА	ДА	ДА
Palo Alto Pan-OS 7, 9	ДА	ДА	ДА
PKCC (OmniAccess 700, OmniSwitch 6850, OmniSwitch 7710, OmniSwitch 7750, OmniSwitch 9000, Onyx)	ДА	ДА	ДА
QTech QSW	ДА	ДА	ДА
Raisecom ISCOM	ДА	ДА	ДА
Rockwell Cisco IOS	ДА	ДА	ДА
TFortis PSW	ДА	ДА	ДА
Azimut Marlin	ДА	ДА	ДА
Siemens Scalance X-300 series, X-400 series, Simatic WinCC	ДА	ДА	ДА
S-Terra VPN Gate	ДА	ДА	ДА
ViPNet Coordinator HW, ViPNet xFirewall, VipNet Prime	ДА	ДА	ДА
TIONIX	ДА	ДА	ДА
Код безопасности Континент	ДА	ДА	ДА
Коммутаторы CS2100 (Бифорком Тек)	ДА	ДА	ДА
VMWare vCenter (vCenter (VCSA, Windows), Standalone ESXi с контролем файлов по HTTPS (SSH), VM (5.0, 5.1, 5.5, 6.0, 6.5, 7), Host, Host с контролем целостности файлов по SSH (HTTPS), Folder, Datacenter, vApp, Resource Pool, ESXi ОС с контролем файлов по HTTPS (SSH), Cluster)	НЕТ	НЕТ	ДА
ESXi ОС с контролем файлов по SSH	ДА	ДА	ДА
СКАЛА-Р 1.91	ДА	ДА	ДА
UiPath Studio, UiPath Orchestrator, UiPath Robot	ДА	ДА	ДА
Primo RPA Orchestrator	ДА	ДА	ДА
UserGate UTM 5, 6, 7	ДА	ДА	ДА
WatchGuard Fireware (OS, XTM OS)	ДА	ДА	ДА
ОС Unix/Linux (AIX, Oracle Oracle SunOS, HP-UX, AltLinux, Red Hat, Debian, Manjaro, Ubuntu, Mint, Fedora, FreeBSD, Red OS, Astra Linux)	ДА	ДА	ДА
ОС Windows (xp, vista, 7, 8, 10, 2000, 2003, 2008r2, 2012, 2012r2, 2016, 2019)	ДА	ДА	ДА
РЕД Виртуализация 7.3.0	ДА	ДА	ДА
СУБД Oracle 10g	ДА	ДА	ДА
СУБД MySQL 5.5.7 и выше	ДА	ДА	ДА
СУБД Firebird	ДА	ДА	ДА
Docker	ДА	ДА	ДА
Citrix XenServer	НЕТ	НЕТ	ДА
Zelax M-1-MEGA, Zelax ZES	ДА	ДА	ДА
ZyXEL ZyNOS	ДА	ДА	ДА

Поддерживаемое оборудование	ОС «РЕД ОС»	ОС «Astra Linux SE»	ОС серии Windows (x64)
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
SIMPLICITY	ДА	ДА	ДА
iFix 3.5	ДА	ДА	ДА
TrainTools	ДА	ДА	ДА
TrainView	ДА	ДА	ДА
Vijeo Citect v 7.40	ДА	ДА	ДА
SCADA АСУД-248	ДА	ДА	ДА
SCADA RTAP A.08.10 (Windows), RTAP A.09.00 (Linux)	ДА	ДА	ДА
Zond2006	ДА	ДА	ДА
Zond2015	ДА	ДА	ДА
Wonderware InTouch (7, 8, 10, 11)	ДА	ДА	ДА
Weidmueller Advanced Line Managed Switches	ДА	ДА	ДА
ПЛК Trei (QNX 6.5)–	ДА	ДА	ДА
ПЛК Ezan (QNX 6.5)	ДА	ДА	ДА

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

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

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

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

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».

1.2.9. 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 серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
Telnet			
SCP, SFTP	Модуль управления устройствами, Модуль взаимодействия с устройствами Континент, Dionis, Docker	Копирование файлов конфигураций и шаблонов проверок безопасности	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
LDAP	Модуль взаимодействия с Active Directory	Active Directory	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
CPMI	Модуль взаимодействия с устройствами CheckPoint	CheckPoint SmartCenter	ОС серии Windows (x64), ОС «Astra Linux SE», ОС «РЕД ОС»
LEA			
Cisco Administrative XML (AXL)	Модуль взаимодействия с сетевыми устройствами Cisco UCM	Cisco UCM	ОС серии Windows (x64)
XenAPI	Модуль взаимодействия с Citrix XenServer	Citrix XenServer	ОС серии Windows (x64)

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

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

Протокол	Где используется	Устройства/Функции	Поддерживаемые ОС
<p>* Используемая в комплексе ПК «Efros Config Inspector» v.4 библиотека libssh поддерживает следующие параметры подключения:</p> <ul style="list-style-type: none"> – 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. Сведения о технических и программных средствах, обеспечивающих выполнение программы

1.3.1 ПК «Efros Config Inspector» v.4 должен устанавливаться на ЭВМ¹ согласно требованиям эксплуатационной документации на комплекс.

1.3.2. Рекомендуемый состав технических средств, который должна иметь ЭВМ, для установки серверной части и внешних модулей ПК «Efros Config Inspector» v.4 рассчитывается на основе данных приведенных в таблицах 4 – 6.

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

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

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

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

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

Таблица 4 – Рекомендуемые требования к производительности ЭВМ установки сервера ПК

Размер контролируемой сети сервером ПК ¹⁾	Аппаратные требования					
	CPU	RAM	ROM ²⁾	Сетевые порты	Рекомендованный объем дискового пространства ³⁾ для хранения данных на срок до	
					90 дней ⁴⁾ , Гбайт	180 дней ⁵⁾ , Гбайт
До 50 ОЗ	От 2 Ghz CPU, Cores: 4	8 GB	SAS 10K и выше	1 порт 100 Мбит/с	Не менее 50	Не менее 100
До 150 ОЗ	от 2 Ghz CPU, Cores: 4	8 GB	SAS 10K и выше	1 порт 100 Мбит/с	Не менее 150	Не менее 300
До 300 ОЗ	от 2 Ghz CPU, Cores: 8	16 GB	SAS 10K и выше	1 порт 100 Мбит/с	Не менее 200	Не менее 400
До 500 ОЗ	от 2 Ghz CPU, Cores: 12	16 GB	SAS 15K и выше	1 порт 1 Гбит/с	Не менее 300	Не менее 600
До 1000 ОЗ	от 2 Ghz CPU, Cores: 16	32 GB	SSD	1 порт 1 Гбит/с	Не менее 600	Не менее 1200
До 2000 ОЗ	от 2 Ghz CPU, Cores: 16	32 GB	SSD	1 порт 1 Гбит/с	Не менее 1200	Не менее 2400
От 2000 ОЗ	Рассчитывается индивидуально. Необходимо обращение в техподдержку.					
<p>1) Для оценки количества объектов защиты (ОЗ) сервера необходимо учитывать непосредственно подключенные ОЗ и ОЗ на подчиненных серверах, если сервер включен в иерархию.</p> <p>При этом ОЗ подчиненных серверов учитываются с коэффициентом 0,35.</p> <p>Итоговое количество ОЗ контролируемой сети определять по формуле:</p> $(n+(0,35\sum(ni))),$ <p>где ni –количество ОЗ на подчинённых серверах; n – количество ОЗ, непосредственно подключенных к серверу</p>						
<p>2) Для повышения отказоустойчивости функционирования решения в составе аппаратной платформы рекомендуется выделить системный раздел, рекомендуемый объем системного раздела не менее 240 Гбайт</p>						
<p>3) Для снижения вероятности потери данных рекомендуется организация RAID-массива в конфигурации RAID1 + 1 диск Hot Spare. Возможно применение RAID-массивов, обладающих более высокой степенью надежности, в соответствии с условиями применения решения и/или требованиями заказчика</p>						
<p>4) Объем дискового пространства рекомендован для хранения данных (события, промежуточные версии конфигураций ОЗ) не менее 90 дней при указанной емкости контролируемой сети. При необходимости хранения больше чем 90 дней, рекомендуется использовать регулярную выгрузку на сторонние носители или рассчитывать объем хранилища по формуле ниже в примечании</p>						
<p>5) Объем дискового пространства рекомендован для хранения данных (события, промежуточные версии конфигураций ОЗ) не менее 180 дней при указанной емкости контролируемой сети. При необходимости хранения больше чем 180 дней, рекомендуется</p>						

Размер контролируемой сети сервером ПК ¹⁾	Аппаратные требования					
	CPU	RAM	ROM ²⁾	Сетевые порты	Рекомендованный объем дискового пространства ³⁾ для хранения данных на срок до	
					90 дней ⁴⁾ , Гбайт	180 дней ⁵⁾ , Гбайт
использовать регулярную выгрузку на сторонние носители или рассчитывать объем хранилища по формуле ниже в примечании						

Таблица 5 – Средние показатели параметров загрузки отчетов по типам устройств

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

Таблица 6 – Средние значения коэффициента производительности сервера ПК

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

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

$$k \cdot \sum(t_i \cdot n_i), \quad (1)$$

где t_i – среднее время загрузки отчетов с контролируемого типа устройств (берется из таблицы 5);

n_i – количество контролируемых на сервере ПК устройств одного типа;

k – коэффициент производительности сервера ПК (берется из таблицы 6).

Свободное дисковое пространство, которое должна иметь ЭВМ для установки только серверной части и внешних модулей, составляет 10 Гб. При установке серверной части и СУБД на одну ЭВМ минимальный объем свободного дискового пространства рассчитывается на основе данных, приведенных в таблице 5, и заданного при настройке параметров работы комплекса периода очистки БД.

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

$$(\sum V_n \cdot n) \cdot T \cdot 24, \quad (2)$$

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

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

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

– ОС специального назначения «Astra Linux Special Edition» v.1.6 (релиз «Смоленск»), v.1.7, сертификат соответствия № 2557 (выдан ФСТЭК России 27.01.2012 г.);

– ОС «РЕД ОС» Муром v.7.2, v.7.3, сертификат соответствия № 4060 (выдан ФСТЭК России 12.01.2019 г.);

– ОС серии Windows 64-разрядные (далее - ОС Windows (x64)):

- Windows Server 2008R2 Foundation Edition SP1;
- Windows Server 2008R2 Standard Edition SP1;
- Windows Server 2008R2 Enterprise Edition SP1;
- Windows Server 2008R2 Datacenter Edition SP1;
- Windows Server 2012/2012R2 Foundation;
- Windows Server 2012/2012R2 Essentials;
- Windows Server 2012/2012R2 Standard;
- Windows Server 2012/2012R2 Datacenter;
- Windows Server 2016 Standard;
- Windows Server 2016 Datacenter;
- Windows Server 2016 Essentials;
- Windows Server 2019 Standard;
- Windows Server 2019 Datacenter;
- Windows Server 2019 Essentials;
- Windows Server 2022 Standard;
- Windows Server 2022 Datacenter;
- Windows Server 2022 Essentials;
- Windows 7 Professional SP1;
- Windows 7 Enterprise SP1;
- Windows 7 Ultimate SP1;
- Windows 8.1 Core;
- Windows 8.1 Professional;
- Windows 8.1 Enterprise;
- Windows 10 Home;
- Windows 10 Pro;
- Windows 10 Enterprise;
- Windows 11 Home;
- Windows 11 Pro;
- Windows 11 Enterprise.

1.3.4. Дополнительно на ЭВМ с серверной частью ПК «Efros Config Inspector» v.4 под управлением ОС серии Windows (x64) должны быть установлены следующие программные средства:

- .NET Framework версии 4.7;
- СУБД (одна из, также поддерживаются новые версии указанных СУБД):
 - PostgreSQL: 11, 12, 13, 14, 15;

- Microsoft SQL Server: 2016, 2017, 2019;
- MySQL: 8.0;
- защищенная СУБД «Jatoba» (сертификат соответствия № 4327 от 19.11.2020, выдан ФСТЭК России);
- SQL Server Native Client – при использовании СУБД MS SQL Server 2017, установленной на отдельном сервере БД;
- ПО Java (JRE) версия 1.8.0.

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

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

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

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

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

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

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

- .NET Framework 4.7.

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

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

Минимальные требования к производительности рабочей станции:

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

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

2. Установка и настройка

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

Перед установкой компонентов ПК «Efros Config Inspector» v.4 нужно удостовериться в наличии установленного на всех используемых ЭВМ комплекса необходимого общесистемного ПО (см. п. 1.3 настоящего Руководства), а также проверить выполнение требований к настройке используемой СУБД (см. п. 2.1 настоящего Руководства).

Установка общесистемного ПО и компонентов ПК «Efros Config Inspector» v.4 на ЭВМ должна производиться пользователем с административными правами (входящим в группу Администраторы (Administrators) ОС).

Установка ПК «Efros Config Inspector» v.4 производится с DVD-диска или другого носителя и заключается в установке перечисленных выше компонентов комплекса.

Далее приведено описание успешного и безопасного сценария установки компонентов комплекса. В случае возникновения проблем установку следует прервать, а после их устранения, в зависимости от причин, – продолжить или начать заново.

На дистрибутивном носителе данных ПК «Efros Config Inspector» v.4 (установочный компакт-диск или другой носитель «ПК «Efros Config Inspector» v.4») записан комплект компонентов ПК для установки на ЭВМ в соответствии с таблицей 7.

Таблица 7 – Комплект файлов компонентов на дистрибутивном носителе данных ПК «Efros Config Inspector» v.4

Компонент комплекса	Инсталяционный файл, архив, каталог файлов	Описание
Windows-агент	<i>Efros Config Inspector Agent 4.msi</i>	Windows-агент для платформы под управлением ОС серии Windows x64 (аналогично серверной части)
	<i>Efros Config Inspector Agent 4.Remote_Install.msi</i>	Windows-агент для платформы под управлением ОС серии Windows x64 (аналогично серверной части) для удаленной установки на АРМ. Примечание – На удаленном АРМ требуется наличие установленных библиотек Microsoft Visual C++ (VC_redist.x64)
	<i>Efros Config Inspector Portable Agent 4. x86.zip</i>	Портативный Windows-агент для платформы под управлением ОС серии Windows x86: Windows Server 2008 R2 SP1; Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, Windows 7 SP1, Windows 8, Windows 10
	<i>Efros Config Inspector Portable Agent 4. Windows 2000, 2003, 2008, XP, Vista, 7.zip</i>	Портативный Windows-агент для платформы под управлением устаревших ОС серии Windows x86:

Компонент комплекса	Инсталяционный файл, архив, каталог файлов	Описание
		Windows Server 2000/2000 R2, Windows Server 2003/2003 R2, Windows Server 2008/2008R2, Windows XP, Windows Vista, Windows 7. Примечание – Для подключения используется модуль Windows Agent 2000
Клиентская консоль	<i>Efos Config Inspector Console 4.msi</i>	Для платформы под управлением ОС серии Windows x86
	<i>Efos Config Inspector Console 4.x64.msi</i>	Для платформы под управлением ОС серии Windows x64
Серверная часть	<i>Efos Config Inspector Server 4.msi</i>	Для платформы под управлением ОС серии Windows x64
	<i>Efrosci_4.X.XXX.X-X_amd64.deb¹</i>	Для платформы под управлением ОС «Astra Linux SE»
	<i>Efrosci_4.X.XXX.X-X_MUROM.x86_64.rpm</i>	Для платформы под управлением ОС «РЕД ОС»
Коллектор задач	<i>Efos Config Inspector Collector 4.msi</i>	Для платформы под управлением ОС серии Windows x64
Внешние модули	Каталог <i>Modules</i>	Содержит zip-архивы с файлами внешних модулей, предназначенных для работы с контролируемым оборудованием
Справка	Архив <i>Описание модулей.zip</i>	Содержит файл-справку <i>Описание модулей.chm</i> с описанием работы внешних модулей программного комплекса

Настройку ПК «Efos Config Inspector» v.4 после установки выполняют в окне настройки серверной части (серверной консоли) и в клиентской консоли.

В серверной консоли в соответствии с настоящим Руководством настраиваются:

- параметры подключения к БД;
- параметр удаленного доступа к серверу ПК (порт для подключения клиентских консолей к серверу ПК);
- параметры запуска Java-приложений на сервере ПК;
- параметры обработки ошибок серверной части комплекса;
- параметры аудита работы администраторов комплекса в серверной консоли.

В клиентской консоли в соответствии с документом «643.72410666.00082-01 96 01-01 «Программный комплекс управления конфигурациями и анализа защищенности «Efos Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование» настраиваются:

- лицензии на использование комплекса;
- внешние модули (подключение, отключение и настройка);
- параметры хранения данных в БД комплекса;
- список пользователей комплекса.

¹ 4.X.XXX.X-X – номер версии ПК «Efos Config Inspector» v.4

При установке серверной части ПК «Efros Config Inspector» v.4 на ЭВМ под управлением ОС Windows встроенные в ПК «Efros Config Inspector» v.4 внешние модули устанавливаются автоматически, при установке серверной части комплекса на ЭВМ под управлением ОС «Astra Linux SE», ОС «РЕД ОС» необходимо выполнить добавление внешних модулей устройств, используя средства клиентской консоли (см. документ «643.72410666.00082-01 96 01-01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование»). Дополнительные внешние модули в обоих случаях устанавливаются отдельно администратором комплекса с использованием дистрибутивов соответствующих модулей.

ВНИМАНИЕ: Для корректной работы некоторых внешних модулей ПК «Efros Config Inspector» v.4 должны быть обязательно установлены пакеты из состава стандартных дистрибутивов ОС:

- 1) Для модуля CheckPoint при установке на ЭВМ под управлением::
 - ОС «Astra Linux SE» обязательна установка пакетов: *ia32-libs*, *libc6-i386*;
 - ОС «РЕД ОС» обязательна установка пакетов: *libstdc++.i686*, *pat.i686*.
- 2) Для модуля MS SQL при установке на ЭВМ под управлением::
 - ОС «Astra Linux SE» обязательна установка пакета *tdsodbc*;
 - ОС «РЕД ОС» обязательна установка пакета *freetds*.
- 3) Для модуля Oracle при установке на ЭВМ под управлением::
 - ОС «Astra Linux SE» обязательна установка пакета *libaio1*;
 - ОС «РЕД ОС» обязательна установка пакета *libaio*.
- 4) Для модуля Sending messages via MS Exchange при установке на ЭВМ под управлением:
 - ОС «Astra Linux SE» обязательна установка пакета *gss-ntlmssp*;
 - ОС «РЕД ОС» обязательна установка пакета *gssntlmssp*.

2.1. Установка СУБД

ПК «Efros Config Inspector» v.4 поддерживает работу с различными СУБД.

Установка и настройка СУБД выполняются в соответствии с эксплуатационной документацией из комплекта поставки используемой версии СУБД.

Особенности настройки СУБД Microsoft SQL Server для удаленного подключения приведены в п. 2.1.1, СУБД MySQL – в п. 2.1.2.

2.1.1. Настройка СУБД Microsoft SQL Server для удаленного подключения

Соединение между сервером ПК «Efros Config Inspector» v.4 и СУБД MS SQL Server возможно по протоколам TCP или Named Pipes, причем способ подключения выбирается в зависимости от настроек СУБД (см. таблицу 8). Для подключения к СУБД достаточно использования одного из протоколов.

Подключение по протоколу Named Pipes рекомендуется использовать только в том случае, если сервер ПК «Efros Config Inspector» v.4 и СУБД MS SQL установлены на одной ЭВМ.

Таблица 8 – Параметры сетевого соединения сервера ПК и СУБД MS SQL

Протокол	Порты	Примечание
TCP\IP	1433 (TCP), 1434 (UDP)	Порты подключения к СУБД и к службе MS SQL Server
Named Pipes	445 (over TCP)	Именованный канал передачи данных

Если сервер ПК и сервер БД установлены на разных ЭВМ, на ЭВМ установки сервера ПК должна быть установлена соответствующая версия SQL Server Native Client (утилита **sqlncli.msi** входит в комплект поставки СУБД или может быть получена у компании-производителя Microsoft). Например, версии СУБД MS SQL 2012 соответствует SQL Server Native Client версии 11.0.

В менеджере настроек СУБД (**Sql Server Configuration Manager**) необходимо разрешить использование протокола именованных каналов (**Named Pipes**) или **TCP/IP**.

Для корректной работы программного комплекса с СУБД MS SQL Server на сервере БД должна быть запущена служба SQL Server Browser.

Для подключения к СУБД должен использоваться пользователь MS SQL Server. Для возможности создания БД комплекса пользователь, учетная запись которого указывается в утилите настройки сервера ПК «Efros Config Inspector» v.4 СУБД (см. раздел 2.2.1 «Настройка параметров подключения к серверу БД» настоящего Руководства), должна быть присвоена роль **dbcreator**.

После создания БД, для корректной работы сервера ПК «Efros Config Inspector» v.4 пользователю, от имени которого происходит подключение к СУБД, достаточно привилегий **public** и разрешения на доступ к ресурсам.

В процессе взаимодействия сервера ПК «Efros Config Inspector» v.4 с БД учетная запись, от имени которой производится подключение к серверу БД, должна являться владельцем данной БД (**SQL Server... → Databases → efroscli_4 → Security → Users → dbo**).

2.1.2. Настройка СУБД MySQL для удаленного подключения

Соединение между сервером ПК «Efros Config Inspector» v.4 и СУБД MySQL возможно по протоколу TCP (см. таблицу 9). В менеджере настроек СУБД подключение по умолчанию настраивается на порт 3306 (TCP).

Таблица 9 – Параметры сетевого соединения сервера ПК и СУБД MySQL

Протокол	Порты	Примечание
TCP	3306	Порт подключения к СУБД

При подключении к удаленной СУБД MySQL для обеспечения корректной работы необходимо, чтобы значение переменной **max_allowed_packet** MySQL сервера было не менее 512 Мб.

Учетная запись, которая указывается в утилите настройки сервера ПК «Efros Config Inspector» v.4, для создания БД должна обладать правами **Server Privileges-Granted: Create, Select, Insert, Delete, Drop, Index**.

Для возможности обновления существующей структуры БД ПК «Efros Config Inspector» v.4 также требуются права **Update**.

После создания БД, пользователю, от имени которого осуществляется подключение к СУБД, достаточно привилегий **Select, Insert, Delete, Index, Update**.

2.2. Установка и настройка серверной части комплекса на ЭВМ под управлением ОС Windows

2.2.1. Установка серверной части комплекса

Для установки серверной части ПК «Efros Config Inspector» v.4 на ЭВМ под управлением ОС Windows следует запустить с используемого носителя установочного комплекта ПК «Efros Config Inspector» v.4 на исполнение файл *Efros Config Inspector Server 4.msi*.

Откроется окно мастера установки серверной части комплекса (рис. 1), в котором для продолжения необходимо выбрать папку для установки серверной части комплекса или оставить заданную по умолчанию (*C:\Program Files\EFROS Config Inspector 4*) и нажать кнопку **Далее**.

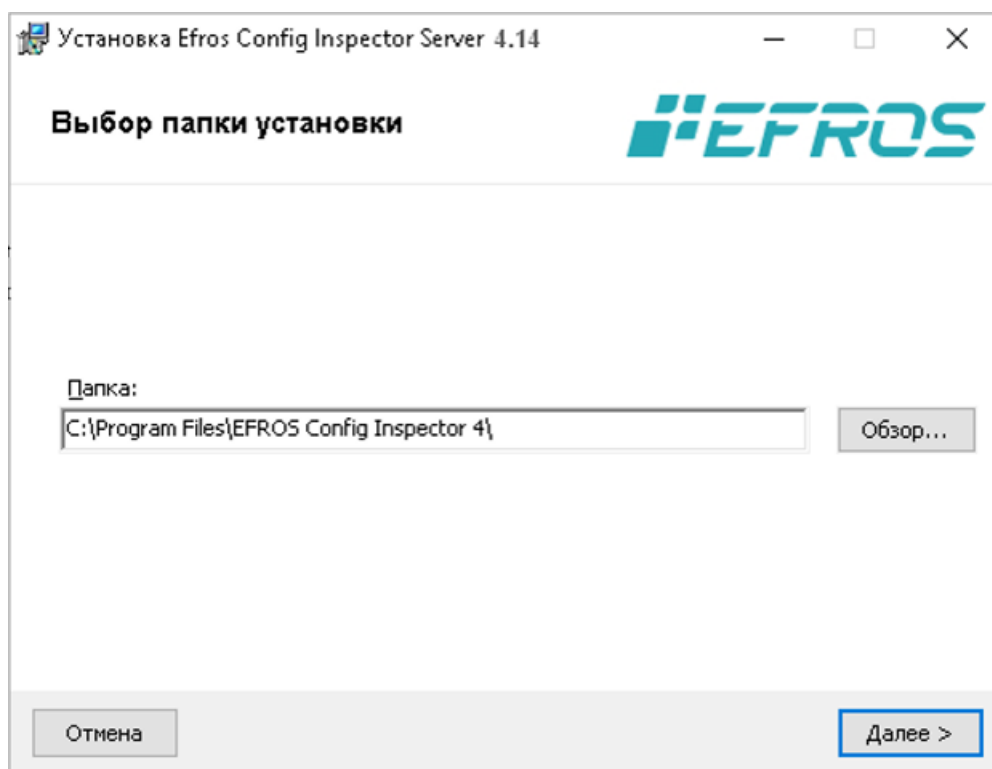


Рисунок 1 – Окно выбора каталога установки серверной части комплекса

На следующем шаге работы мастера установки следует выбрать модули для копирования (рис 2):

1) Внешние модули:

- **Сетевые устройства** – модули поддержки сетевых устройств различных производителей;
- **Операционные системы** – модули поддержки операционных систем;
- **Виртуализация** – модули поддержки гипервизоров и средств виртуализации;
- **Сервисные модули** – модули отправки писем и уведомлений во внешние системы;
- **Прикладное программное обеспечение** – модули поддержки прикладного программного обеспечения (СУБД, SCADA, Uipath).

2) Компонент Microsoft Visual C++ 2015-2019.

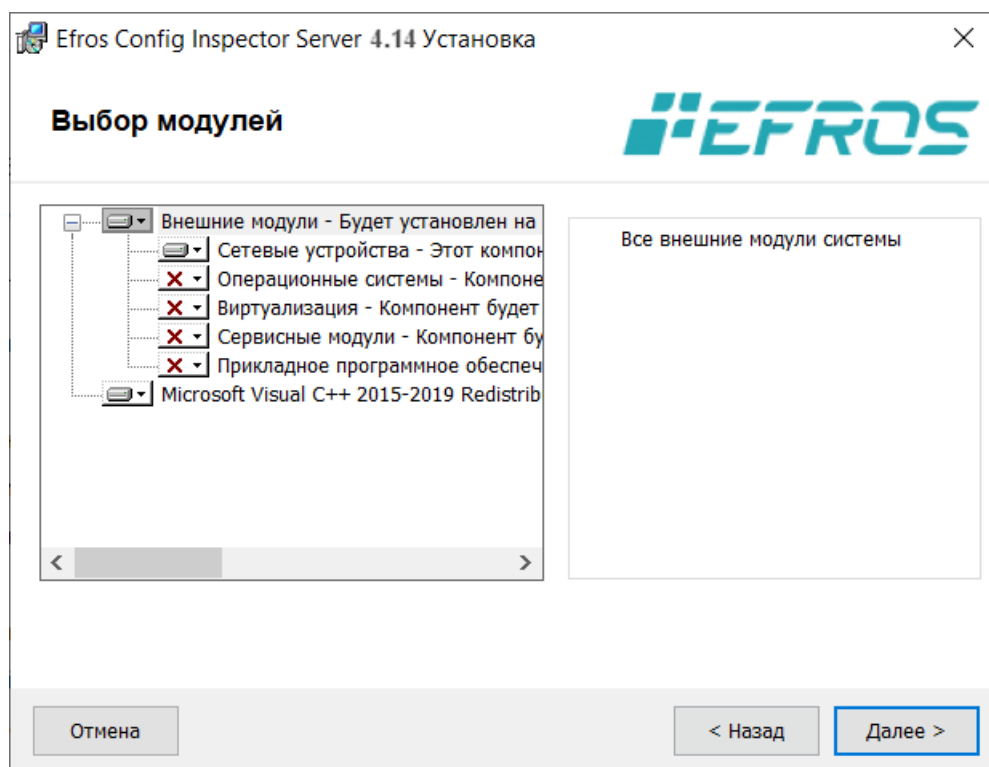


Рисунок 2 – Окно выбора модулей

Примечание – Список модулей можно увидеть, перейдя на вкладку **Модули** раздела **Настройки** клиентской консоли комплекса сразу после завершения установки серверной части комплекса и клиентской консоли.

Для продолжения установки следует нажать кнопку **Далее**.

В появившемся диалоговом окне начала установки для запуска процесса установки с заданными ранее параметрами следует нажать кнопку **Установить** (рис. 3).

Ход процесса установки серверной части комплекса будет отображаться в окне мастера установки (рис. 4).

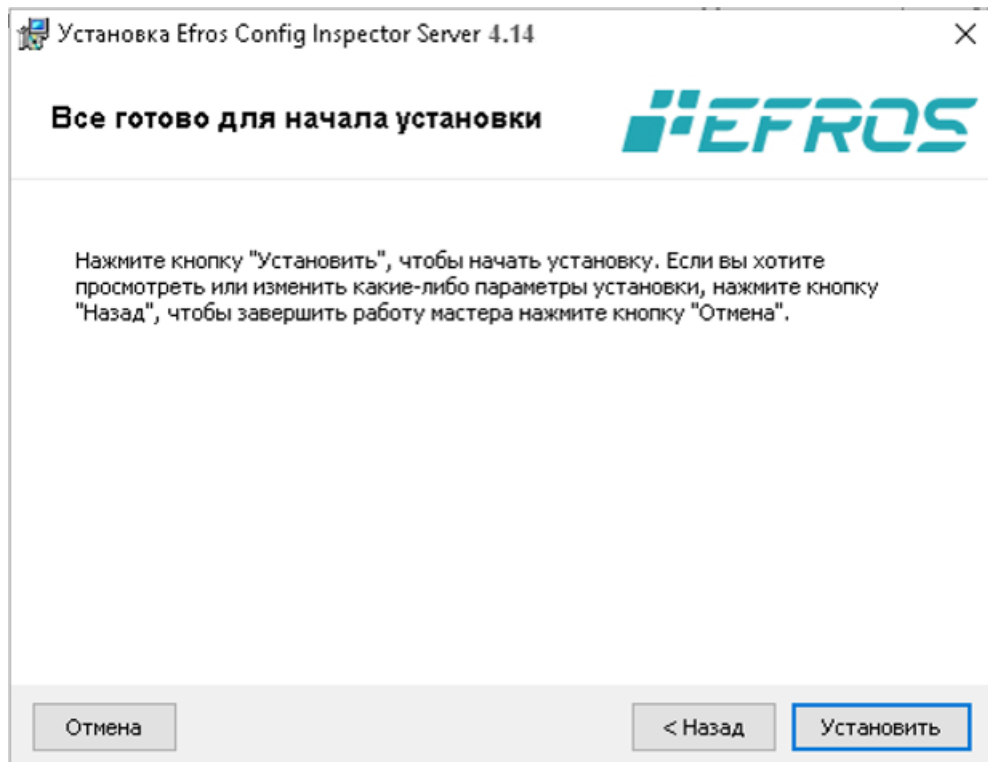


Рисунок 3 – Окно начала установки

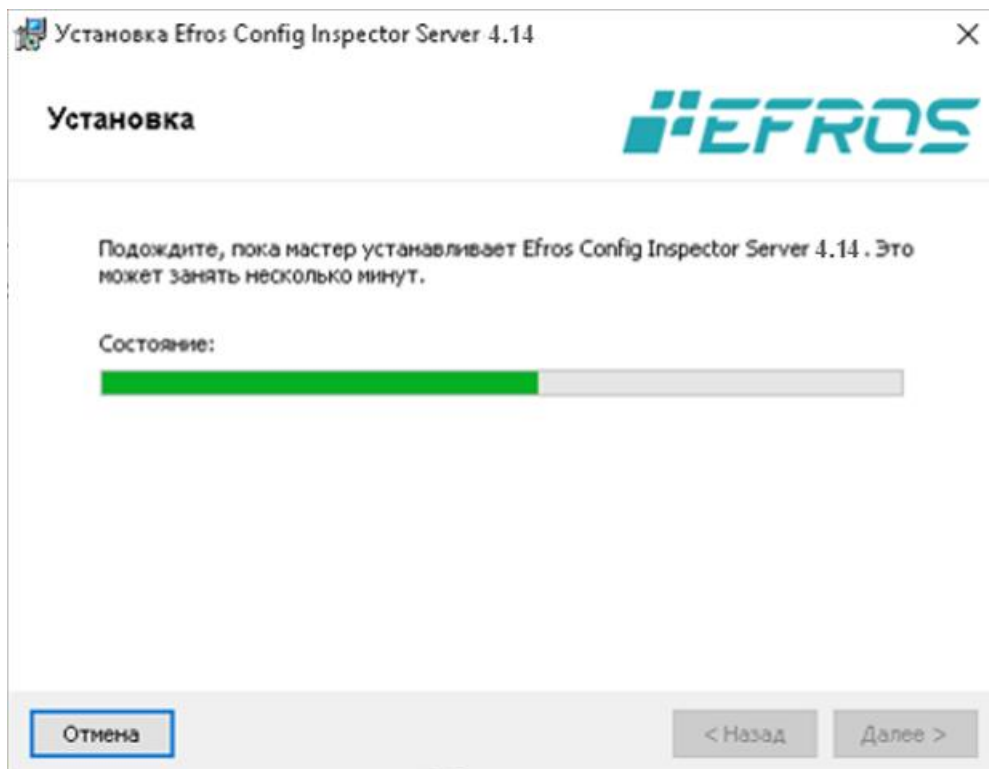


Рисунок 4 – Окно процесса установки серверной части комплекса

После завершения установки серверной части комплекса откроется диалоговое окно завершения работы мастера установки (рис. 5).

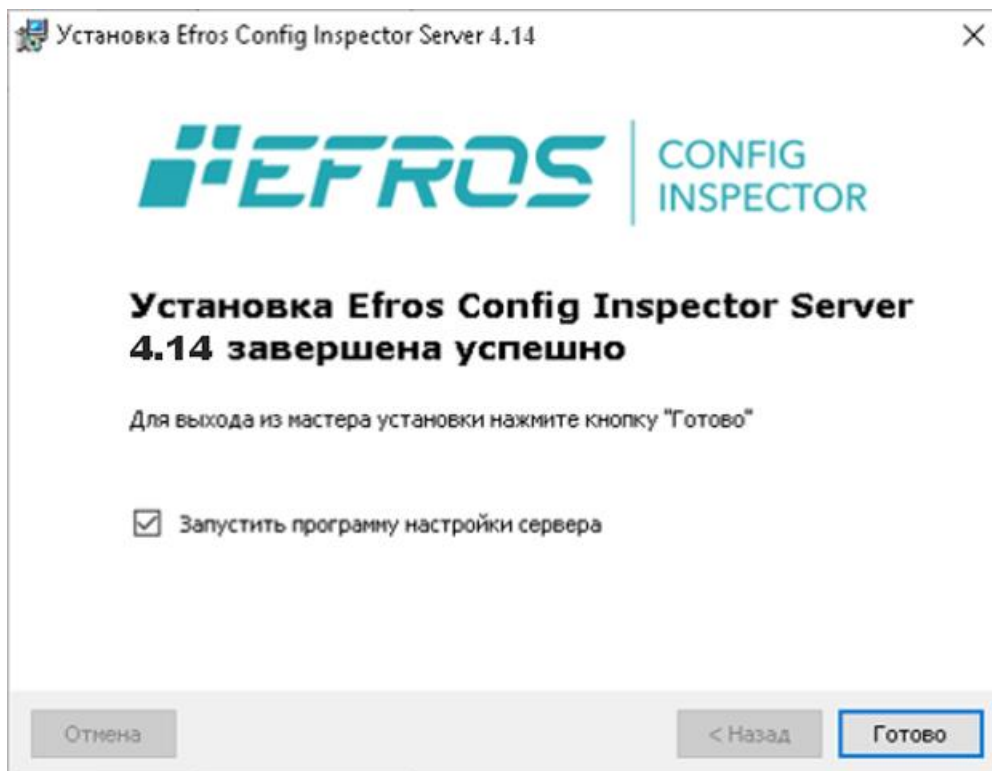


Рисунок 5 – Окно завершения работы мастера установки

Возможны два варианта завершения установки серверной части комплекса:

- без настройки сервера ПК – снять отметку с параметра **Запустить программу настройки сервера** в окне завершения работы мастера установки (см. рис. 5) и нажать кнопку **Готово**. Окно завершения работы мастера установки закроется. Служба сервера ПК (*EFROS CI Service 4*) не будет запущена. Настройку сервера ПК необходимо будет выполнить позднее из серверной консоли (см. п. 2.2.6 «Настройка сервера ПК в серверной консоли» настоящего Руководства);
- с настройкой сервера ПК – оставить отметку параметра **Запустить программу настройки сервера** и нажать кнопку **Готово**. В результате откроется окно мастера настройки параметров подключения сервера ПК к серверу БД и настройки службы сервера ПК. Описание работы мастера настройки сервера ПК приведено в п.п. 2.2.2 – 2.2.5 настоящего Руководства.

2.2.2. Настройка параметров подключения к серверу БД

На первом этапе работы мастера настройки сервера ПК «Efros Config Inspector» v.4 откроется окно настройки параметров подключения серверной части комплекса к серверу БД (рис. 6), в котором доступны для выбора два возможных способа использования БД:

- создать новую БД;
- подключиться к уже существующей БД.

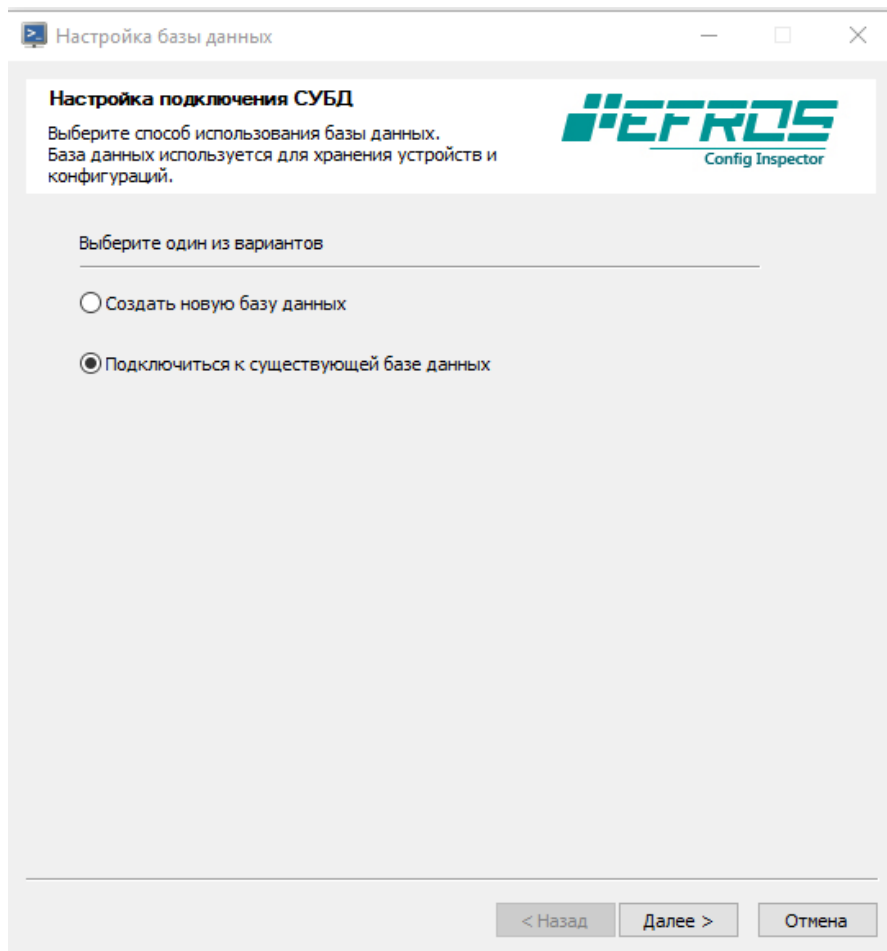


Рисунок 6 – Окно настройки параметров подключения к серверу БД

На любом этапе работы мастера настройки параметров сервера ПК можно нажать кнопку **Отмена** – работа мастера настройки будет прекращена и служба ПК (*EFROS CI Service 4*) не будет запущена. Служба запустится только после создания подключения сервера ПК к серверу БД. Дальнейшую настройку параметров можно будет осуществить через серверную консоль. Подробнее настройка соединения сервера ПК «Efros Config Inspector» v.4 с сервером БД описана в настоящем Руководстве (см. п. 2.2.6).

2.2.3. Создание базы данных

Перед созданием БД, если используется СУБД MySQL, необходимо внести следующие изменения в конфигурацию сервера MySQL:

- в директории установки СУБД MySQL открыть файл *my.ini*;
- в блоке [mysqld] добавить параметр *max_allowed_packet=512M*;
- перезапустить службу MySQL.

Для создания новой БД программного комплекса необходимо в окне настройки подключения СУБД (см. рис. 6) выбрать пункт **Создать новую базу данных** и нажать кнопку **Далее**. В результате откроется окно создания БД (рис. 7).

В окне создания БД комплекса необходимо заполнить поля в соответствии с таблицей 10.

Настройка подключения СУБД

Выберите способ использования базы данных. База данных используется для хранения устройств и конфигураций.

Выберите БД _____

Тип БД: PostgreSQL

Адрес: localhost

Имя БД: efrosci_4

Включить защиту данных (алгоритм AES-256)

Для создания базы данных введите пользователя с правами superuser:

Логин: admin

Пароль: ●●●●●●●●

Использовать данного пользователя для подключения к базе данных

< Назад Далее > Отмена

Рисунок 7 – Окно ввода параметров создания БД

Таблица 10 – Перечень полей окна **Настройка базы данных**

Поле	Описание/Назначение
Тип БД	Из раскрывающегося списка выбирается тип подключаемой СУБД MySQL, PostgreSQL/Jatoba, Microsoft SQL Server
Адрес	Указывается IP-адрес или имя используемого сервера БД. При размещении СУБД и сервера ПК на одной ЭВМ в поле Адрес можно оставить значение по умолчанию <i>localhost</i> . При подключении к СУБД Postgre и MySQL в поле после адреса через символ «:» может быть указан порт подключения. При использовании СУБД Microsoft SQL Server Express в поле Адрес необходимо ввести имя экземпляра сервера БД в формате <i>Имя_сервераИмя_экземпляра_БД</i> (например, <i>localhost\SQLEXPRESS</i>). Точное имя сервера и экземпляра сервера БД MS SQL Server можно увидеть в окне подключения к серверу БД (MS SQL Server Management Studio). По умолчанию экземпляр сервера БД MS SQL Server 2008/2012 Express имеет имя <i>SQLEXPRESS</i>
Имя БД	Имя создаваемой БД комплекса. По умолчанию используется имя БД <i>efrosci_4</i>
Логин, Пароль	Соответственно, имя и пароль пользователя СУБД, обладающего

Поле	Описание/Назначение
	правами создания и редактирования БД (например, для СУБД MySQL можно указать имя и пароль встроенного администратора root , для СУБД PostgreSQL – postgres). При использовании СУБД MS SQL Server должна использоваться учетная запись локального пользователя SQL Server. При этом пользователю, от имени которого происходит создание БД, должна быть присвоена роль dbcreator
Использовать данного пользователя для подключения к базе данных	Переключатель устанавливается, если введенные при создании новой БД имя и пароль пользователя СУБД в дальнейшем будут использоваться для подключения сервера ПК к БД
Включить защиту данных (алгоритм AES-256)	Переключатель устанавливается, если требуется защита хранящихся в БД комплекса отчетов с конфигурациями контролируемого оборудования. Защита данных выполняется по алгоритму AES-256, ключ защиты данных хранится в реестре сервера ПК и привязан к конфигурации сервера

После заполнения всех полей в окне **Создание базы данных** для запуска операции создания БД комплекса на сервере БД следует нажать кнопку **Далее**. В случае ввода некорректных параметров подключения к серверу БД откроется окно с сообщением об ошибке. Для продолжения настройки необходимо исправить некорректные данные и повторить шаги по созданию БД комплекса.

В зависимости от состояния параметра **Включить защиту данных (алгоритм AES-256)** работа мастера настройки параметров сервера ПК будет отличаться:

- а) Параметр **Включить защиту данных (алгоритм AES-256)** отмечен:
 - откроется окно с предупреждением о включении механизма защиты данных используемой БД комплекса, в котором следует нажать кнопку **Да/Yes** (рис. 8). При нажатии кнопки **Нет/No** операция создания БД будет отменена, откроется окно с соответствующим сообщением, в котором необходимо нажать кнопку **ОК**;
 - в открывшемся информационном окне с сообщением об успешном создании БД и предложением экспортировать созданный ключ защиты данных для резервирования (рис. 9) следует нажать кнопку **Да/Yes** для запуска процедуры экспорта ключа защиты данных БД комплекса.

Примечание – В случае отказа от операции экспорта ключа защиты данных (нажата кнопка **Нет/No** в информационном окне с сообщением об успешном создании БД) работа мастера настройки параметров сервера ПК продолжится без открытия окна экспорта ключа защиты данных БД комплекса.

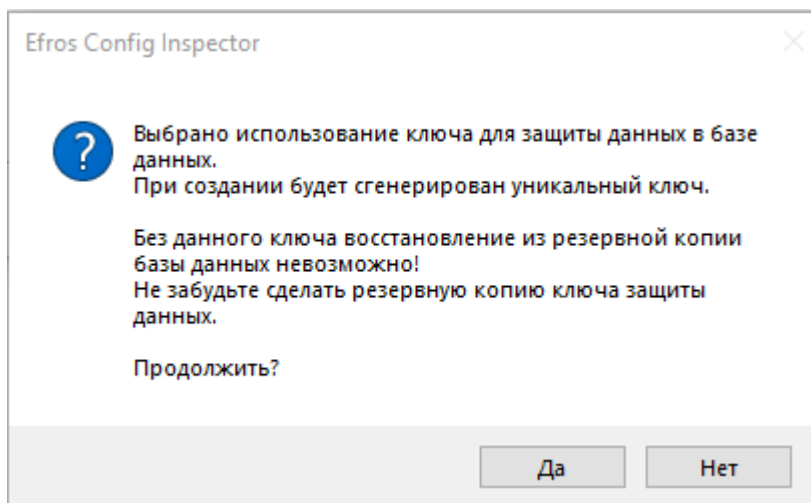


Рисунок 8 – Предупреждение о включении механизма защиты БД комплекса

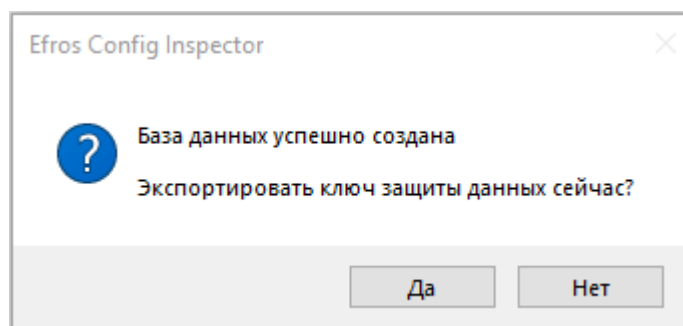


Рисунок 9 – Запрос на запуск операции экспорта ключа защиты данных БД комплекса

- в открывшемся окне **Экспорт ключа защиты данных** (рис. 10) необходимо в соответствующие поля ввести пароль администратора программного комплекса (при инсталляции серверной части комплекса создается учетная запись администратора комплекса **root**, которой присваивается пароль **root**), пароль, с использованием которого будет модифицирован экспортируемый ключ защиты данных БД комплекса, и нажать кнопку **ОК**;
 - для резервирования ключа защиты данных БД комплекса необходимо сохранить его, нажав кнопку **Сохранить ключ**, при этом откроется диалоговое окно выбора каталога для сохранения ключа. В дальнейшем этот ключ может понадобиться при восстановлении работоспособности программного комплекса, связанной, например, с переносом серверной части комплекса на другую платформу.
- б) Параметр **Включить защиту данных (алгоритм AES-256)** не отмечен:
- если в окне создания БД нажата кнопка **Далее**, БД комплекса на сервере БД будет создана без появления дополнительных окон – произойдет переход к окну **Настройка подключения СУБД** с результатами проверки корректности соединения сервера ПК с указанной БД (см. п. 2.2.4 настоящего Руководства).

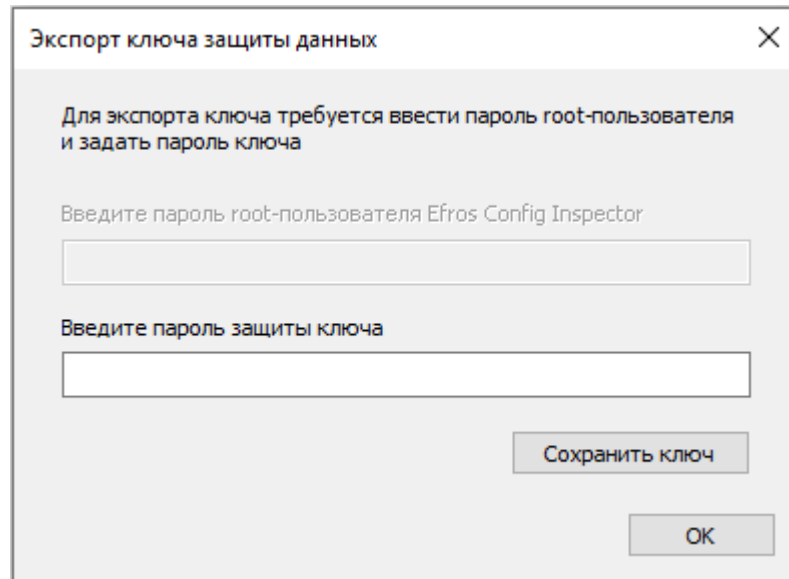


Рисунок 10 – Окно экспорта ключа защиты данных БД комплекса

После успешной проверки подключения сервера ПК к серверу БД нажать в открывшемся окне кнопку **Next**. Откроется окно настройки параметров службы сервера, в котором, при необходимости, можно изменить номер используемого TCP-порта для внешних подключений к серверу ПК, путь к каталогу размещения программного обеспечения Java (JRE) и настроить параметры аудита работы компонентов серверной части комплекса (см. п. 2.2.5 настоящего Руководства). Для обеспечения безопасной работы комплекса рекомендуется изменить пароль встроенного администратора (**root**) средствами клиентской консоли.

2.2.4. Подключение к существующей базе данных

При выборе на первом шаге работы мастера настройки сервера ПК пункта **Подключиться к уже существующей базе данных** окно мастера настройки сервера ПК примет вид в соответствии с рисунком 11. Также это окно открывается и после этапа создания новой БД комплекса. В окне **Настройка базы данных** доступны для заполнения следующие поля (подробное описание этих полей приведено в п. 2.2.3 настоящего Руководства):

- **Тип БД** – тип используемой СУБД.
- **Адрес** – IP-адрес или имя используемого сервера БД.
- **Имя БД** – имя существующей на сервере БД комплекса.
- **Логин и Пароль** – имя и пароль пользователя СУБД, от имени которого будет происходить подключение к серверу БД.

В окне **Настройка базы данных** также будут выведены результаты проверки корректности соединения сервера ПК с указанной БД. В случае успешной проверки выводится сообщение «*Проверка базы данных выполнена успешно*» (см. рис. 11).

В случае ввода некорректных параметров подключения сервера ПК к серверу БД будет выведено сообщение об ошибке. Следует исправить неверно введенные данные и заново проверить возможность подключения сервера ПК к БД, нажав кнопку **Далее**.

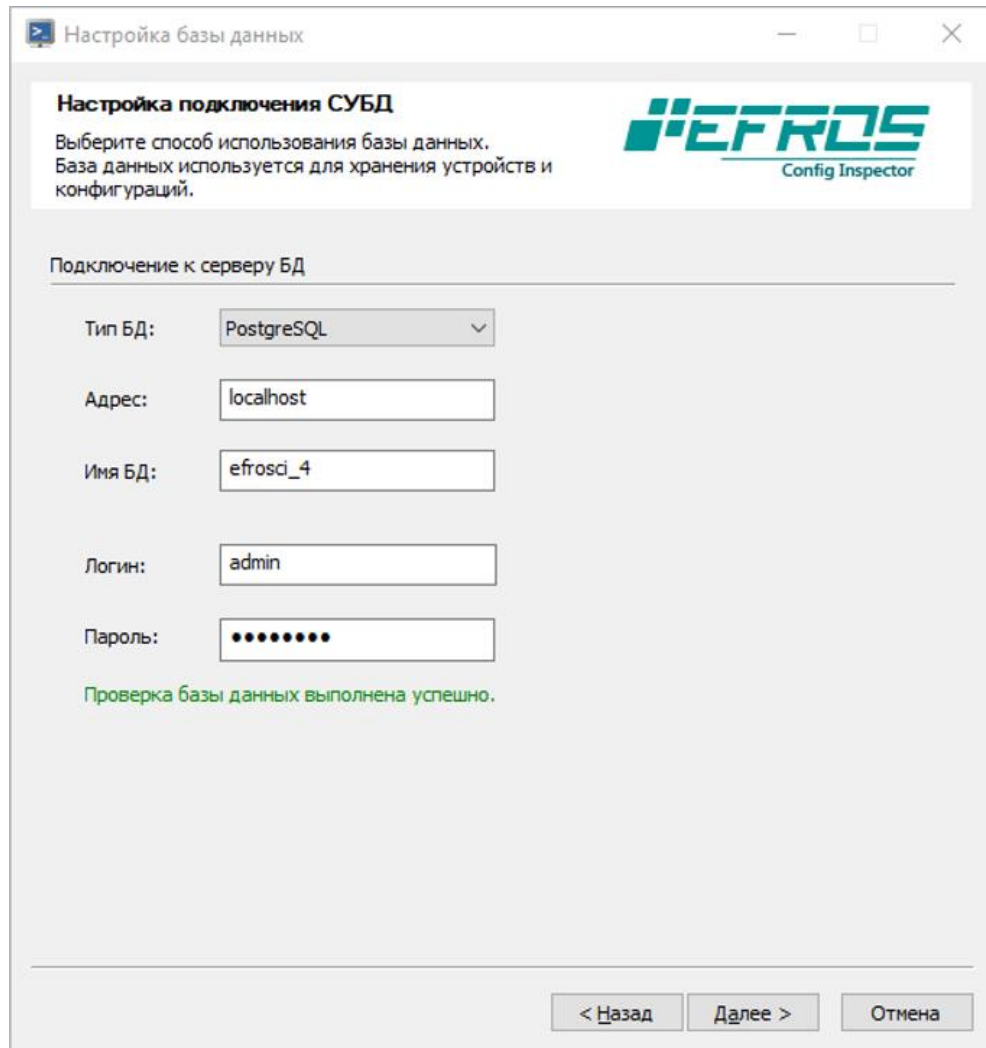


Рисунок 11 – Задание параметров подключения к БД

При наличии в БД, к которой осуществляется подключение, более 500 000 записей журнала событий на экран будет выведено предложение (рис. 12) о выборе режима обновления БД.

Для продолжения выполнения подключения выбрать приемлемые настройки обновления записей, учитывая, что время подключения к существующей БД будет зависеть от количества переносимых записей журнала событий, и нажать кнопку **ОК**.

В случае ввода корректных параметров подключения сервера ПК к защищенной БД откроется окно ввода ключа защиты данных БД (рис. 13), в котором необходимо в соответствующие поля ввести пароль, с использованием которого был защищен ключ и значение ключа защиты данных. После ввода всех необходимых данных следует нажать кнопку **ОК**.

В случае ввода неверных значений пароля и/или ключа защиты данных кнопка **ОК** будет неактивна, а в окне ввода ключа защиты данных отобразится соответствующее сообщение. В случае отмены операции (по нажатию кнопки **Cancel**) откроется окно с сообщением «Ключ задан неверно», в мастере настройки отобразится сообщение «Ошибка проверки ключа базы данных».

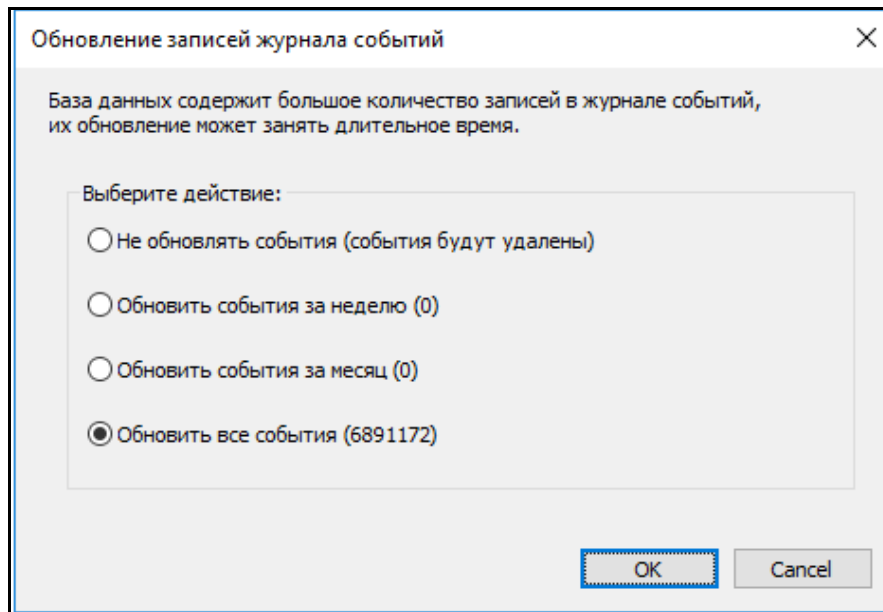


Рисунок 12 – Задание параметров действия по обновлению событий при подключении к БД

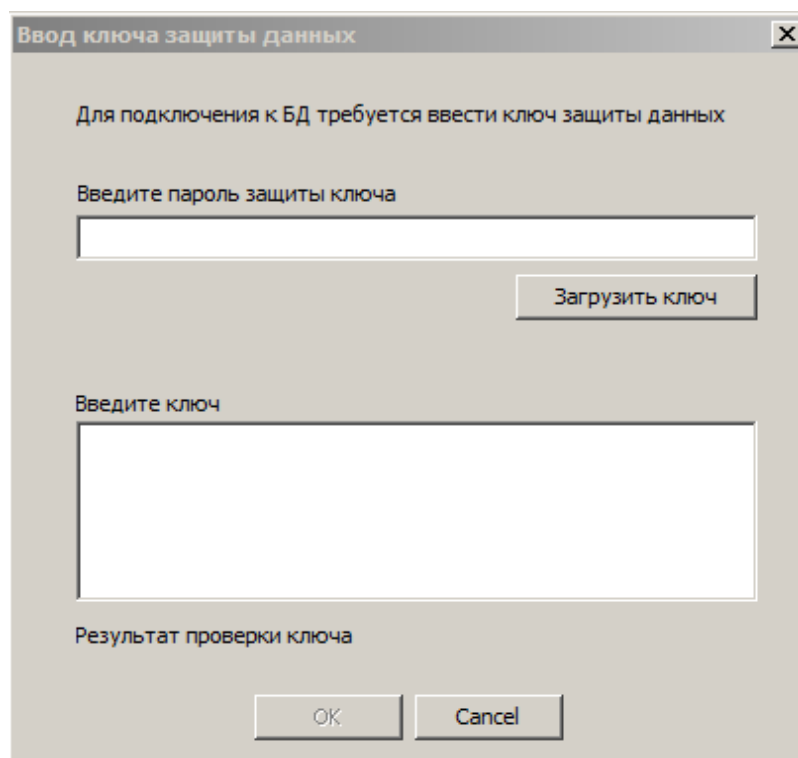


Рисунок 13 – Окно ввода ключа защиты данных БД комплекса

При успешной проверке соединения сервера ПК с защищенной БД откроется окно с сообщением «*Проверка базы данных выполнена успешно*», после нажатия в котором кнопки **OK** откроется окно **Задание параметров подключения к БД** с соответствующим сообщением (см. пример на рис. 11).

Для продолжения работы мастера настройки сервера ПК – нажать кнопку **Далее/Next** в окне **Настройка базы данных**.

2.2.5. Настройка параметров службы сервера ПК

После успешной проверки подключения сервера ПК к серверу БД откроется окно настройки параметров службы сервера (рис. 14), в котором при необходимости можно изменить номер используемого TCP-порта для внешних подключений к серверу ПК, путь к каталогу размещения программного обеспечения Java (JRE), используемый язык сервера (*русский, английский*), настроить параметры аудита работы компонентов серверной части комплекса.

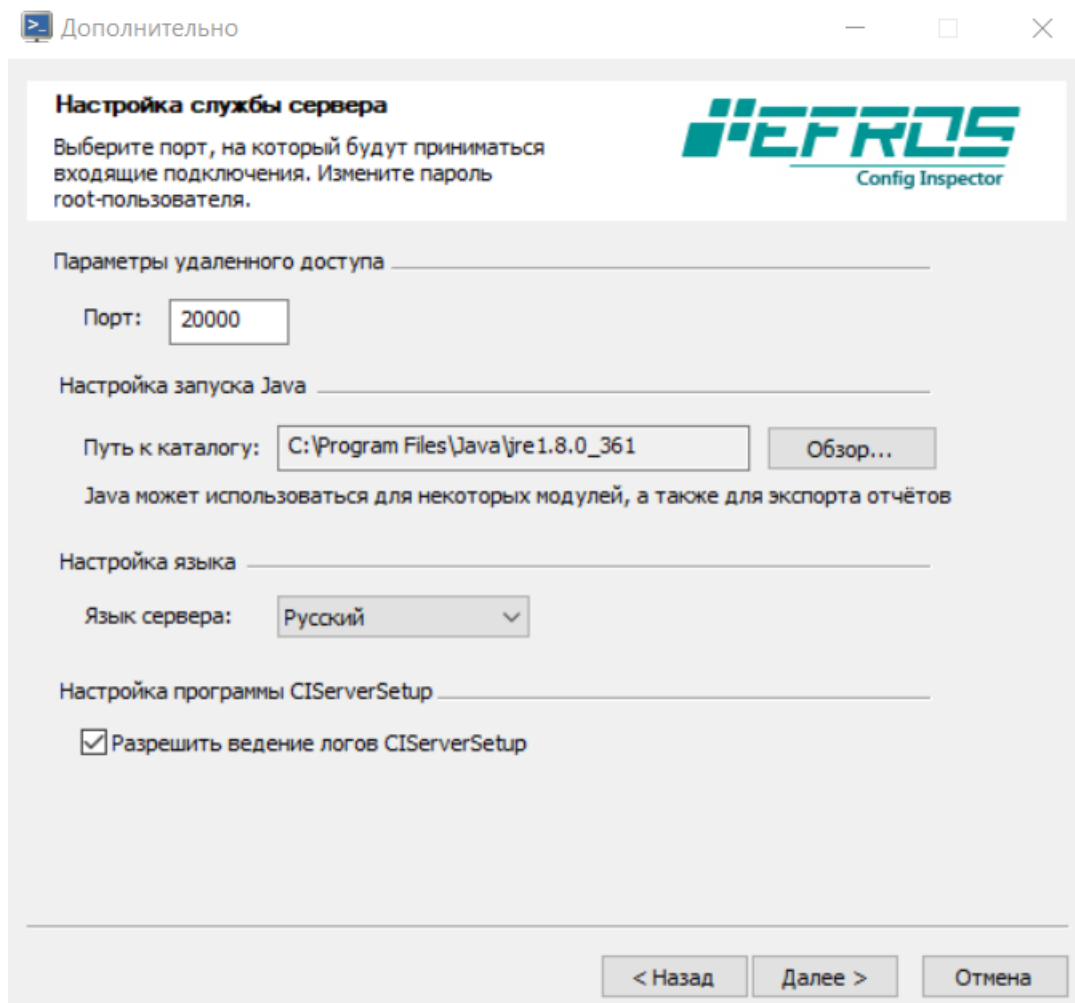


Рисунок 14 – Окно настройки службы сервера

В поле **Порт** указывается номер TCP-порта, по которому будет происходить соединение клиентских консолей комплекса с сервером. По умолчанию в серверной части и клиентской консоли установлено значение TCP-порта 20000. В случае изменения номера порта, используемого серверной частью комплекса, также необходимо изменить номер используемого порта в настройках клиентской консоли. Подробнее настройка параметров клиентской консоли программного комплекса описана в документе 643.72410666.00082-01 96 01-01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование».

В области **Настройка запуска Java** мастер настройки сервера ПК автоматически введет в поле **Путь к каталогу** полный путь к каталогу размещения программного

обеспечения Java (JRE), если это программное обеспечение установлено на сервере ПК. В дальнейшем, при необходимости, изменить путь к каталогу с установленным ПО Java можно из серверной консоли (подробнее о настройке серверной части ПК см. п. 2.2.6 «Настройка сервера ПК в серверной консоли» настоящего Руководства).

Установка параметра **Разрешить ведение логов CIServerSetup** включает возможность регистрации действий администратора комплекса по настройке комплекса из серверной консоли.

Для продолжения работы мастера настройки параметров сервера ПК нажать в окне настройки службы сервера (см. рис. 14) кнопку **Далее**. Откроется окно запуска службы ПК (рис. 15), в котором перечислены установленные параметры сервера ПК.

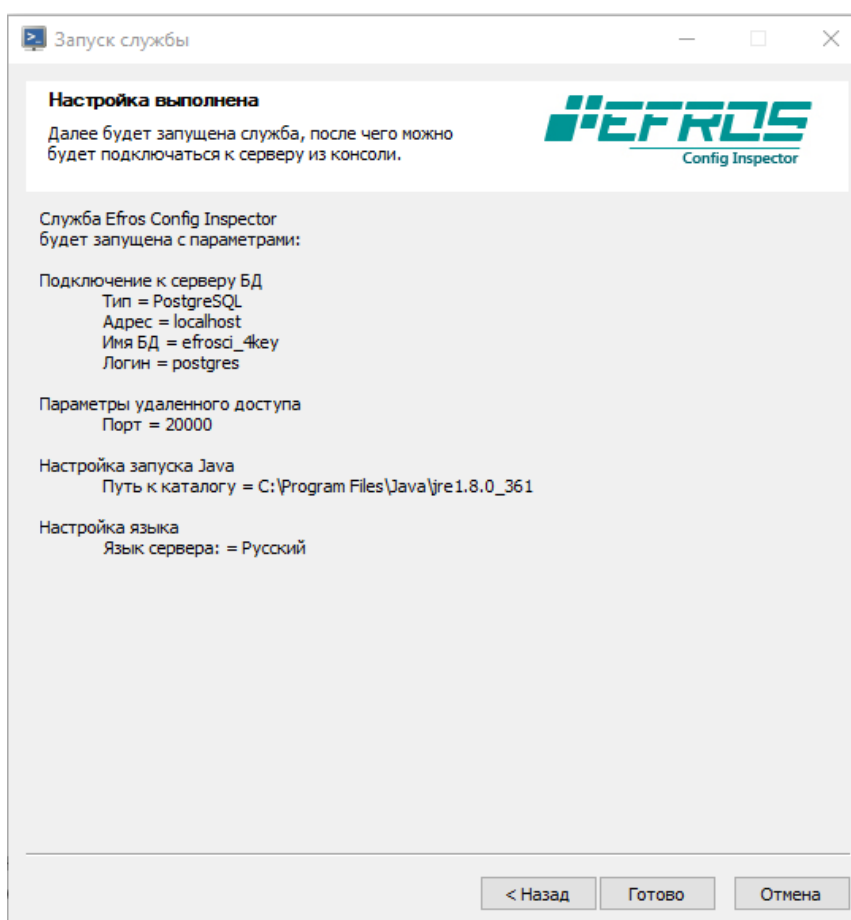


Рисунок 15 – Окно запуска службы ПК

Для окончания работы мастера настройки сервера ПК нажать кнопку **Готово**, после чего появится сообщение об успешном запуске службы (рис. 16).

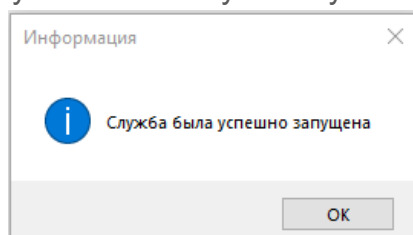


Рисунок 16 – Сообщение об успешном запуске службы

Запуск серверной консоли осуществляется из меню **Пуск** на панели задач (рис. 17). Для этого следует выбрать **Все программы**→**Efros Config Inspector 4** →**CIServerSetup**:

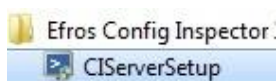


Рисунок 17 – Вызов серверной консоли комплекса из меню **Пуск**

2.2.6. Настройка сервера ПК в серверной консоли

Если была снята отметка с параметра **Запустить программу настройки сервера** в окне завершения работы мастера установки, то служба сервера ПК (**EFROS CI Service 4**) не будет запущена. Окно завершения работы мастера установки закрывается. Открытие окна настройки серверной части комплекса (рис. 18) производится на сервере с помощью меню **Пуск** на панели задач. Для этого следует выбрать **Все программы** →**Efros Config Inspector4** → **CIServerSetup**.

Данное окно имеет три вкладки: **Службы**, **База данных** и **Дополнительно**.

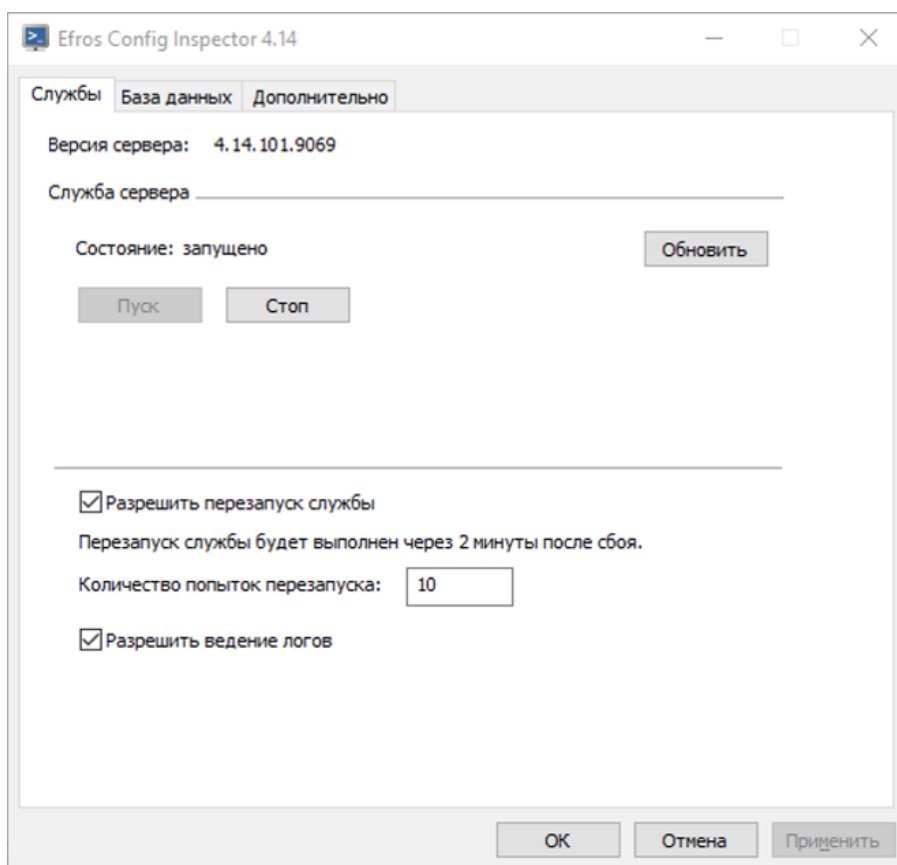


Рисунок 18 – Серверная консоль, вкладка **Службы**

2.2.6.1. Вкладка Службы

Вкладка **Службы** (см. рис. 18) предназначена для управления работой и задания некоторых параметров службы сервера ПК.

Назначение основных элементов управления вкладки:

- кнопка **Обновить** – для обновления строки состояния службы в окне серверной консоли;

- кнопки **Пуск**, **Стоп** – для запуска и остановки службы серверной части программного комплекса соответственно;
- переключатель **Разрешить перезапуск службы** – для автоматического перезапуска службы сервера ПК, если возникнут какие-либо сбои в ее работе, при установленном переключателе;
- поле ввода **Количество попыток перезапуска** – для задания количества попыток перезапуска службы сервера ПК для случаев неудачных попыток запуска;
- переключатель **Разрешить ведение логов** – для сохранения логов работы службы сервера ПК в папке %ProgramData%\EFROS Config Inspector v.4\Server\Loggs.

2.2.6.2. Вкладка База данных

Вкладка **База данных** (рис. 19) предназначена для настройки подключения сервера ПК «Efros Config Inspector» v.4 к серверу БД. Перечень параметров для настройки приведен в таблице 11.

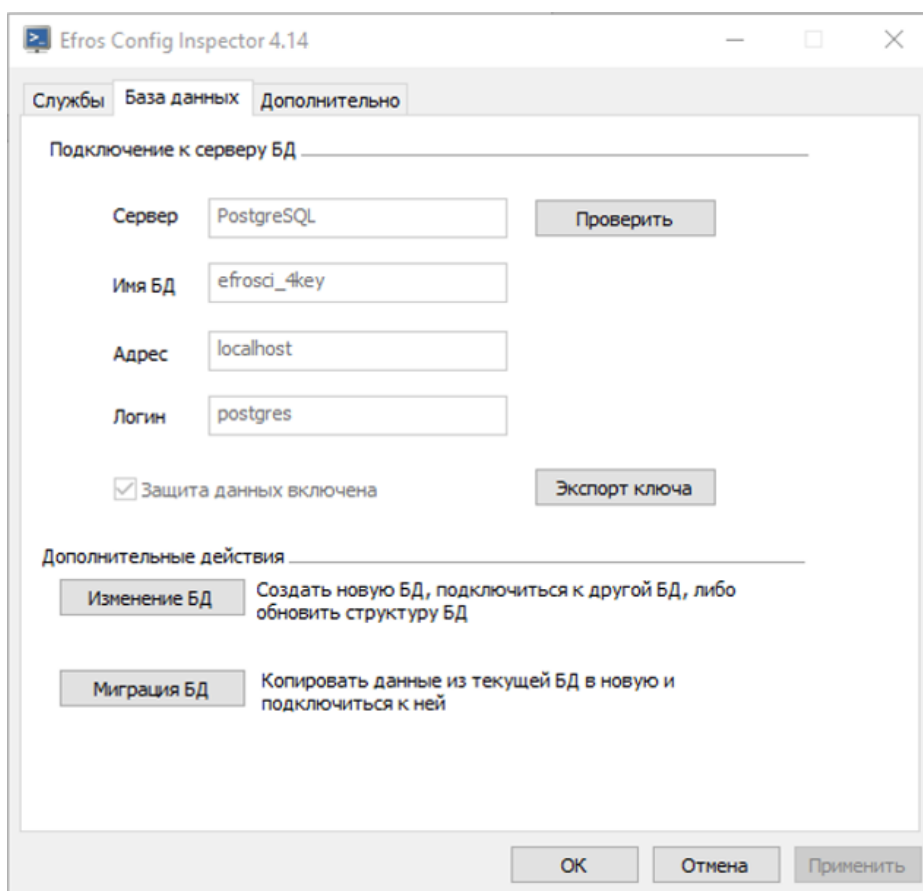


Рисунок 19 – Серверная консоль, вкладка **База данных**

Таблица 11 – Перечень параметров подключения сервера ПК к серверу БД

Параметр	Описание/Назначение
Сервер	Тип СУБД, установленной на сервере БД. MySQL, PostgreSQL, Microsoft SQL Server
Имя БД	Имя БД программного комплекса
Адрес	IP-адрес (или доменное имя) сервера БД

Параметр	Описание/Назначение
Логин	Имя пользователя для подключения к серверу БД
Защита данных включена	Параметр использования механизма защиты данных БД комплекса

Кнопка **Проверить** предназначена для проверки наличия и версии БД программного комплекса на сервере БД. При нажатии кнопки:

- устанавливается соединение с указанным сервером БД;
- на сервере БД проверяется наличие БД комплекса;
- проверяется версия используемой БД;
- проверяется совпадение ключа защиты данных;
- в зависимости от результатов проверки выводится соответствующее сообщение.

Кнопка **Экспорт ключа** позволяет выполнить резервирование ключа защиты данных БД комплекса, который может понадобиться при переносе серверной части комплекса на другую платформу. Подробнее о процедуре резервирования ключа защиты данных БД комплекса см. п. 6.3 «Резервирование ключа защиты данных БД комплекса» настоящего Руководства.

Кнопка **Изменение БД** предназначена для изменения параметров подключения сервера ПК к серверу БД, в котором доступны следующие операции:

- создать новую БД;
- изменить настройки подключения к существующей БД;
- обновить версию БД (в случае, если БД на сервере уже существует).

Кнопка **Миграция БД** предназначена для копирования существующей БД программного комплекса на другой сервер БД в любую СУБД, из списка поддерживаемых комплексом (либо в иную СУБД, используемую на текущем сервере). Подробнее процесс копирования используемой БД средствами консоли серверной части комплекса описан в пункте 6.1.3 «Миграция БД программного комплекса» настоящего Руководства.

После нажатия кнопки **Изменение БД** откроется окно настройки подключения к БД (рис. 20), в котором есть два варианта: **Создать новую базу данных** или **Подключиться к существующей базе данных**.

Процедуры создания новой БД и подключения к существующей БД подробно описаны, соответственно, в пунктах 2.2.3 «Создание базы данных» и 2.2.4 «Подключение к существующей базе данных» настоящего Руководства.

Изменение настроек подключения сервера ПК к серверу БД вступит в силу после перезагрузки службы сервера ПК. Перезагрузка службы будет выполнена автоматически при подтверждении этого в соответствующем информационном окне.

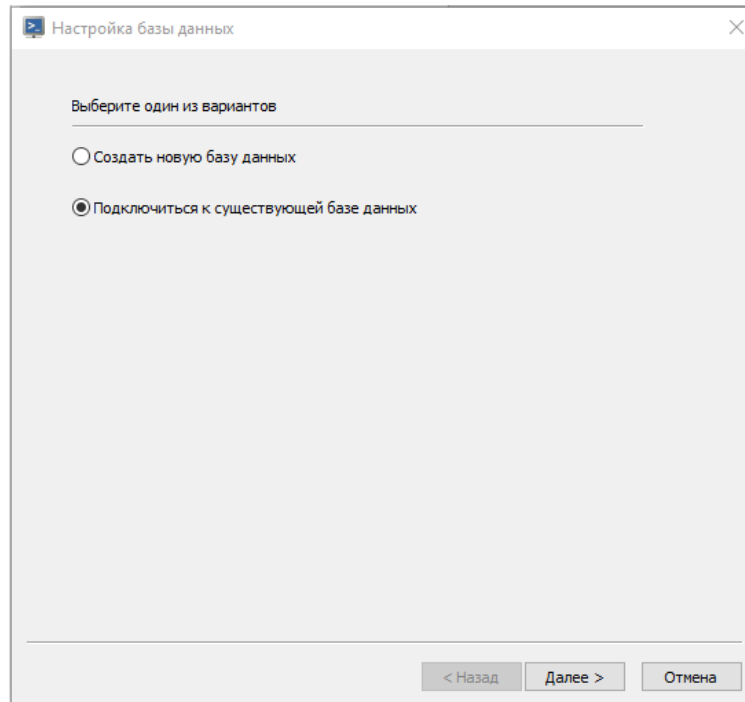


Рисунок 20 – Выбор варианта настройки соединения комплекса с БД

2.2.6.3. Вкладка Дополнительно

Вкладка **Дополнительно** (рис. 21) предназначена для изменения настроек удаленного доступа к серверу ПК, параметров запуска Java-приложений и параметров аудита работы серверной части комплекса. Перечень параметров приведен в таблице 12.

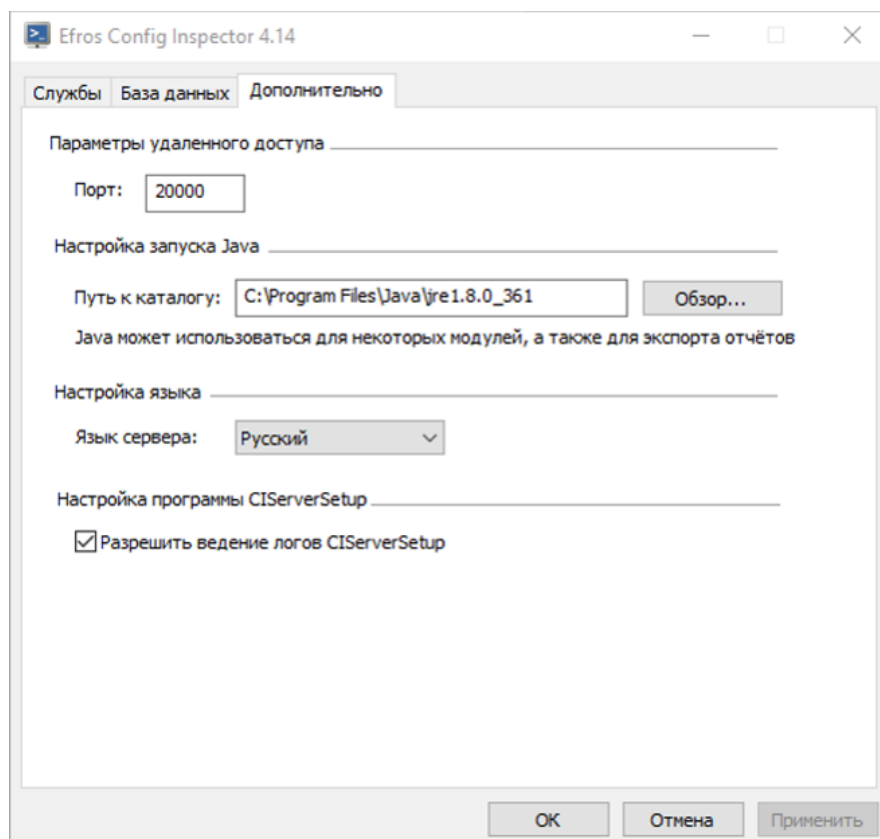


Рисунок 21 – Серверная консоль, вкладка **Дополнительно**

Таблица 12 – Перечень настраиваемых параметров сервера ПК

Параметр	Описание/Назначение
Параметры удаленного доступа	
Поле <i>Порт</i>	Номер TCP-порта для подключения клиентских консолей к серверу ПК
Настройка запуска Java	
Поле <i>Путь к каталогу</i>	Путь к каталогу размещения ПО Java. Путь можно ввести вручную или воспользоваться кнопкой Обзор
Настройка языка	
<i>Язык сервера</i>	Выбор языка из выпадающего списка (русский, английский)
Настройка программы CIServerSetup	
Переключатель <i>Разрешить ведение логов CIServerSetup</i>	Включение (отключение) возможности регистрации действий администратора комплекса по настройке комплекса из серверной консоли

2.3. Установка и настройка серверной части комплекса на ЭВМ под управлением ОС «Astra Linux SE», ОС «РЕД ОС»

2.3.1. Установка серверной части комплекса

Установку и настройку ПК «Efros Config Inspector» v.4 на сервере под управлением ОС «Astra Linux SE» осуществляется при помощи терминала *Fly* вызываемого из меню **Пуск** (**Пуск** → **Системные** → **Терминал Fly**) либо нажатием комбинации клавиш **ALT+T**. Пример открытия терминала *Fly* при помощи меню **Пуск** представлен на рисунке 22.

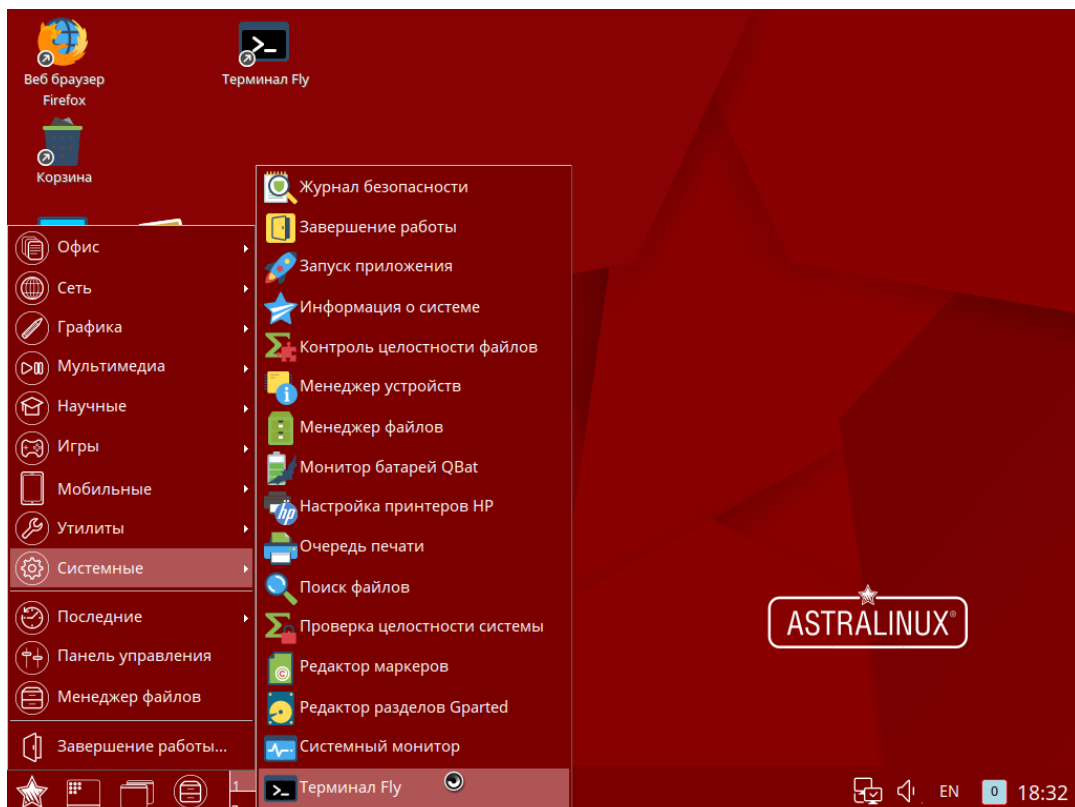


Рисунок 22 – Открытие Терминала Fly

При установке комплекса на сервер под управлением ОС «РЕД ОС» используется терминал GNOME, запуск терминала осуществляется из меню **Пуск (Пуск → Системные → Терминал)** как показано на рисунке 23.

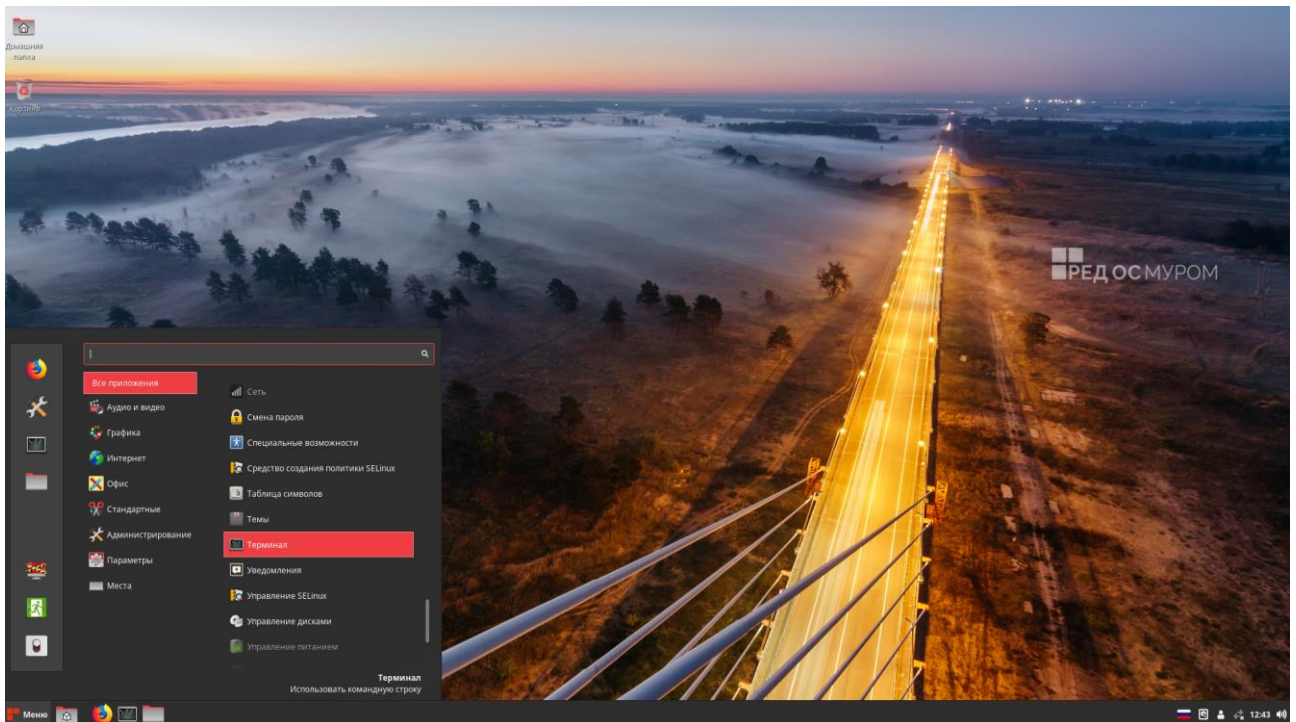


Рисунок 23 – Открытие Терминала GNOME

Для установки серверной части ПК «Efros Config Inspector» v.4 администратору необходимо выполнить следующие действия:

1) На ЭВМ установки сервера ПК, в окне ввода пароля, ввести верный логин и пароль пользователя с привилегиями локального администратора системы, проконтролировать уровень конфиденциальности и уровень целостности, нажать кнопку **ДА**.

2) Открыть *терминал* и выполнить действия:

– для сервера ПК на ЭВМ под управлением ОС «Astra Linux SE»:

а) установить системный пакет *curl* из состава дистрибутива ОС «Astra Linux SE» командой:

```
“sudo apt-get install curl”
```

б) выполнить установку пакета серверной части комплекса командой:

```
“sudo dpkg -i путь_до_файла/efroscli_4.X.XXX.X-X_amd64.deb”
```

– для сервера ПК на ЭВМ под управлением ОС «РЕД ОС»:

а) в *терминале GNOME* перейти под учетную запись *root*, выполнив команду:

```
“su –”
```

б) ввести пароль;

- в) перейти в каталог с дистрибутивом ПК «Efros Config Inspector» v.4, указав команду (для примера указан каталог *tmp*):

```
"cd /tmp/"
```

- г) выполнить установку сервера командой (рис. 24):

```
"yum install efrosci-4.X.XXX.X-X.MUROM.x86_64.rpm"
```

```
[redos@redos tmp]$ su -
Пароль:
Последний вход в систему:Пт мар 20 15:18:39 MSK 2020на pts/0
[root@redos ~]#
[root@redos ~]# cd /tmp/
[root@redos tmp]# yum install efrosci-4.14.1.1-2.MUROM.x86_64.rpm
Загружены модули: fastestmirror, langpacks
Проверка efrosci-4.14.1.1-2.MUROM.x86_64.rpm: efrosci-4.14.1.1-2.el7.x86_64
efrosci-4.14.1.1-2.MUROM.x86_64.rpm отмечен для установки
Разрешение зависимостей
--> Проверка сценария
--> Пакет efrosci.x86_64 0:4.14.1.1-2.el7 помечен для установки
--> Проверка зависимостей окончена
base/x86_64 | 3.6 kB 00:00:00
base/x86_64/group_gz | 42 kB 00:00:00
base/x86_64/primary_db | 15 MB 00:00:01
updates/x86_64 | 2.9 kB 00:00:00
updates/x86_64/primary_db | 435 kB 00:00:00

Зависимости определены
=====
Package Architecture Version Repository Size
=====
Установка:
efrosci x86_64 4.14.1.1-2.el7 /efrosci-4.14.1.1-2.MUROM.x86_64 209 М
=====
Итого за операцию
=====
Установить 1 пакет

Общий размер: 209 М
Объем изменений: 209 М
Is this ok [y/d/N]: y
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
 Установка : efrosci-4.14.1.1-2.el7.x86_64 1/1
 Проверка : efrosci-4.14.1.1-2.el7.x86_64 1/1

Установлено:
efrosci.x86_64 0:4.14.1.1-2.el7

Выполнено!
```

Рисунок 24 – Окно установки сервера ПК

– после успешной установки автоматически откроется окно настроек службы сервера ПК (см. п. 2.3.2) (далее – серверная консоль), в котором в соответствии с п. 2.3.2 необходимо:

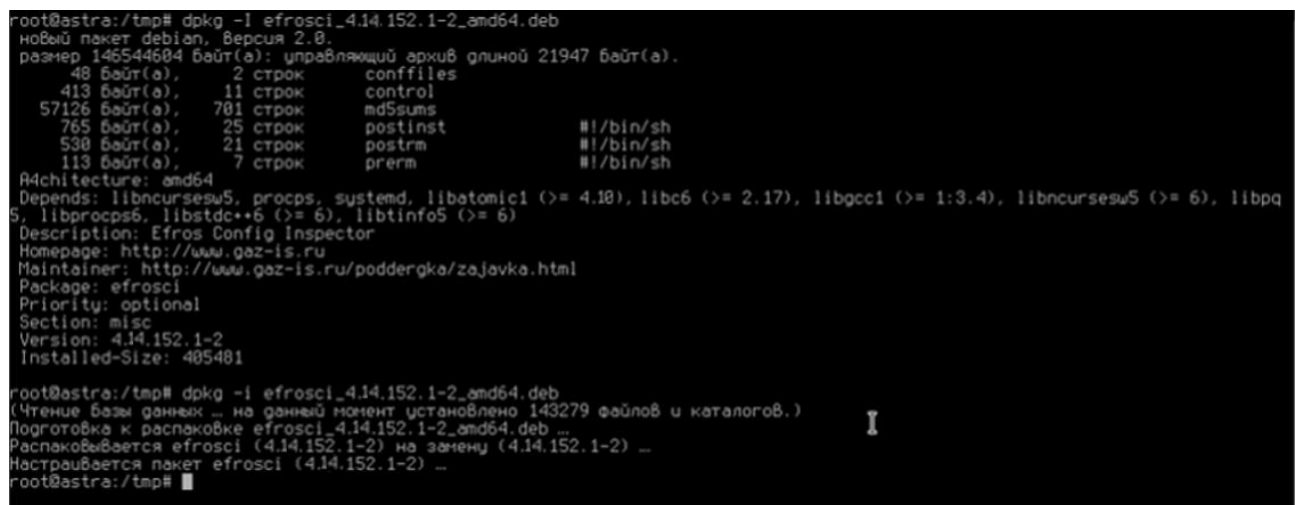
- проконтролировать заданные по умолчанию параметры работы сервера ПК и внести, при необходимости, изменения;
- выполнить действия по созданию БД комплекса или по подключению к существующей БД;
- выполнить запуск службы сервера ПК;
- завершить работу с консолью, выбрав пункт **Выход**.

По завершении настроек в окне терминала отобразится сообщение об успешной установке и настройке пакета, пример сообщения приведен на рисунке 25.

3) Проверить корректность работы службы серверной части комплекса можно, выдав команду:

```
“sudo systemctl status efroscli.service”
```

После установки серверной части комплекса внешние модули установлены не будут. Необходимо выполнить добавление внешних модулей устройств, используя средства клиентской консоли (см. документ «643.72410666.00082-01 96 01-01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование»).



```
root@astra:/tmp# dpkg -i efroscli_4.14.152.1-2_amd64.deb
новый пакет debian, версия 2.0.
размер 146544604 байт(а): управляющий архив длиной 21947 байт(а).
 48 байт(а), 2 строк conffiles
 413 байт(а), 11 строк control
 57126 байт(а), 781 строк md5sums
 765 байт(а), 25 строк postinst #!/bin/sh
 530 байт(а), 21 строк postrm #!/bin/sh
 113 байт(а), 7 строк prerm #!/bin/sh
Architecture: amd64
Depends: libcursesw5, procps, systemd, libatomic1 (>= 4.10), libc6 (>= 2.17), libgcc1 (>= 1:3.4), libncursesw5 (>= 6), libpq5, libprocps6, libstdc++6 (>= 6), libtinfo5 (>= 6)
Description: Efros Config Inspector
Homepage: http://www.gaz-is.ru
Maintainer: http://www.gaz-is.ru/poddergka/za/javka.html
Package: efroscli
Priority: optional
Section: misc
Version: 4.14.152.1-2
Installed-Size: 485481

root@astra:/tmp# dpkg -i efroscli_4.14.152.1-2_amd64.deb
(Чтение базы данных ... на данный момент установлено 143279 файлов и каталогов.)
Подготовка к распаковке efroscli_4.14.152.1-2_amd64.deb ...
Распаковывается efroscli (4.14.152.1-2) на замену (4.14.152.1-2) ...
Настраивается пакет efroscli (4.14.152.1-2) ...
root@astra:/tmp#
```

Рисунок 25 – Окно терминала с сообщением об успешном завершении установки сервера ПК

Для экспорта некоторых типов отчетов в формат PDF необходима установка Java Runtime Environment. Для ОС «Astra Linux SE» необходимо скачать (с официального сайта <https://www.java.com/>) и распаковать скачанный архив, выполнив команду:

```
“sudo tar -C /opt -xzf Загрузки/jre-8uXXX-linux-x64.tar.gz”
```

После чего проверить корректность указанного пути к Java в утилите настройки службы сервера ПК, запустив утилиту настройки службы сервера и открыв раздел **Дополнительно** (см. п. 2.3.2.3).

2.3.2. Настройка сервера ПК в серверной консоли

Для выполнения настройки параметров работы сервера ПК в серверной консоли после его установки и в процессе работы необходимо запустить утилиту настройки службы сервера ПК командой:

```
“sudo efroscli-settings”
```

Окно серверной консоли (рис. 26) содержит:

- информацию о состоянии службы сервера ПК (запущена, остановлена);
- номер версии сервера ПК;
- ссылки на разделы: **Настройка службы сервера**, **Настройка базы данных** и **Дополнительно**;
- команду **Выход** для завершения работы с консолью.

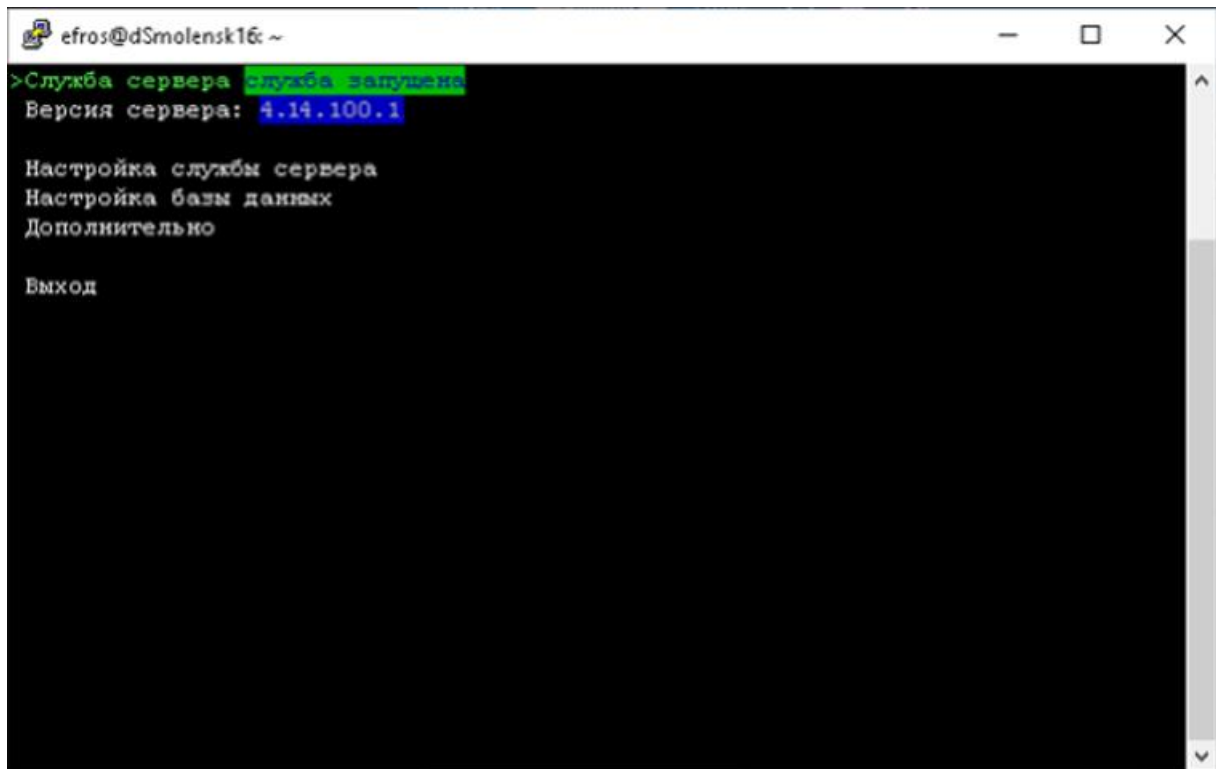
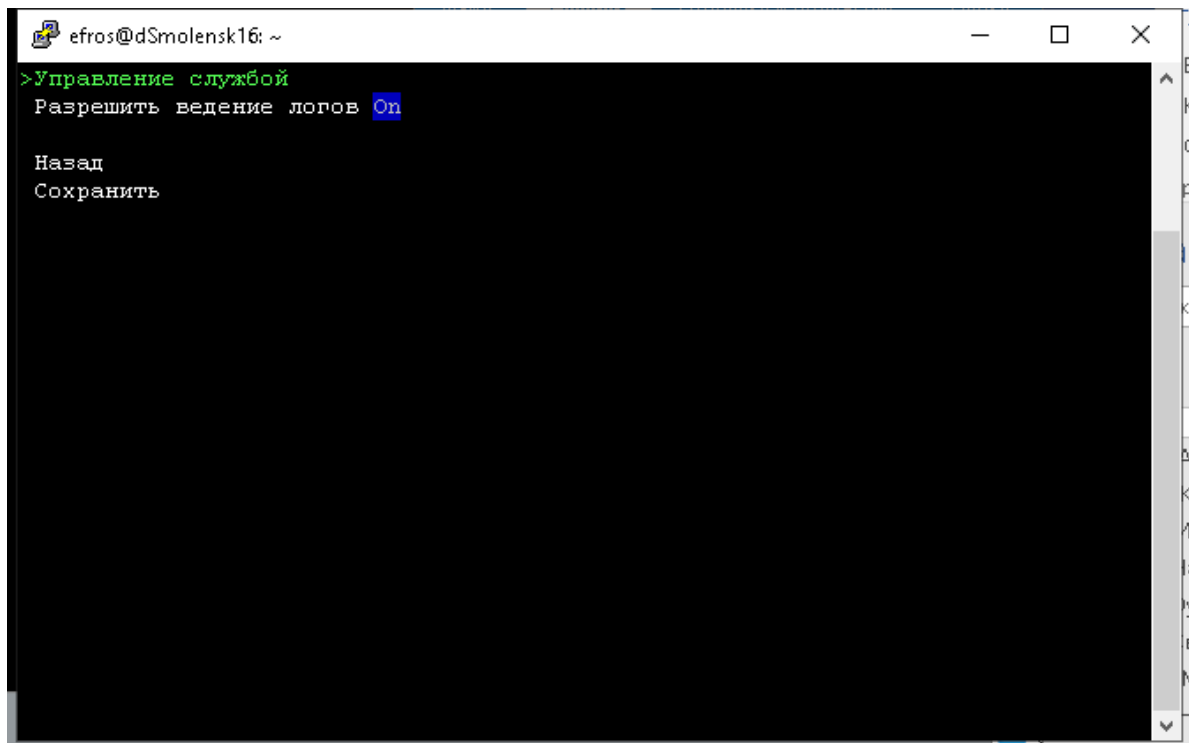


Рисунок 26 – Окно серверной консоли

2.3.2.1. Раздел Настройка службы сервера

Раздел **Настройка службы сервера** (рис. 27) предназначен для управления работой службы сервера ПК и задания некоторых параметров службы сервера ПК.

Рисунок 27 – Серверная консоль, раздел **Настройка службы сервера**

Назначение основных элементов управления раздела:

- при выборе пункта **Управление службой** открывается окно (рис. 28) с командами **Пуск**, **Стоп** – для запуска и остановки службы серверной части программного комплекса соответственно;
- параметр **Разрешить ведение логов** – для сохранения логов работы службы сервера ПК в папке `/var/log/efrosci`.

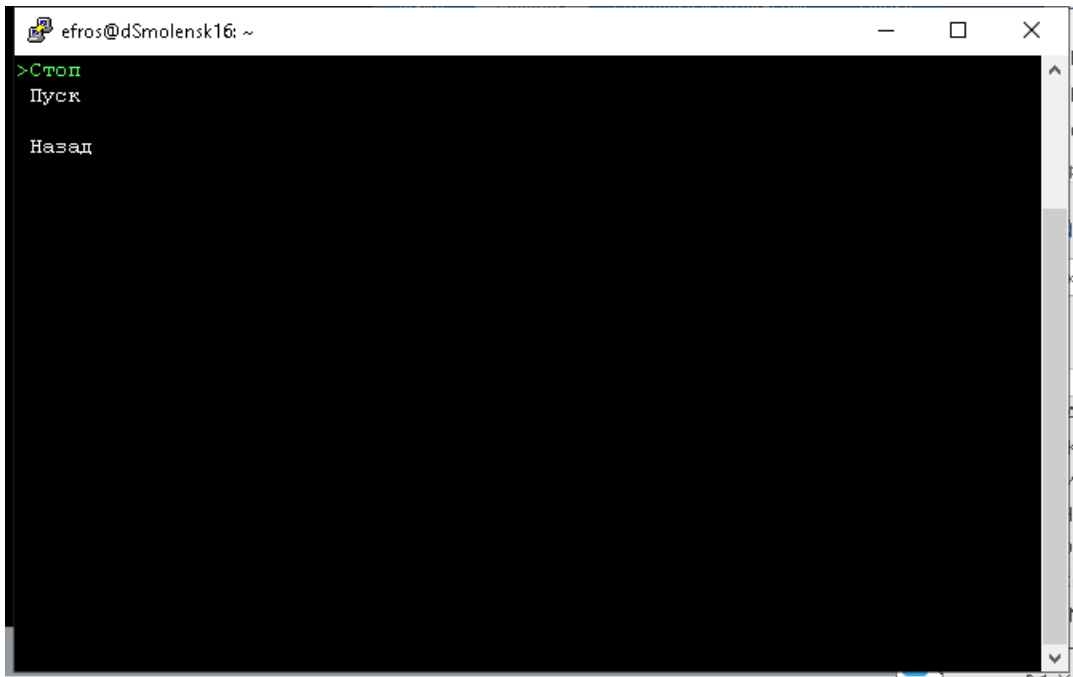


Рисунок 28 – Серверная консоль, **Управление службой**

Для сохранения внесенных изменений необходимо выбрать команду **Сохранить**, для выхода из режима редактирования без сохранения изменений и для перехода в родительское окно – выбрать команду **Назад**.

2.3.2.2. Раздел Настройка базы данных

Раздел **Настройка базы данных** (рис. 29) предназначен для настройки подключения сервера ПК к серверу БД. Перечень параметров для настройки приведен в таблице 13.

Команда **Проверить** предназначена для проверки наличия и версии базы данных программного комплекса на сервере БД. При нажатии кнопки:

- устанавливается соединение с указанным сервером БД;
- на сервере БД проверяется наличие БД комплекса;
- проверяется версия используемой БД;
- проверяется совпадение ключа защиты данных;
- в зависимости от результатов проверки выводится соответствующее сообщение.

Ссылка **Изменение БД** предназначена для перехода в окно изменения параметров подключения сервера ПК к серверу БД, в котором доступны следующие операции:

- создать новую БД;
- изменить настройки подключения к существующей БД;
- обновить версию БД (в случае, если БД на сервере уже существует).

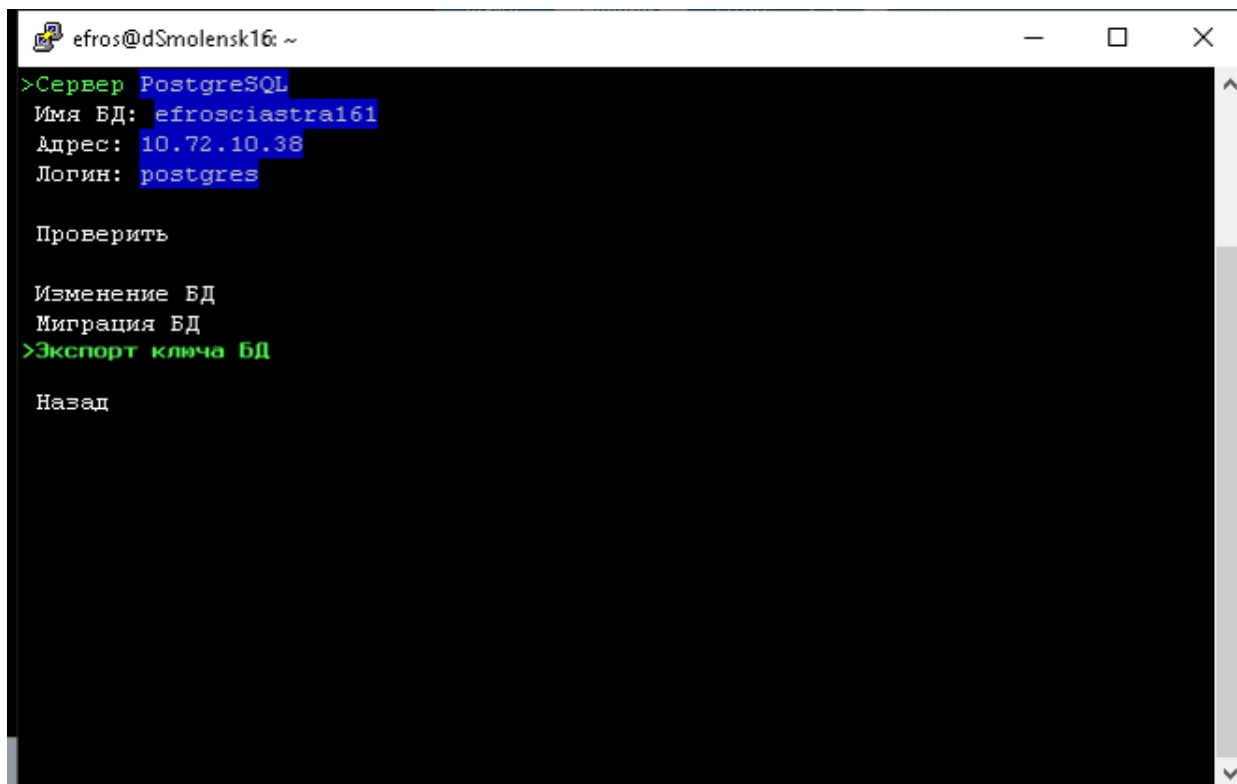
Рисунок 29 – Серверная консоль, раздел **Настройка базы данных**

Таблица 13 – Перечень параметров подключения ПК к серверу баз данных

Параметр	Описание/Назначение
Сервер	Тип СУБД, установленной на сервере баз данных: PostgreSQL/Jatoba, MySQL
Имя БД	Имя базы данных комплекса
Адрес	IP-адрес (или доменное имя) сервера БД
Логин	Имя пользователя для подключения к серверу БД

После нажатия кнопки **Изменение БД** откроется окно настройки подключения к БД (рис. 30), в котором есть два варианта: **Создать новую базу данных** или **Подключиться к существующей базе данных**.

Ссылка **Миграция БД** предназначена для копирования существующей БД комплекса на другой сервер баз данных в любую СУБД, из списка поддерживаемых комплексом (либо в иную СУБД, используемую на текущем сервере). Подробнее процесс копирования используемой БД средствами консоли серверной части ПК описан в пункте 6.1 «Операции с БД» настоящего Руководства.

Ссылка **Экспорт ключа БД** предназначена для выполнения резервирования ключа защиты данных БД комплекса, если при создании БД установлено подключение к БД с шифрованием (см. пункт 2.3.3 «Создание базы данных»).

Процедуры создания новой БД и подключения к существующей БД подробно описаны, соответственно, в пунктах 2.3.3 «Создание базы данных» и 2.3.4 «Подключение к существующей базе данных» настоящего Руководства.

Изменение настроек подключения сервера ПК к серверу БД вступит в силу после перезапуска службы сервера ПК в разделе **Настройка службы сервера**.

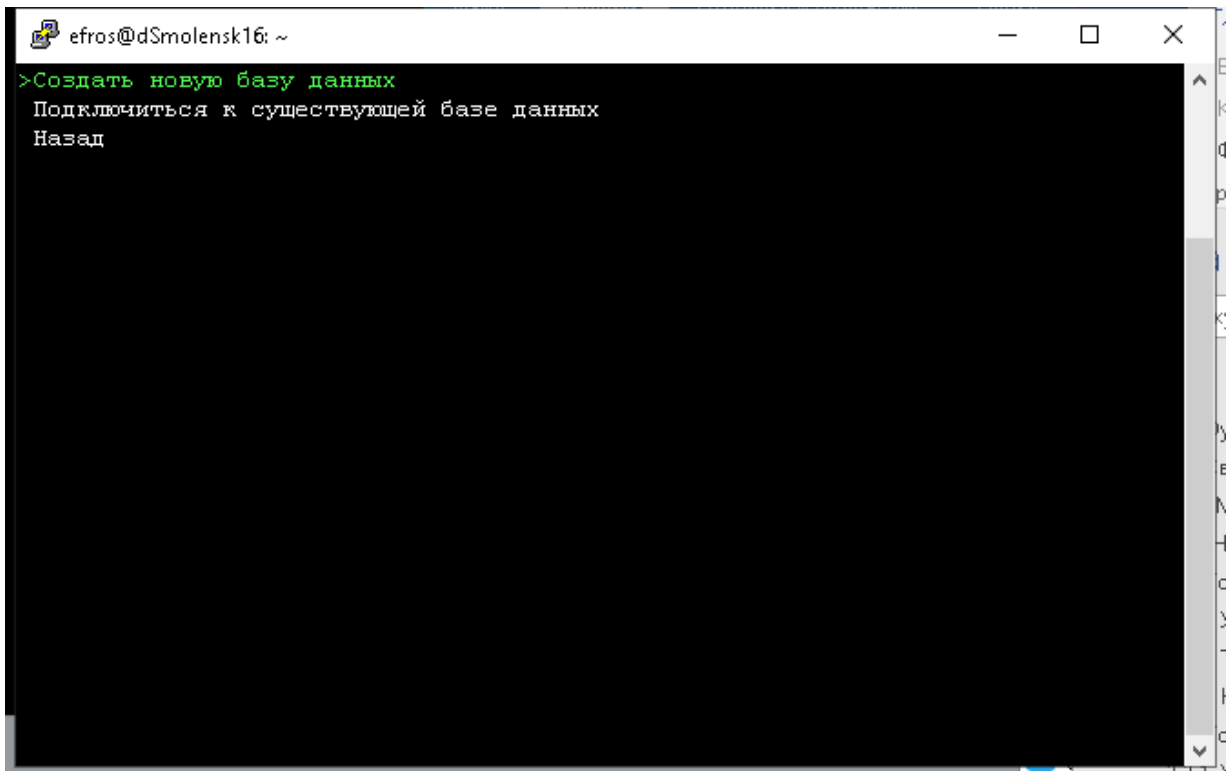


Рисунок 30 – Выбор варианта настройки соединения сервера ПК с БД

2.3.2.3. Раздел Дополнительно

Раздел **Дополнительно** (рис. 31) предназначен для изменения настроек удаленного доступа к серверу ПК, параметров запуска Java-приложений и параметров работы серверной части ПК. Перечень параметров приведен в таблице 14.

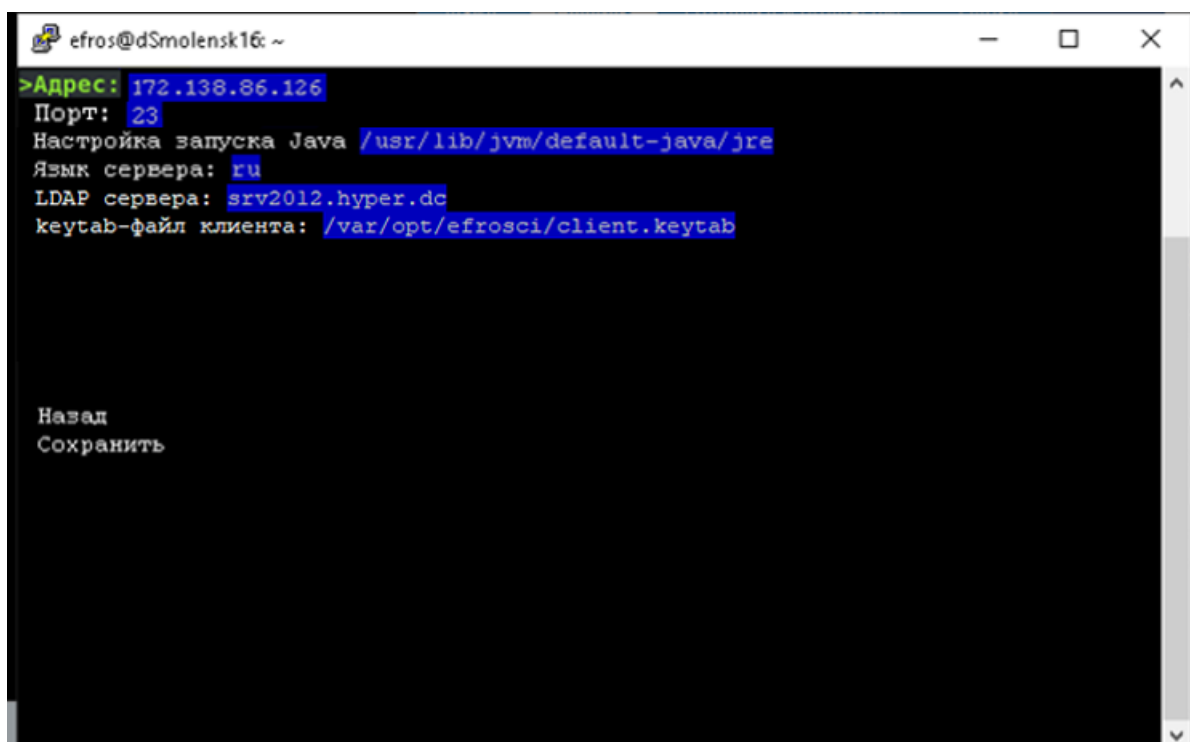


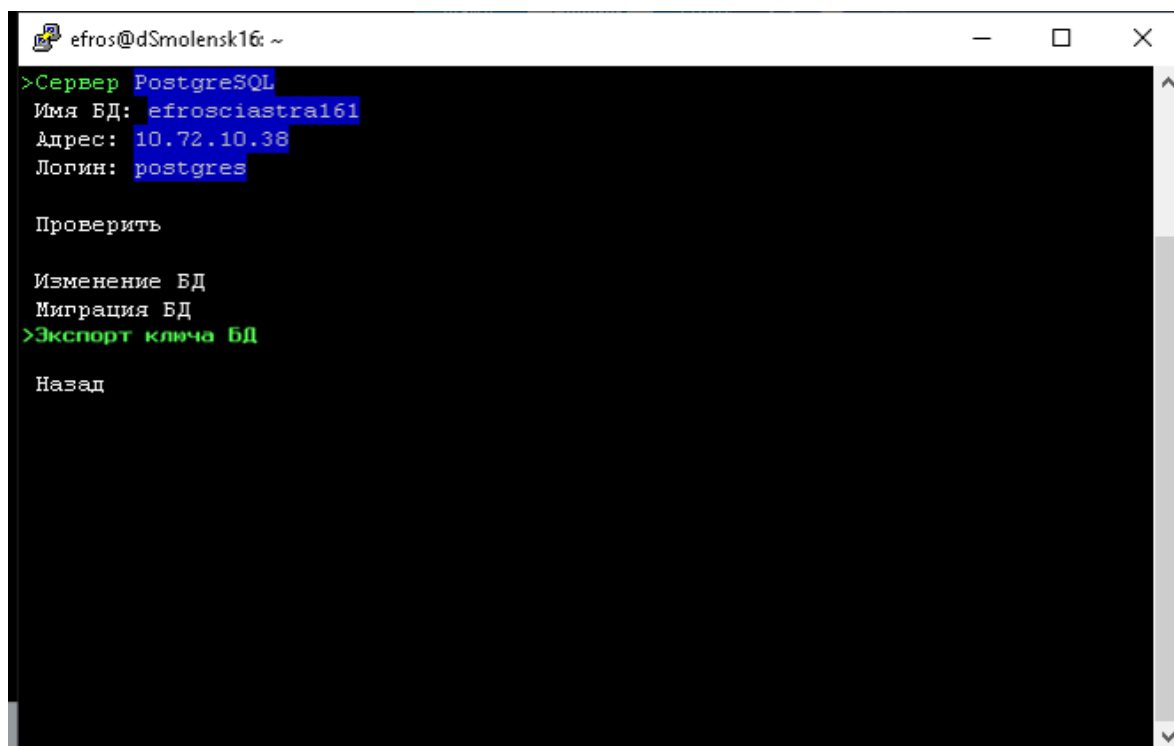
Рисунок 31 – Серверная консоль, раздел **Дополнительно**

Таблица 14 – Перечень настраиваемых параметров сервера ПК

Параметр	Описание/Назначение
<i>Параметры удаленного доступа</i>	
<i>Адрес</i>	Адрес сервера ПК
<i>Порт</i>	Номер TCP-порта для подключения к серверу программного комплекса
<i>Настройка запуска Java</i>	Путь к каталогу размещения ПО Java
<i>Язык сервера</i>	Выбор языка (ru – русский, en – английский).
<i>LDAP сервера</i>	Адрес сервера службы каталогов. Может быть указано несколько адресов, указание производится через запятую. Адрес может быть указан как в формате IP-адреса, так и доменного имени (FQDN)
<i>keytab-файл клиента</i>	Путь к файлу keytab. Keytab-файл изначально нужно сгенерировать, необходим для аутентификации в системе через Kerberos

2.3.3. Создание БД комплекса

После завершения установки сервера ПК необходимо настроить параметры подключения к БД. Для этого в окне серверной консоли (см. п. 2.3.2) перейти в раздел **Настройка базы данных** (рис. 32).

Рисунок 32 – Выбран раздел **Настройка базы данных**

Далее выбрать пункт **Изменение БД** → **Создать новую базу данных** (рис. 33) и в открывшемся окне указать параметры создаваемой БД:

- **Тип БД** – указать тип установленной СУБД;

- **Адрес** – указывается IP-адрес или имя используемого сервера БД. При размещении СУБД и сервера ПК на одной ЭВМ в поле **Адрес** можно указать значение *localhost*;
- **Имя БД** – имя создаваемой БД комплекса;
- **Логин и Пароль** – соответственно, имя и пароль пользователя СУБД, обладающего правами создания и редактирования БД, (например, для СУБД PostgreSQL – postgres). При этом пользователю, от имени которого происходит создание БД, должна быть присвоена роль sysadmin;
- **Использовать данного пользователя для подключения к базе данных** – устанавливается **On**, если введенные при создании новой БД имя и пароль пользователя СУБД в дальнейшем будут использоваться для подключения сервера ПК к БД;
- **Включить защиту данных (алгоритм AES-256)** – устанавливается **On**, если требуется защита хранящихся в БД комплекса отчетов с конфигурациями контролируемого оборудования. Защита данных выполняется по алгоритму AES-256, ключ защиты данных хранится в реестре сервера ПК и привязан к конфигурации сервера. Окно ввода пароля защиты ключа и места хранения ключа приведено на рис. 34. Переход к этому окну происходит при нажатии ENTER после вывода сообщения о создании БД.

После заполнения всех полей в окне создания новой БД для запуска операции создания БД комплекса на сервере БД, следует выбрать команду **Создать новую базу данных**.

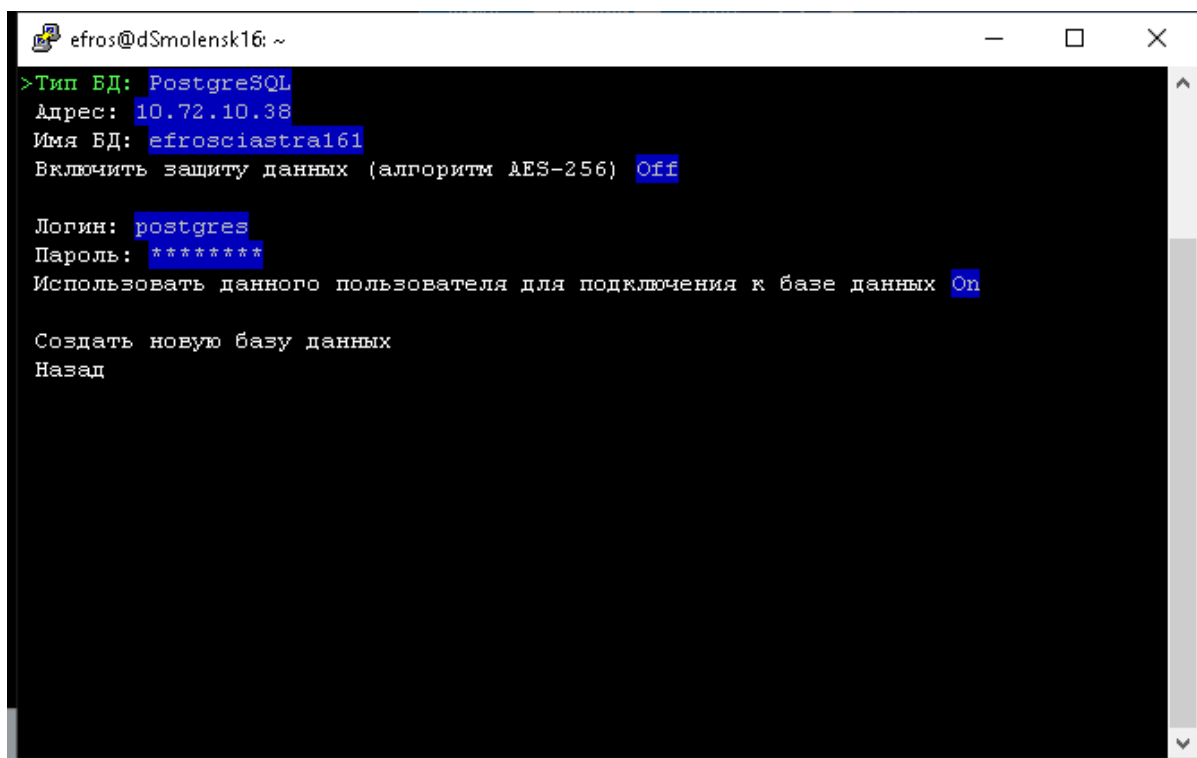


Рисунок 33 – Окно создания новой БД

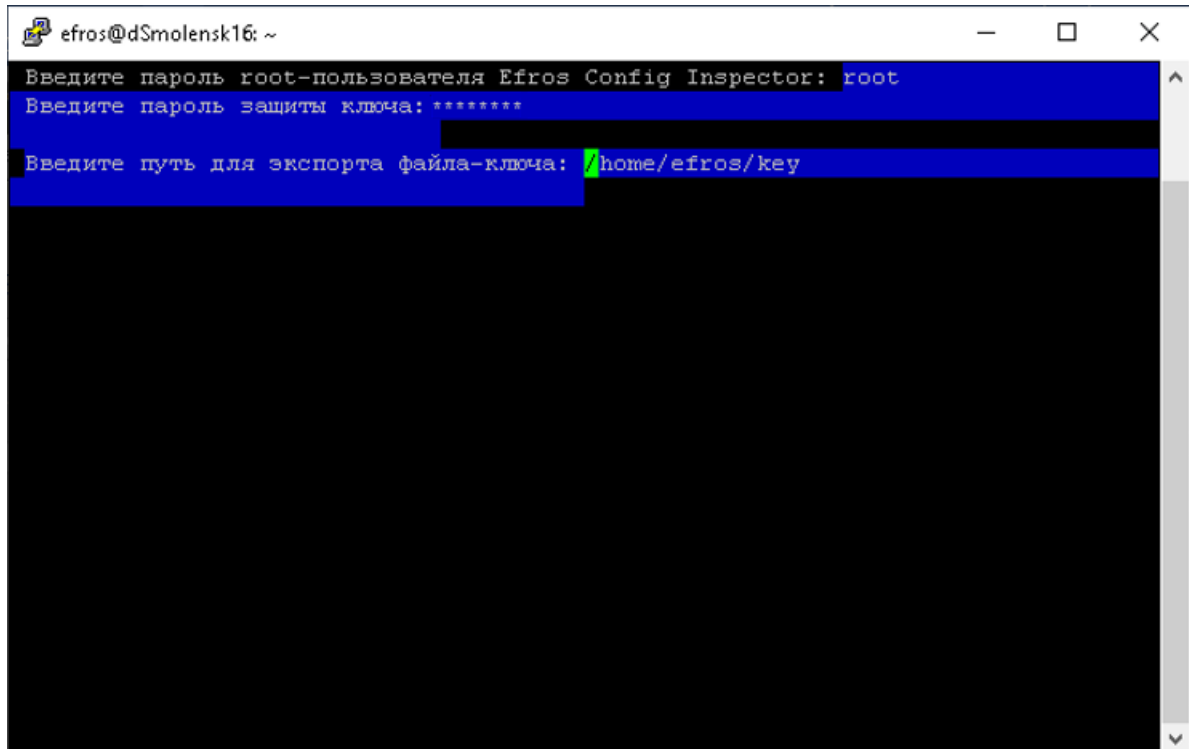


Рисунок 34 – Окно ввода параметров для ключа защиты данных БД

Для проверки подключения сервера ПК к созданной БД – выбрать в окне раздела **Настройка базы данных** службы комплекса (см. рис. 33) пункт **Проверить**. В нижней части окна отобразится сообщение с результатами проверки (рис. 35).

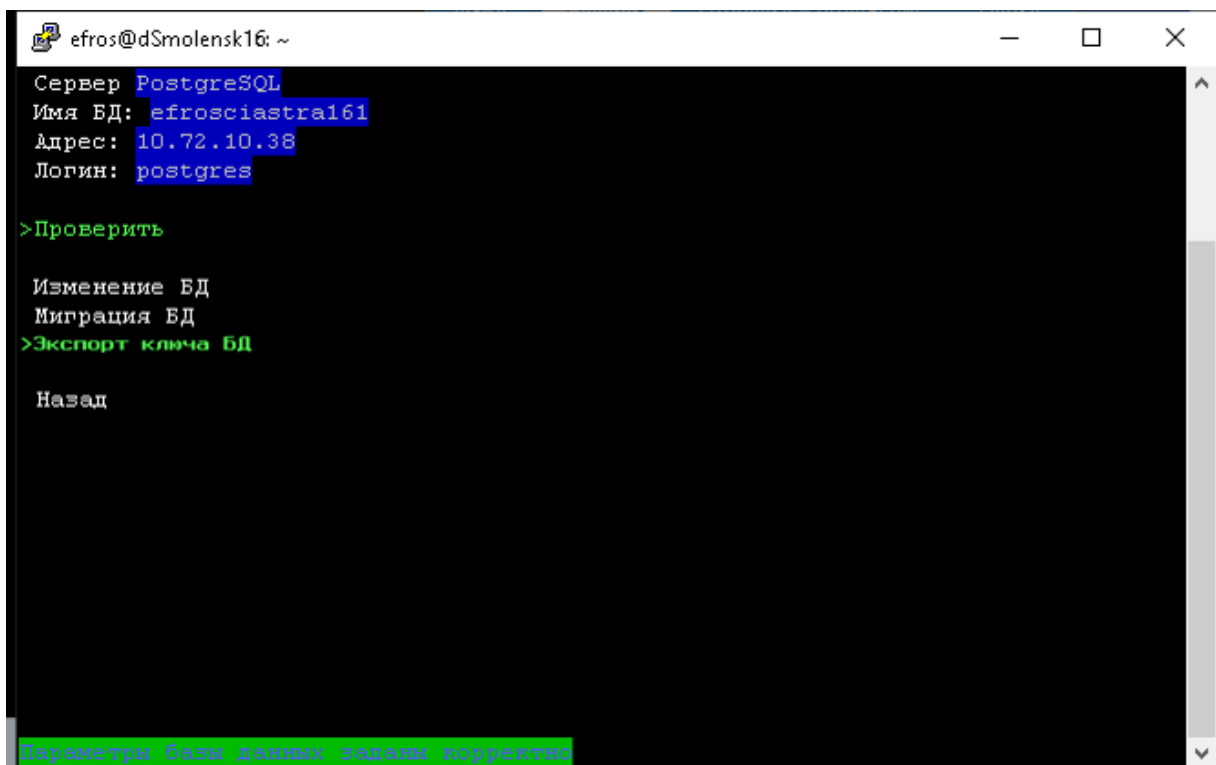


Рисунок 35 – Окно настройки службы комплекса с результатами проверки

В случае некорректных параметров подключения сервера ПК к серверу БД будет выведено сообщение об ошибке. Следует исправить неверно введенные данные и

заново проверить возможность подключения сервера ПК к БД, повторив приведенные выше действия.

2.3.4. Подключение к существующей базе данных

Для подключения сервера ПК к уже существующей БД необходимо выбрать в окне серверной консоли раздел **Настройка базы данных** (см. рис. 29), далее пункты **Изменение БД** → **Подключиться к существующей базе данных**.

В открывшемся окне (рис. 36) доступны для заполнения следующие поля (подробное описание этих полей приведено в п. 2.3.3 настоящего Руководства):

- **Тип БД** – тип используемой СУБД;
- **Адрес** – IP-адрес или имя используемого сервера БД;
- **Имя БД** – имя существующей на сервере БД комплекса;
- **Логин и Пароль** – имя и пароль пользователя СУБД, от имени которого будет происходить подключение к серверу БД.

Далее необходимо заполнить поля требуемыми данными и выбрать пункт **Соединить**. В окне отобразится сообщение с результатами проверки корректности соединения сервера ПК с указанной БД. В случае успешной проверки выводится сообщение аналогично рисунку 36.

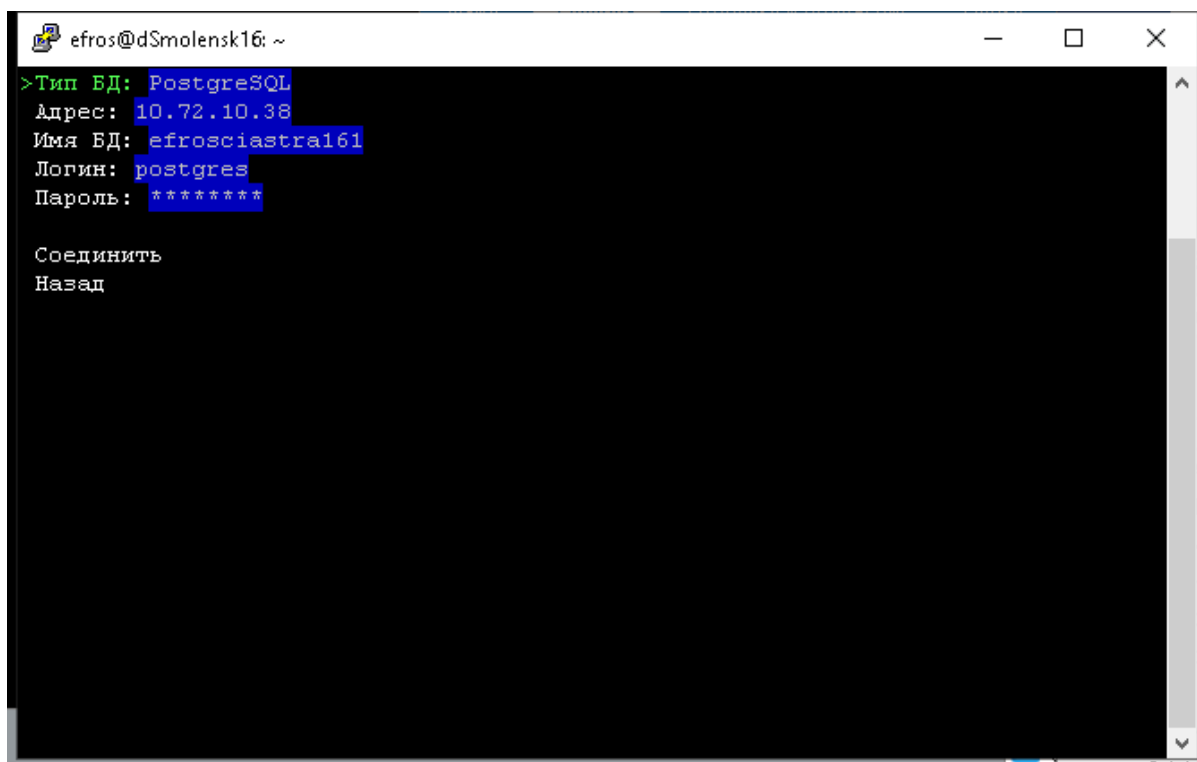


Рисунок 36 – Окно параметров подключения к БД

В случае ввода некорректных параметров подключения сервера ПК к серверу БД будет выведено сообщение об ошибке. Следует исправить неверно введенные данные и заново проверить возможность подключения сервера ПК к БД, выбрав пункт **Соединить**.

В случае ввода корректных параметров подключения сервера ПК к защищенной БД откроется запрос ввода ключа защиты данных БД, далее указать пароль, с использованием которого был защищен ключ, и значение ключа защиты данных.

В случае ввода неверных значений пароля и/или ключа защиты данных в окне серверной консоли отобразится соответствующее сообщение.

При успешной проверке соединения сервера ПК с защищенной БД также в окне серверной консоли отобразится соответствующее сообщение.

Для применения внесенных изменений выполните перезапуск службы сервера ПК в разделе **Настройка службы сервера** (см. п. 2.3.2.1).

2.4. Установка windows-агента комплекса

2.4.1. Установка windows-агента

Windows-агент ПК «Efros Config Inspector» v.4 устанавливается на контролируемые рабочие станции (сервера) под управлением ОС MS Windows (x64), и предназначен для обеспечения операций контроля целостности файловых объектов. Для установки windows-агента ПК «Efros Config Inspector» v.4 необходимо войти на контролируемую рабочую станцию (сервер) от имени учетной записи с правами администратора этой рабочей станции (сервера) и запустить с используемого носителя установочного комплекта ПК «Efros Config Inspector» v.4 на исполнение файл *Efros Config Inspector Agent 4.msi*.

Откроется окно мастера установки windows-агента (рис. 37), в котором следует выбрать папку для установки агента или оставить заданную по умолчанию (*C:\Program Files\EFROS Config Inspector 4*) и нажать кнопку **Далее**.

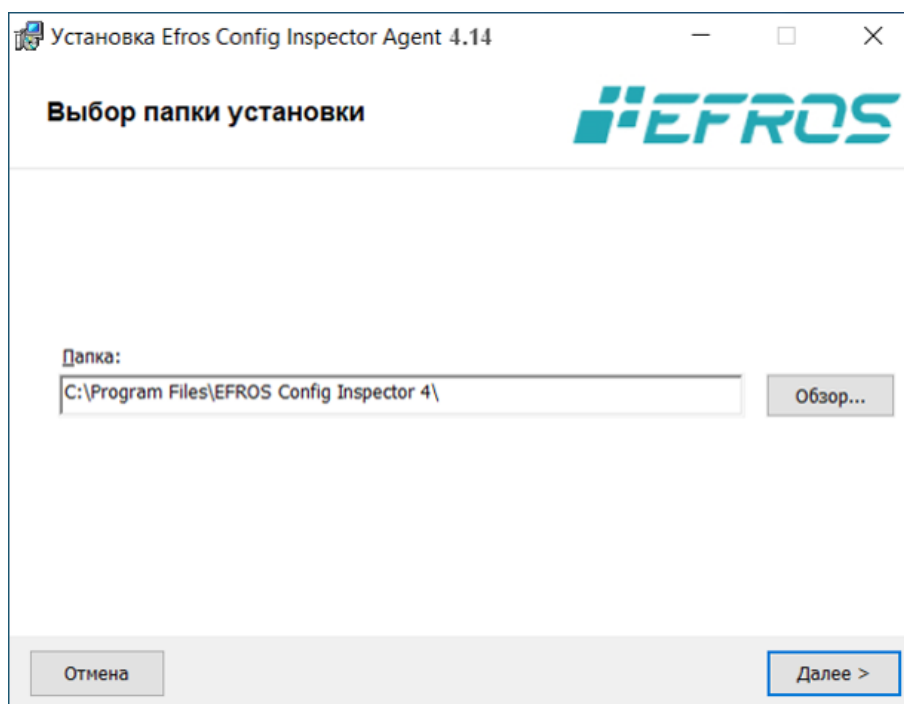


Рисунок 37 – Диалоговое окно выбора папки установки windows-агента комплекса

В диалоговом окне готовности мастера к установке (рис. 38) для запуска процесса инсталляции с заданными ранее параметрами следует нажать кнопку **Установить**:

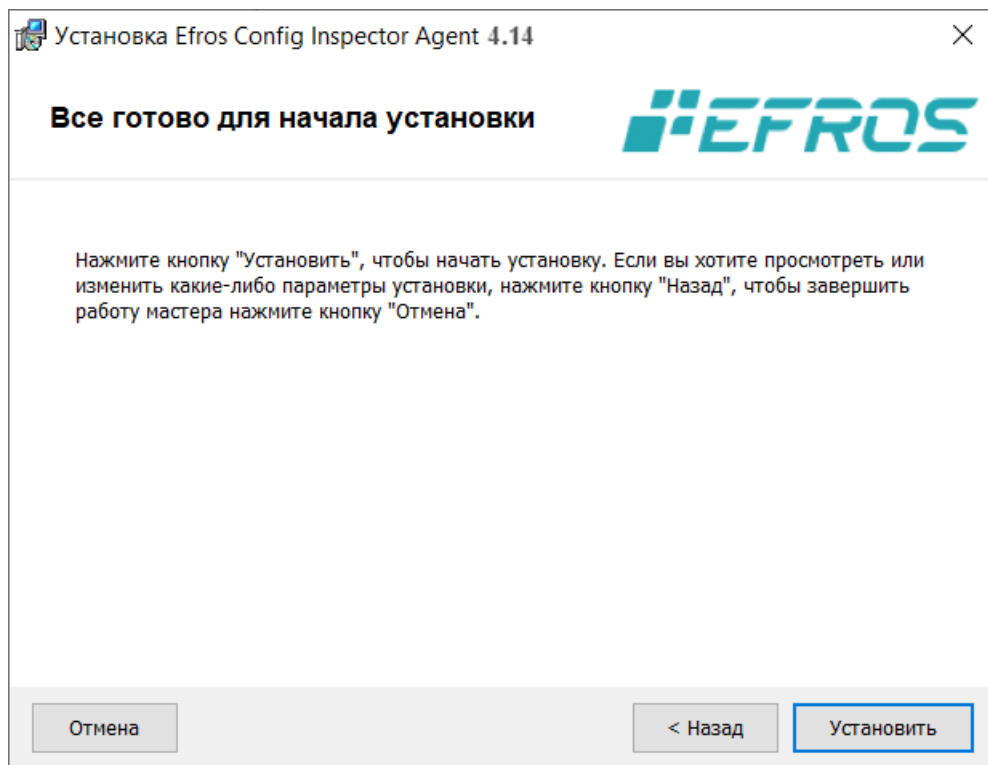


Рисунок 38 – Диалоговое окно готовности к установке

Ход установки windows-агента программного комплекса будет отображаться в окне мастера установки (рис. 39).

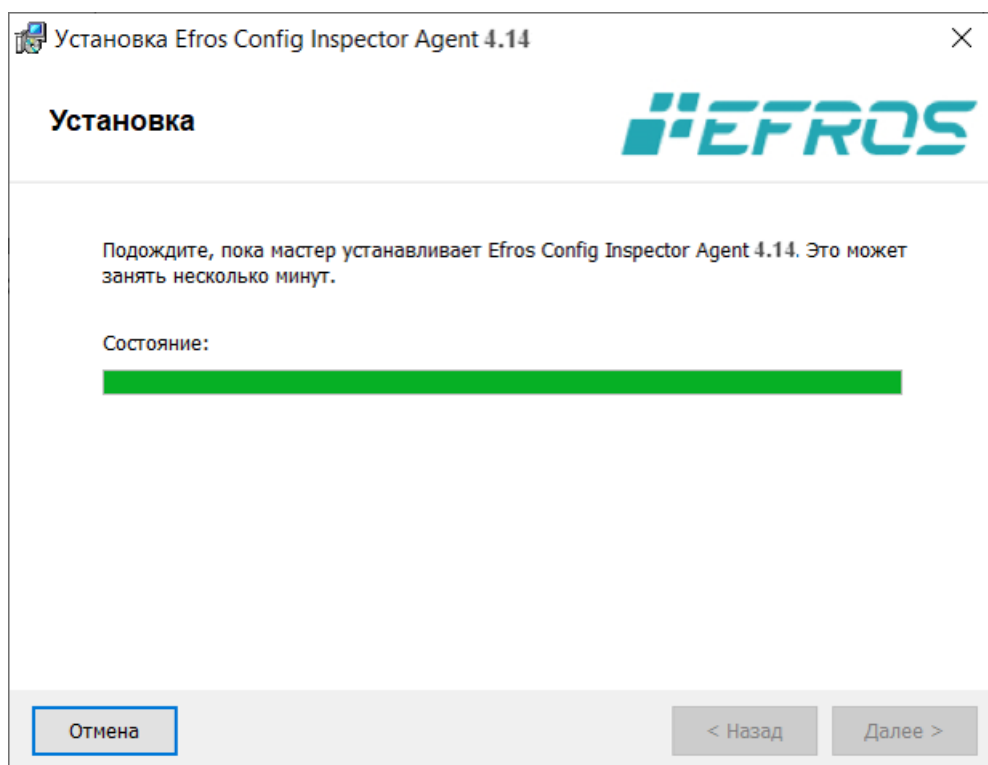


Рисунок 39 – Диалоговое окно процесса установки

После окончания установки windows-агента откроется диалоговое окно завершения работы мастера установки (рис. 40), в котором следует нажать кнопку **Готово**.

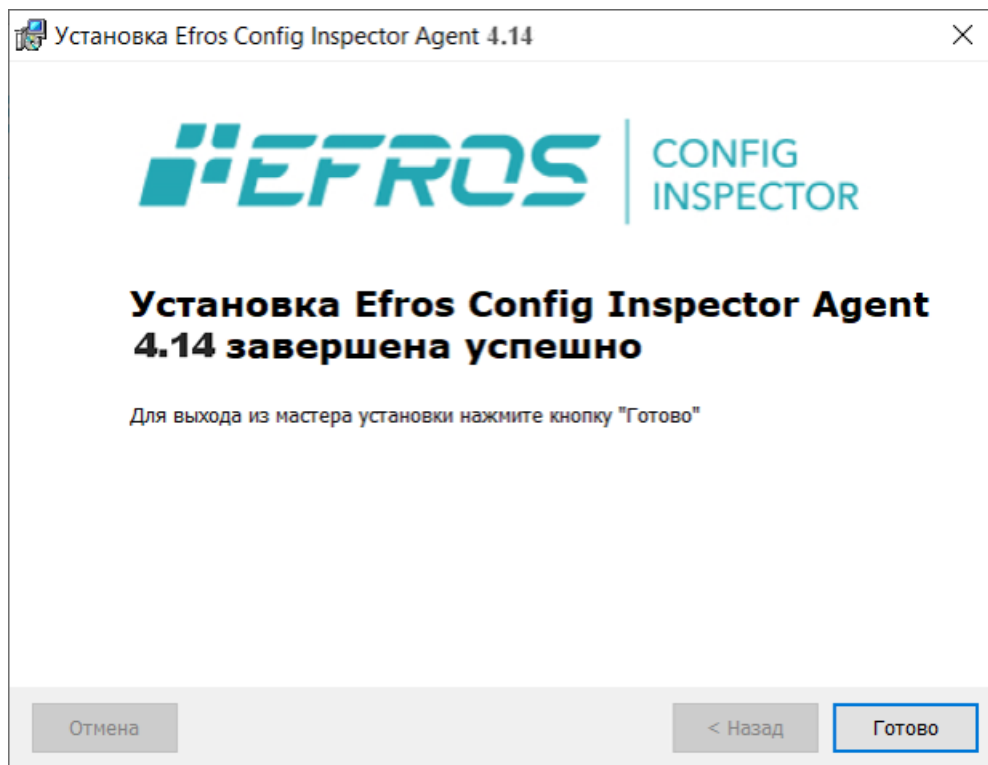


Рисунок 40 – Диалоговое окно завершения работы мастера установки

Windows-агент ПК «Efros Config Inspector» v.4 устанавливается на контролируруемую рабочую станцию (сервер) в качестве службы *EFROS CI Agent Service 4*, которая запускается в автоматическом режиме при загрузке ОС от имени системной учетной записи (*Local System*).

Настройка параметров службы windows-агента выполняется в окне настройки параметров службы «Efros Config Agent» v.4 (C:\Program Files\EFROS Config Inspector 4\Agent\WASetup.exe).

2.4.2. Настройка параметров службы windows-агента

Вызов окна настройки параметров службы «Efros Config Agent» v.4 осуществляется путем запуска файла *WASetup.exe* из директории *C:\Program Files\EFROS Config Inspector 4\Agent*.

Во вкладке **Службы** окна настройки параметров службы «Efros Config Agent» v.4 находятся (рис. 41):

- кнопка **Пуск** – для запуска службы windows-агента;
- кнопка **Стоп** – для остановки службы windows-агента;
- кнопка **Обновить** – для обновления статуса службы windows-агента;
- параметр **Разрешить ведение логов**.

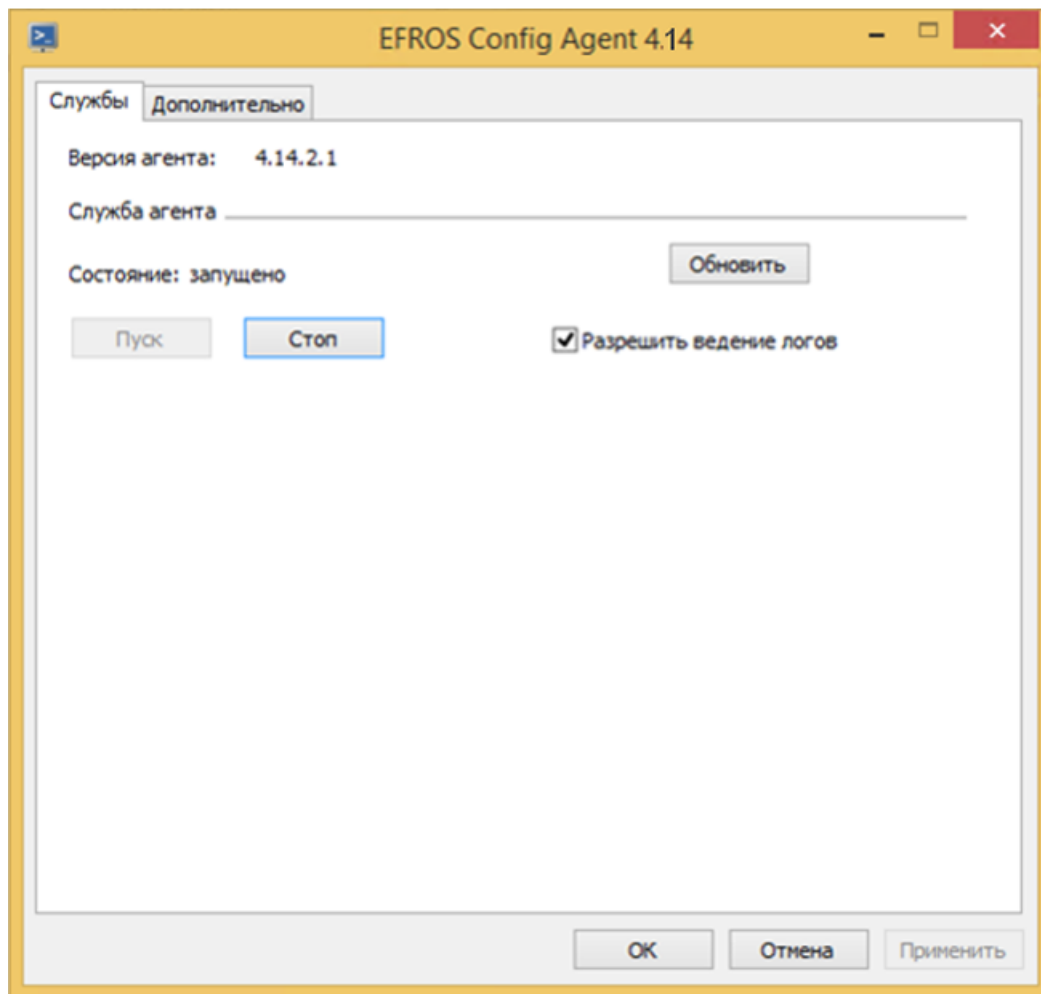


Рисунок 41 – Вкладка **Службы** окна настройки параметров службы «Efros Config Agent» v.4

Во вкладке **Дополнительно** (рис. 42) доступны для настройки параметры, приведенные в таблице 15.

После завершения настройки службы windows-агента, необходимо нажать кнопку **Применить** и кнопку **ОК** для закрытия окна. После этого настроенные параметры будут приняты и вступят в силу при следующем запуске службы windows-агента.

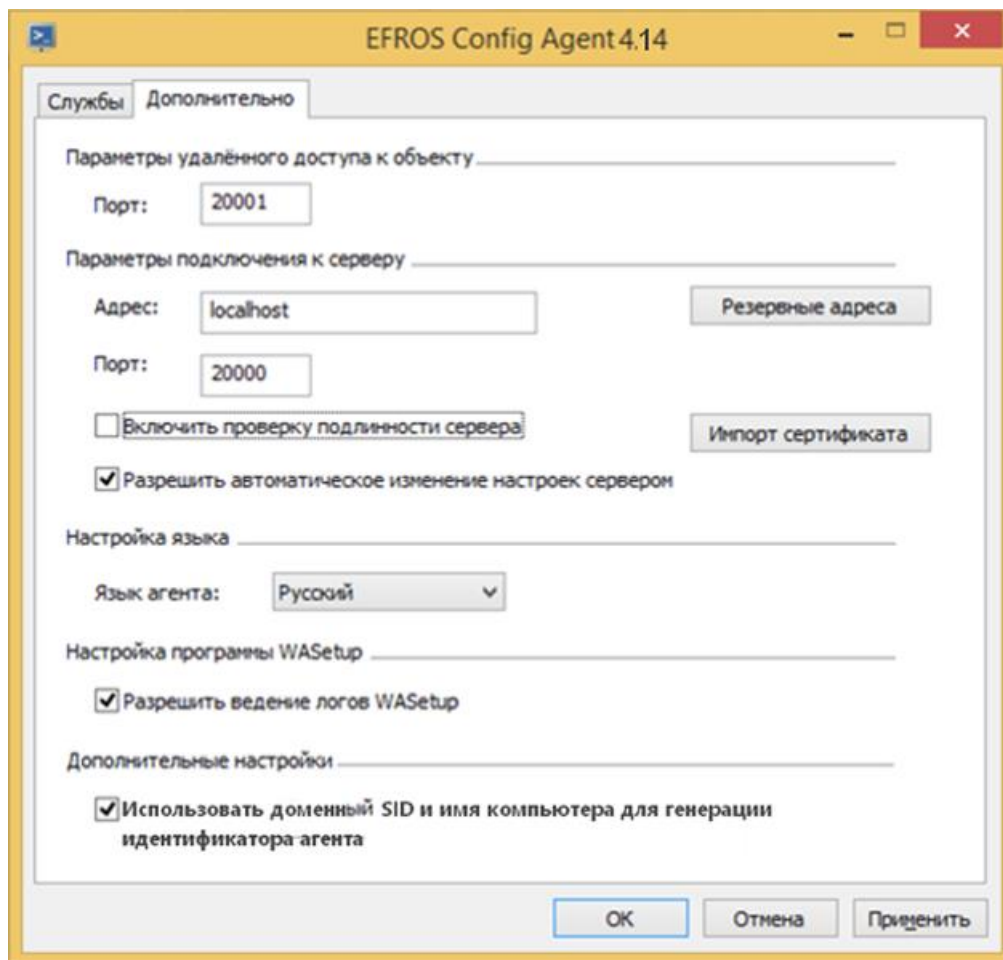


Рисунок 42 – Вкладка **Дополнительно** окна настройки параметров службы «Efros Config Agent» v.4

Таблица 15 – Настройки службы windows-агента, доступные во вкладке **Дополнительно**

Параметр	Назначение
Параметры удаленного доступа к объекту	
Порт	Номер порта, используемого для установки связи между сервером ПК и windows-агентом (для оповещения о включении windows-агента)
Параметры подключения к серверу	
Адрес	IP-адрес сервера ПК или его DNS-имя. Если серверная часть комплекса и windows-агент установлены на один компьютер, то в поле можно ввести 127.0.0.1 или localhost (значение по умолчанию)
Порт	Номер порта, используемого для подключения сервера ПК к windows-агенту
Кнопка <i>Резервные адреса</i>	Позволяет задавать резервные адреса для установки связи с резервными серверами ПК. В случае работы комплекса в режиме отказоустойчивости, windows-агент получает информацию о резервных серверах ПК, с которыми он может работать в случае отказа основного сервера ПК

Параметр	Назначение
<i>Включить проверку подлинности сервера</i>	<p>При включенном параметре (флаг в поле установлен) происходит проверка серверной части и windows-агента с помощью сертификата.</p> <p>При первом подключении устройства с установленным windows-агентом проверка подлинности должна быть выключена как в окне настройки windows-агента, так и в клиентской консоли для внешнего модуля Windows (см. пунктом «Внесение изменений в параметры работы внешнего модуля» документа «643.72410666.00082-01 96 01-01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование»).</p> <p>После первого успешного подключения устройства для использования проверки подлинности сервера по сертификату необходимо включить проверку подлинности в окне настройки windows-агента и в клиентской консоли, после чего windows-агент принимает сертификат серверной части. Во время взаимодействия серверной части и windows-агента происходит проверка, основанная на принятом сертификате. Другие серверные части, не имеющие данного сертификата, не смогут установить соединение с windows-агентом</p>
Кнопка <i>Импорт сертификата</i>	Позволяет устанавливать сертификат взаимодействия с серверной частью вручную
<i>Разрешить автоматическое изменение настроек сервером</i>	При включенном параметре (флаг в поле установлен) настройки windows-агента (адрес сервера, проверка подлинности сертификатом) могут быть автоматически изменены сервером ПК
<i>Язык агента</i>	Позволяет выбрать язык windows-агента (русский, английский)
<i>Разрешить ведение логов WASETUP</i>	Включает/отключает ведение логов программы настройки windows-агента <i>WASETUP</i>
<i>Использовать доменный компьютер или имя компьютера для генерации идентификатора агента</i>	Позволяет автоматически генерировать uuid windows-агента на основе SID домена и имени компьютера при подключении ОС в домен. Используется для обеспечения уникальности uuid windows-агента в случае клонирования виртуальных машин с предустановленным windows-агентом

2.4.3. Подготовка flash накопителя для контроля Windows с использованием портативного Windows-агента

В пункте приведены правила подготовки flash накопителя для контроля устаревших ОС серии Windows x86 с помощью портативного Windows-агента ПК «Efros Config Inspector» v.4.

2.4.3.1. Подготовка flash накопителя с поддержкой проверки подлинности

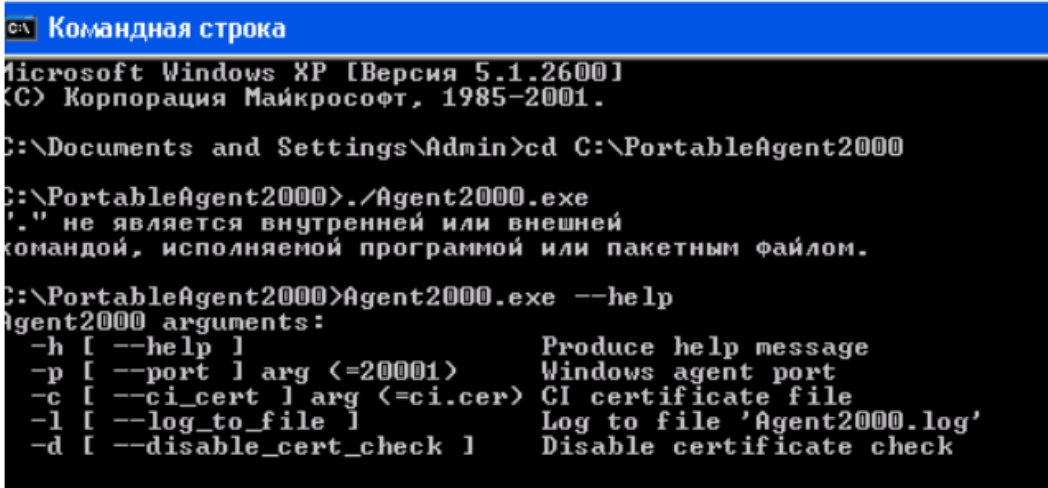
Для использования портативного Windows-агента для платформы под управлением устаревших ОС серии Windows x86 (Windows Server 2000/2000 R2, Windows Server 2003/2003 R2, Windows Server 2008/2008R2, Windows XP, Windows Vista, Windows 7) на flash необходимо провести первичную подготовку:

- 1) Разрешить запись для flash.
- 2) Записать портативный Windows-агент и дополнительные внешние библиотеки на flash. .
- 3) Экспортировать сертификат сервера и поместить его на flash для дальнейшей работы агента с необходимым сервером. Получить сертификат можно двумя способами:

- автоматически – для автоматического получения сертификата необходимо запустить проверку Windows устройства, добавленного на сервере ПК «Efros Config Inspector» v.4, после чего агент автоматически запишет на flash накопитель полученный от сервера сертификат с именем «ci.cer»;

- вручную – для ручной записи сертификата необходимо выполнить экспорт со стороны сервера. На сервере открыть браузер и перейти по ссылке <https://localhost:20000/download/ci.cer>. После получения сертификата перенести его на flash накопитель.

- 4) Запретить запись для flash.
- 5) Запустить агент с аргументами в соответствии с рис. 43.



```
с:\ Командная строка
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\Admin>cd C:\PortableAgent2000

C:\PortableAgent2000>./Agent2000.exe
'.' не является внутренней или внешней
командой, исполняемой программой или пакетным файлом.

C:\PortableAgent2000>Agent2000.exe --help
Agent2000 arguments:
-h [ --help ]          Produce help message
-p [ --port ] arg (<=20001)  Windows agent port
-c [ --ci_cert ] arg (<=ci.cer)  CI certificate file
-l [ --log_to_file ]      Log to file 'Agent2000.log'
-d [ --disable_cert_check ]  Disable certificate check
```

Рисунок 43 – Аргументы запуска портативного Windows-агента

2.4.3.2. Подготовка flash накопителя без проверки подлинности

Для использования портативного Windows-агента на flash необходимо провести первичную подготовку:

- 1) Разрешить запись для flash.
- 2) Записать портативный Windows-агент и дополнительные внешние библиотеки на flash.
- 3) Запретить запись для flash.

- 4) Запустить агент. Запуск агента с ключом `-d` (см. рис. 43) позволит отключить проверку подлинности, при подключении любым сервером ПК «Efros Config Inspector» v.4 сертификат проверяться не будет.

2.5. Установка и настройка коллектора задач

Для установки коллектора задач ПК «Efros Config Inspector» v.4 следует запустить с используемого носителя установочного комплекта ПК «Efros Config Inspector» v.4 на исполнение файл *Efros Config Inspector Collector 4.msi*.

Откроется окно мастера установки коллектора задач (рис. 44), в котором следует выбрать папку для установки коллектора задач или оставить заданную по умолчанию (*C:\Program Files\EFROS Config Inspector 4*) и нажать кнопку **Далее**.

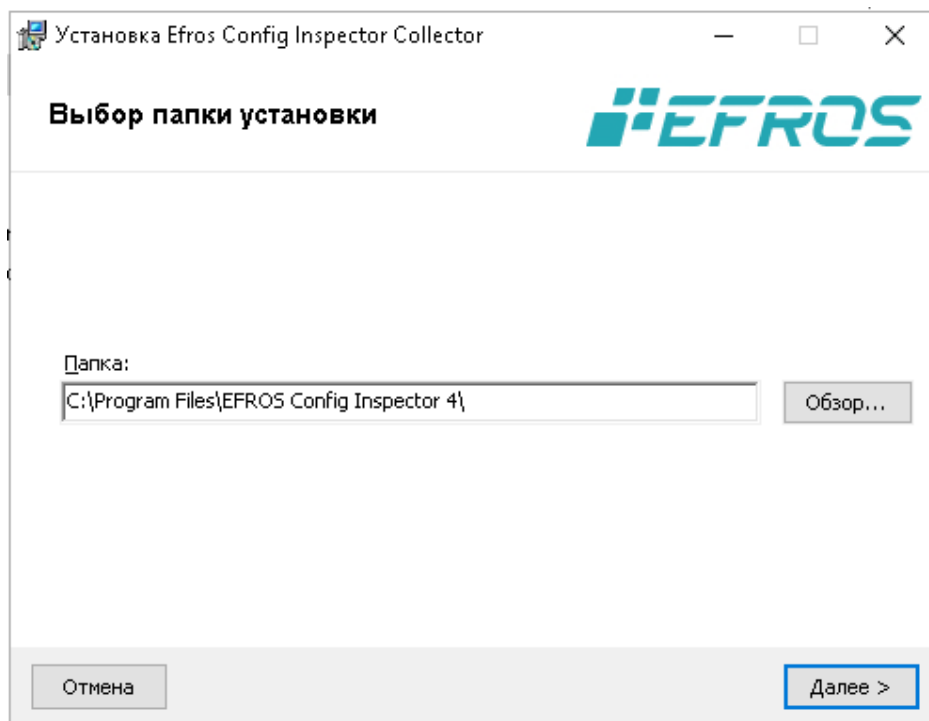


Рисунок 44 – Окно выбора каталога установки коллектора задач

В диалоговом окне начала установки для запуска процесса установки следует нажать кнопку **Установить** (рис. 45).

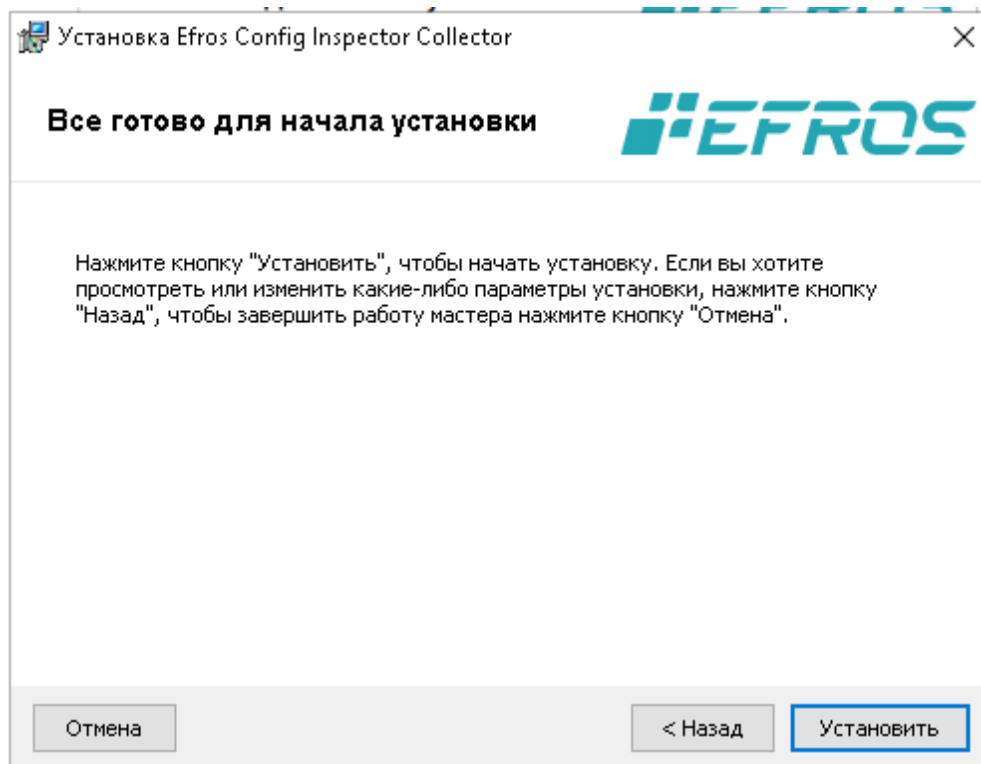


Рисунок 45 – Окно начала установки

По завершении установки откроется диалоговое окно завершения работы мастера установки (рис. 46), в котором следует нажать кнопку **Готово**:

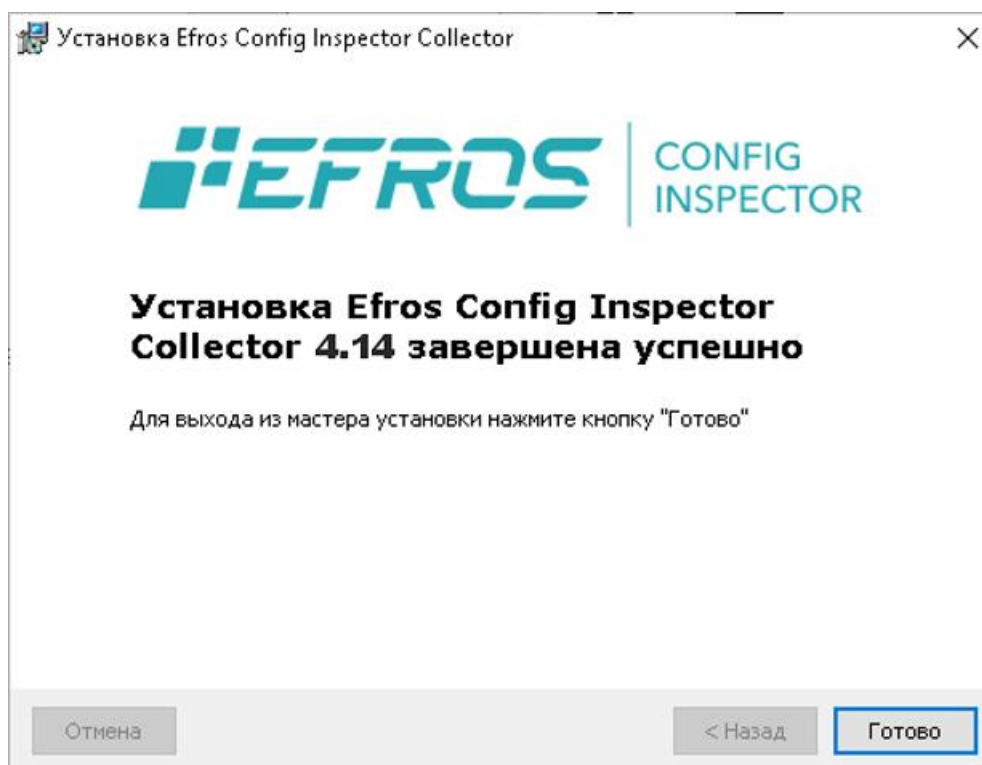


Рисунок 46 – Окно завершения установки

В результате выполнения мастера установки будет установлен «Efros Config Inspector Collector» v 4.

Настройка параметров службы коллектора задач выполняется в окне настройки параметров службы «Efros Config Collector» v.4.

Вызов окна настройки параметров службы «Efros Config Collector» v.4 осуществляется из меню **Пуск** на панели задач. Для этого следует выбрать **Все программы** → **Efros Config Inspector 4** → **CollectorSetup**.

Во вкладке **Службы** окна настройки параметров службы «Efros Config Collector» v.4 находятся (рис. 47):

- кнопка **Пуск** – для запуска службы коллектора логов;
- кнопка **Стоп** – для остановки службы коллектора задач;
- кнопка **Обновить** – для обновления статуса службы коллектора задач;
- параметр **Разрешить ведение логов**.

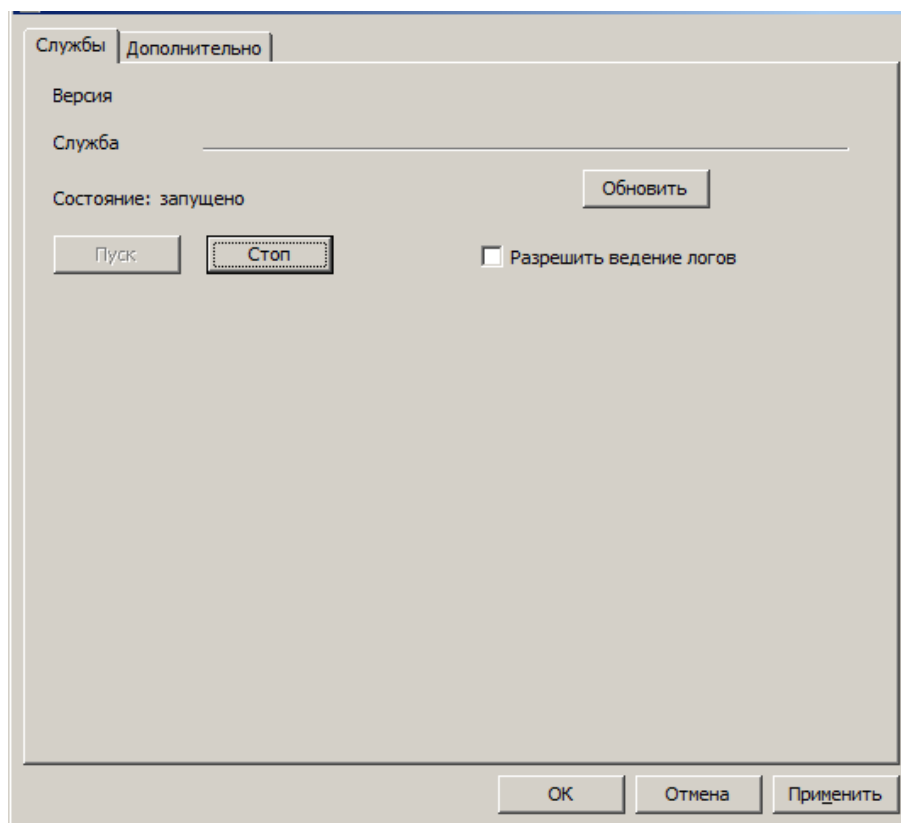


Рисунок 47 – Вкладка **Службы**

Во вкладке **Дополнительно** находится (рис. 48):

- поле **Порт** – номер порта, используемого для установки связи с серверной частью;
- параметр **Включить проверку подлинности удаленного сервера** – при включенном параметре происходит проверка серверной части и коллектора задач с помощью сертификата;
- кнопка **Импорт сертификата** – позволяет устанавливать сертификат взаимодействия с серверной частью вручную;
- поле **Путь к каталогу** с кнопкой **Обзор** – позволяет установить каталог, в котором находится Java;

- поле **Язык коллектора** – позволяет выбрать язык коллектора (русский, английский);
- параметр **Разрешить ведение логов CollectorSetup**.

Примечание – При первом подключении коллектор задач принимает сертификат серверной части. Во время взаимодействия серверной части и коллектора задач происходит проверка, основанная на принятом сертификате. Другие серверные части, не имеющие данного сертификата, не смогут установить соединение с коллектором задач.

После завершения настройки службы коллектора, необходимо нажать кнопку **Применить** и кнопку **ОК** для закрытия окна. После этого, настроенные параметры будут приняты и вступят в силу при следующем запуске службы коллекторов.

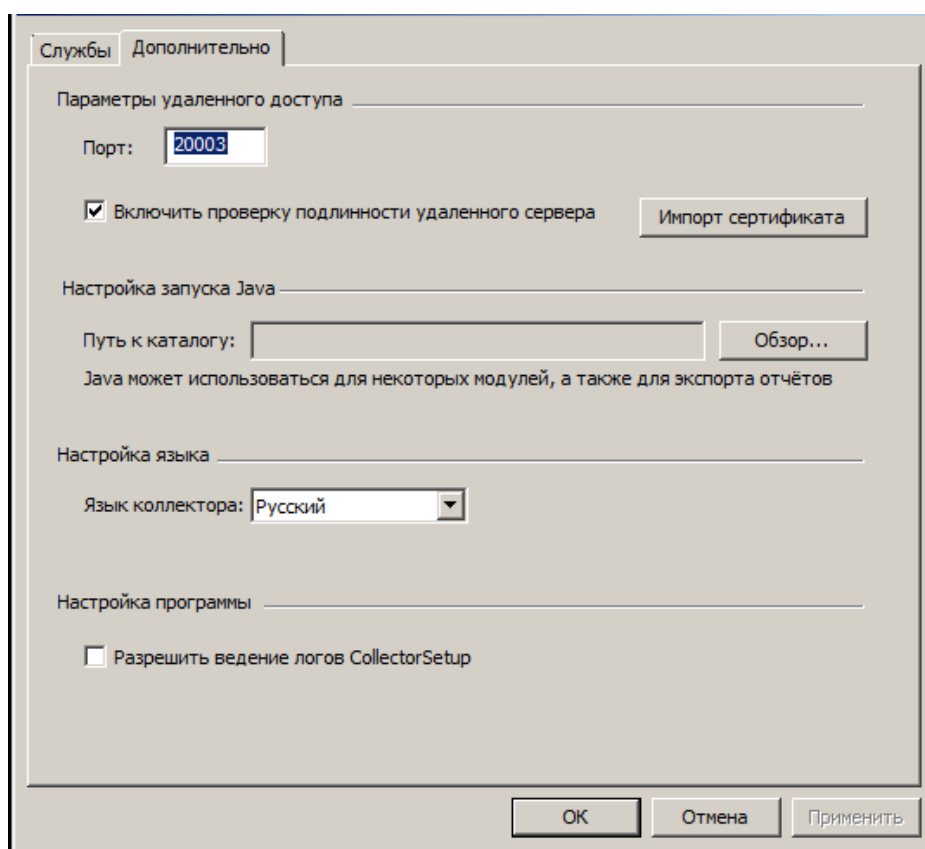


Рисунок 48 – Вкладка **Дополнительно**

2.6. Установка клиентской консоли комплекса

Для установки клиентской консоли ПК «Efros Config Inspector» v.4 следует запустить с используемого носителя установочного комплекта ПК «Efros Config Inspector» v.4 на исполнение файл *Efros Config Inspector Console 4.msi* (для x86-разрядных ОС) или *Efros Config Inspector Console 4.x64.msi* (для x64-разрядных ОС).

Откроется окно мастера установки клиентской консоли, в котором следует выбрать папку для установки консоли или оставить заданную по умолчанию (*C:\Program Files\EFROS Config Inspector 4*) и нажать кнопку **Далее**. На рисунке 49 приведен пример установки 86-разрядной версии клиентской консоли ПК «Efros Config Inspector» v.4 для 64-разрядных ОС.

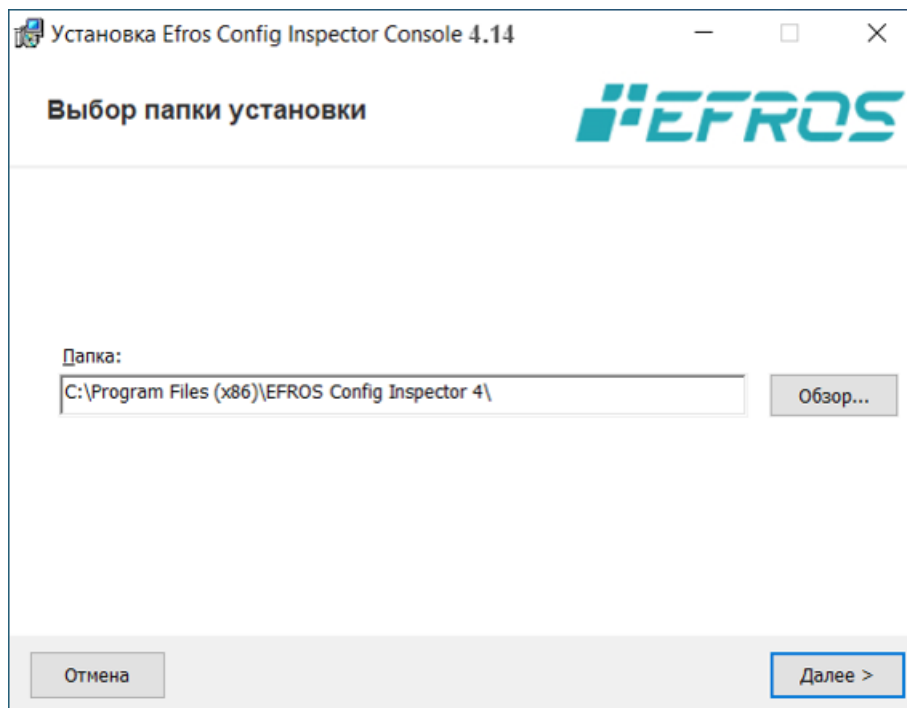


Рисунок 49 – Диалоговое окно выбора папки установки консоли

На следующем шаге, в окне **Параметры установки** (рис. 50), следует установить переключатели для выбора места расположения ярлыков вызова клиентской консоли: на **Рабочем столе** и/или в меню **Все программы**.

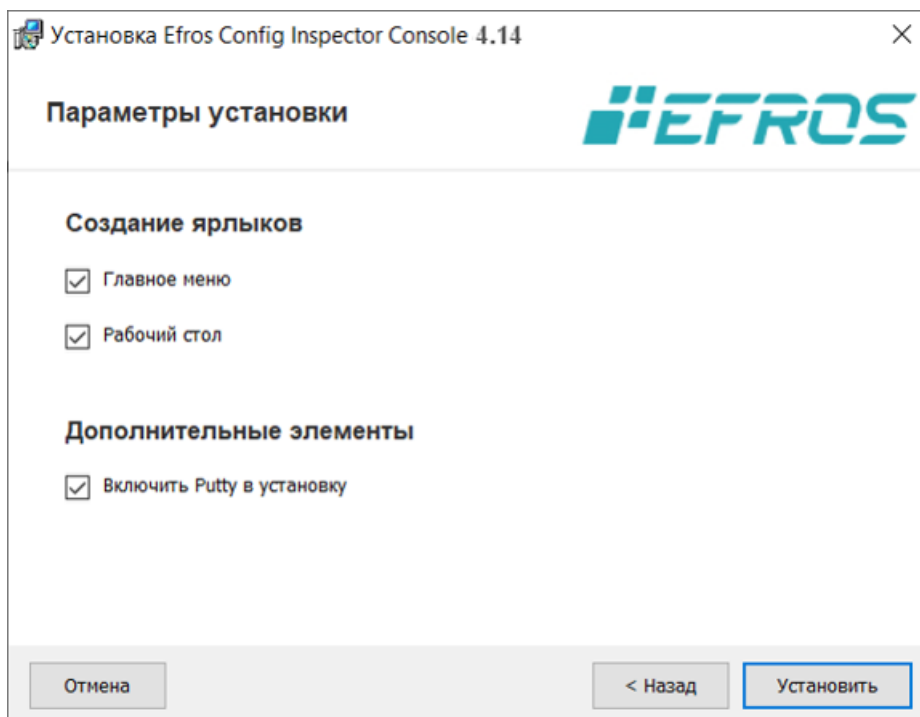


Рисунок 50 – Окно Параметры установки

В окне отметить параметр **Включить Putty в установку**, при необходимости установки этого клиента для соединения с его помощью с контролируемым комплексом сетевым оборудованием, и нажать кнопку **Установить** для запуска процесса инсталляции локальной консоли с заданными ранее параметрами.

Ход установки клиентской консоли программного комплекса будет отображаться в окне мастера установки (рис. 51).

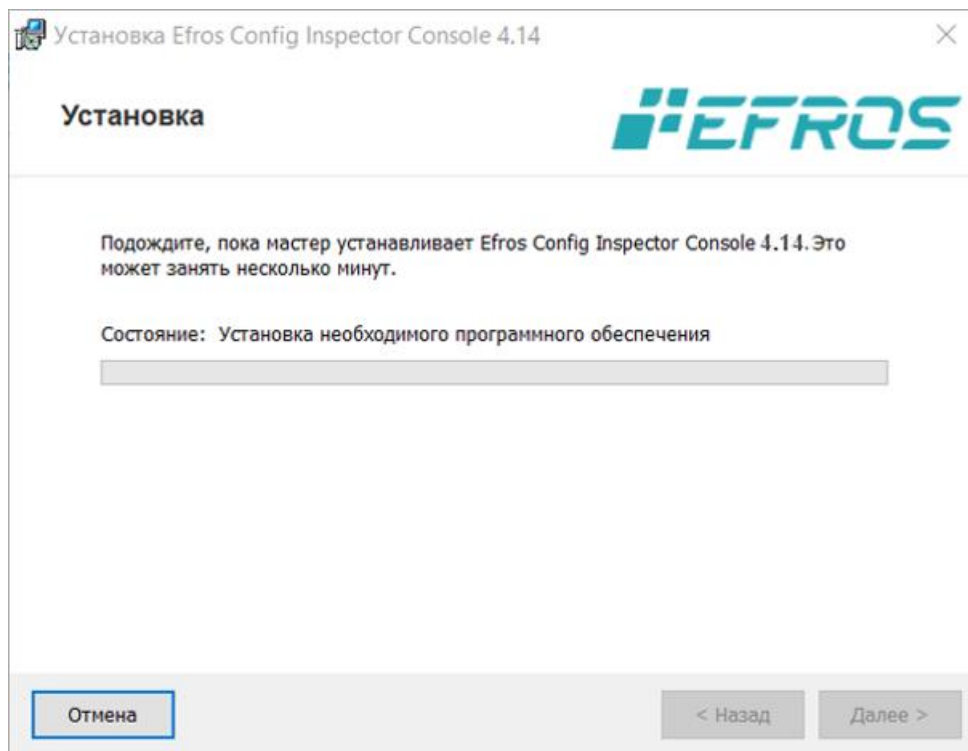


Рисунок 51 – Диалоговое окно процесса установки

По завершении установки откроется диалоговое окно завершения работы мастера установки (рис. 52), в котором следует нажать кнопку **Готово**:

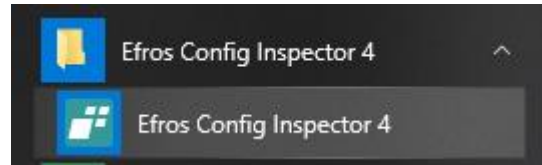


Рисунок 52 – Диалоговое окно завершения работы мастера установки

В результате установки клиентской консоли в выбранных в окне **Параметры установки** местах будут созданы ярлыки для запуска клиентской консоли. Соответственно запуск клиентской консоли ПК «Efros Config Inspector» v.4 можно будет выполнить, дважды щелкнув по пиктограмме ярлыка (рис. 53, а) на рабочем столе или выбрав в меню **Пуск** → **Все программы** → **Efros Config Inspector 4** → **Efros Config Inspector 4** (рис. 54, б).



а)



б)

Рисунок 53 – Запуск клиентской консоли ПК «Efros Config Inspector» v.4

3. Обновление компонентов комплекса

Обновление компонентов ПК «Efros Config Inspector» v.4 (серверная часть, клиентская консоль, windows-агент, внешние модули, коллекторы) выполняется отдельно при помощи инсталляторов новых версий компонентов комплекса.

Процесс обновления аналогичен описанному выше процессу установки компонентов комплекса (см. раздел 2 «Установка и настройка» настоящего Руководства). Предварительное удаление компонентов предыдущей версии ПК «Efros Config Inspector» v.4 не требуется.

Примечание – При повторной установке сервера ПК на ЭВМ под управлением ОС «Astra Linux SE» возможна ситуация, когда отсутствуют конфигурационные файлы сервера (*/etc/efrosci/config.ini*, */etc/efrosci/metrix.ini*, */etc/efrosci/krb_realm_map.conf*). Установка стандартным способом при этом будет заканчиваться ошибкой. В этом случае доступны следующие варианты устранения проблемы:

- полностью удалить сервер ПК с настройками, используя команду:

```
“sudo apt purge efrosci“
```

- установить сервер ПК с настройками по умолчанию, используя команду:

```
“sudo dpkg --install --force-confdef efrosci_****“
```

При обновлении серверной части комплекса обновлять сервер БД не требуется.

После обновления версии серверной части комплекса необходимо обязательно обновить и все установленные на ЭВМ администраторов и пользователей комплекса клиентские консоли.

После завершения работы мастера обновления сервера ПК запустится мастер настройки сервера ПК. Порядок настройки серверной части комплекса после обновления полностью аналогичен настройке сервера ПК после его первичной установки. Подробно процесс настройки рассмотрен в разделе 2 «Установка и настройка» настоящего Руководства.

Во время настройки серверной части комплекса возможно потребуются обновить структуру используемой БД комплекса (см. п. 3.1 «Обновление структуры базы данных»).

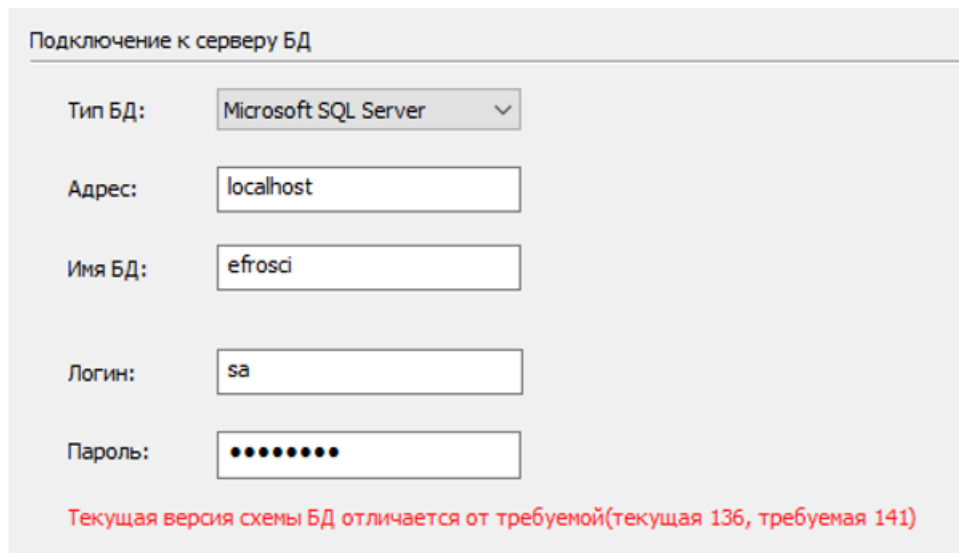
3.1. Обновление структуры базы данных

3.1.1. Обновление структуры базы данных при установке сервера ПК на ЭВМ под управлением ОС серии Windows

При необходимости обновления структуры БД в процессе установки и при настройке серверной части комплекса в окне настройки БД отобразится сообщение в соответствии с рис. 54.

Для обновления структуры БД следует нажать кнопку **Далее/Next**, в открывшемся окне с предложением сделать резервную копию БД – нажать кнопку **Да/Yes**. После чего последовательно откроются окна с сообщениями об успешном обновлении БД и успешном выполнении проверки соединения с существующей БД.

По окончании работы мастера настройки программного комплекса будет выполнен перезапуск службы серверной части комплекса (*EFROS CI Service 4*).



Подключение к серверу БД

Тип БД: Microsoft SQL Server

Адрес: localhost

Имя БД: efros_ci

Логин: sa

Пароль: ●●●●●●

Текущая версия схемы БД отличается от требуемой(текущая 136, требуемая 141)

Рисунок 54 – Запрос на обновление структуры БД

В случае отказа от обновления структуры БД (в окне-запросе нажата кнопка **Нет/No**) дальнейшая работа серверной части комплекса будет невозможна, поскольку запуск службы *EFROS CI Service 4* по окончании работы мастера настройки завершится ошибкой из-за несоответствия версий серверной части комплекса и используемой БД (рис. 55).

ВНИМАНИЕ: При отказе от операций обновления структуры используемой базы данных служба ПК не запустится!

Выполнение вышеуказанных операций по обновлению структуры БД программного комплекса возможно выполнить позже – из серверной консоли (**Пуск** → **Все программы** → **Efros Config Inspector 4** → **CI Server Setup**) во вкладке **База данных**.

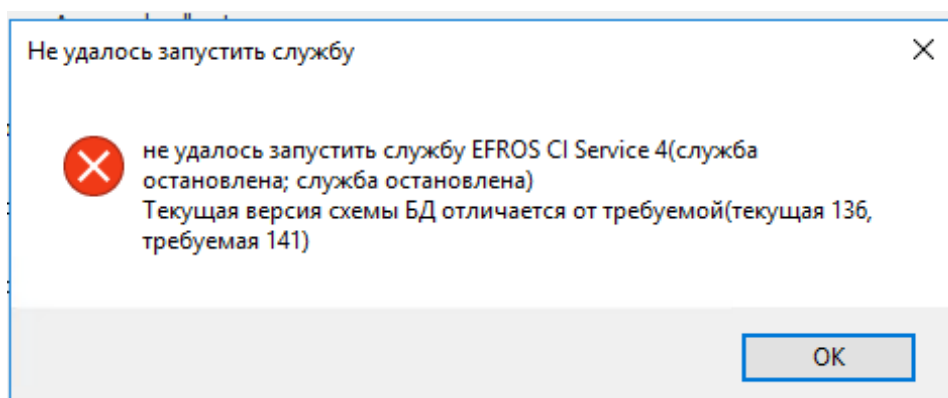


Рисунок 55 – Ошибка запуска службы серверной части комплекса

3.1.2. Обновление структуры базы данных при установке сервера ПК на ЭВМ под управлением ОС «Astra Linux SE», ОС «РЕД ОС»

Для обновления необходимо перейти в раздел **Настройки базы данных** и выбрать пункт **Изменение БД** (см. п. 2.3.2.2). Затем выбрать пункт **Подключиться к существующей базе данных**, выполнить команду **Соединить**.

В случае, когда версия БД на сервере отличается от требуемой, появится соответствующее уведомление с предложением обновить структуру БД (рис. 56).

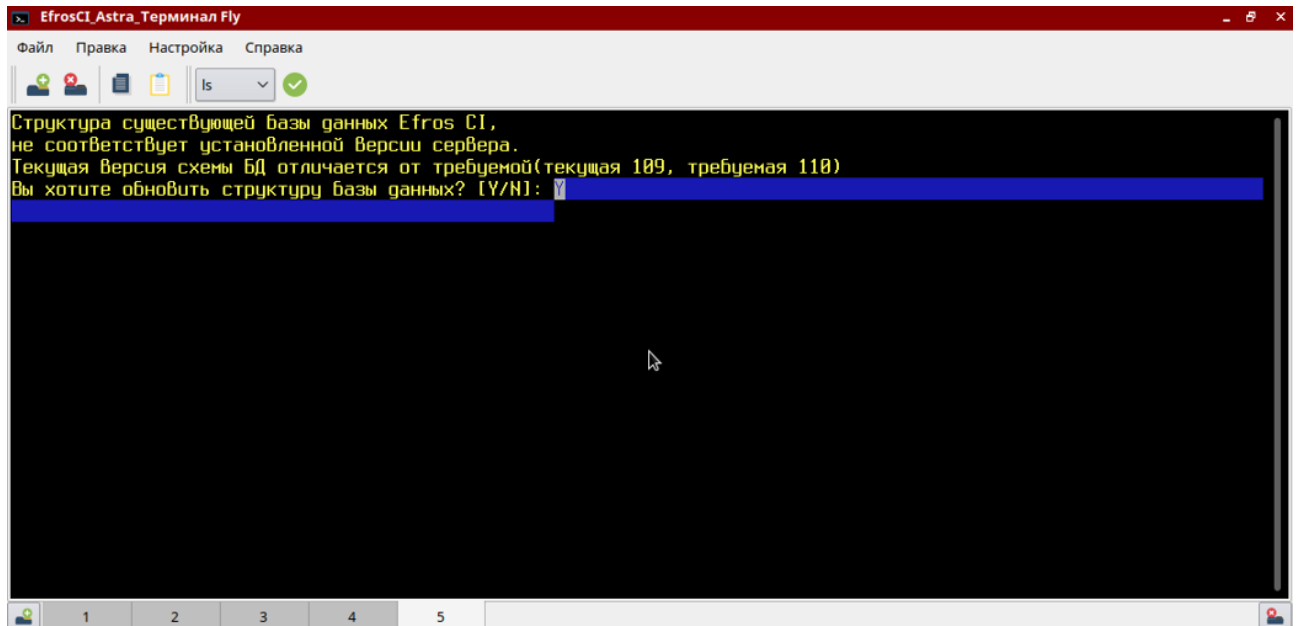


Рисунок 56 – Уведомление с предложением обновить структуру БД

В случае подтверждения появится уведомление о рекомендации сделать резервную копию БД (рис. 57).

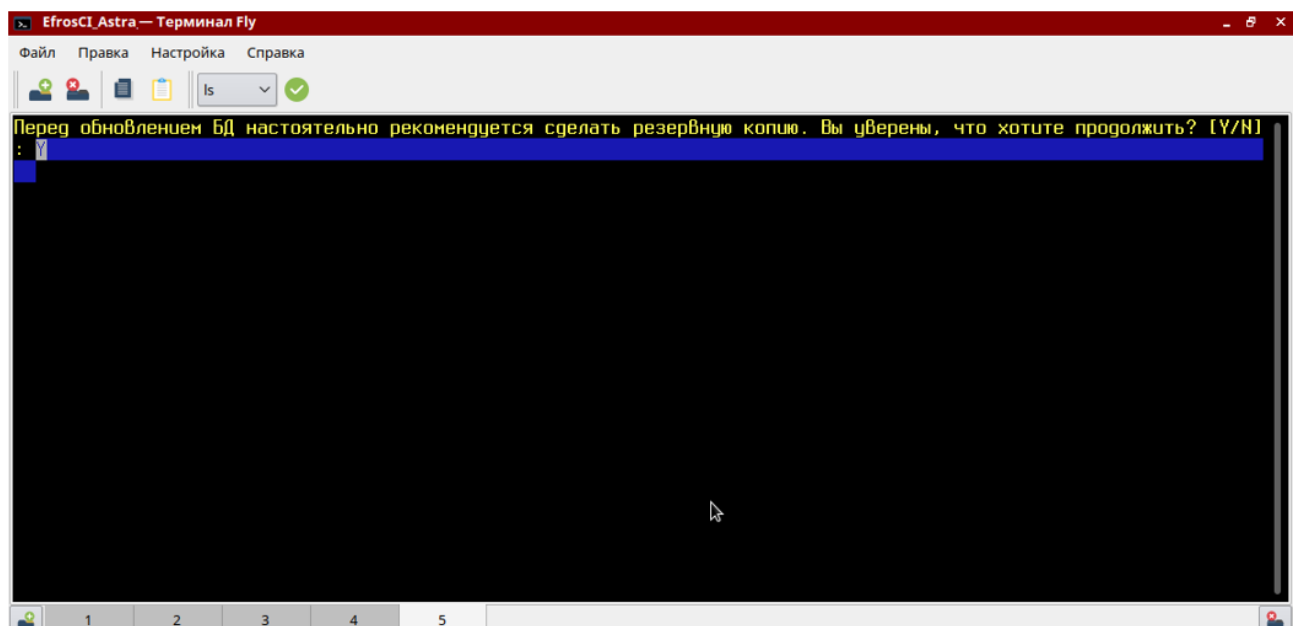


Рисунок 57 – Уведомление о рекомендации сделать резервную копию БД

В случае подтверждения начнется процесс обновления структуры БД. По завершении процесса обновления появится соответствующее сообщение "*Migration finished*" (рис. 58).

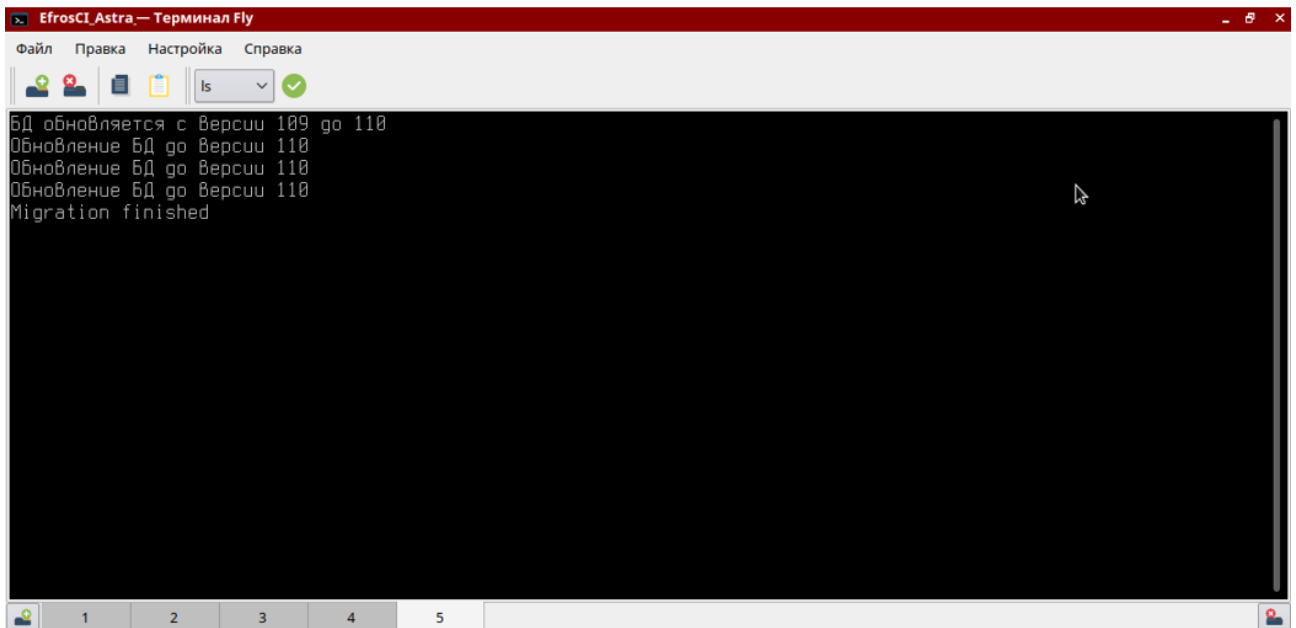


Рисунок 58 – Уведомление о завершении процесса обновления БД

Необходимо нажать клавишу ENTER для проверки структуры БД. По окончании в окне отобразится сообщение в соответствии с рисунком 59. Обновление структуры базы данных проведено успешно. При повторном нажатии клавиши ENTER произойдет переход в окно настроек подключения к БД.

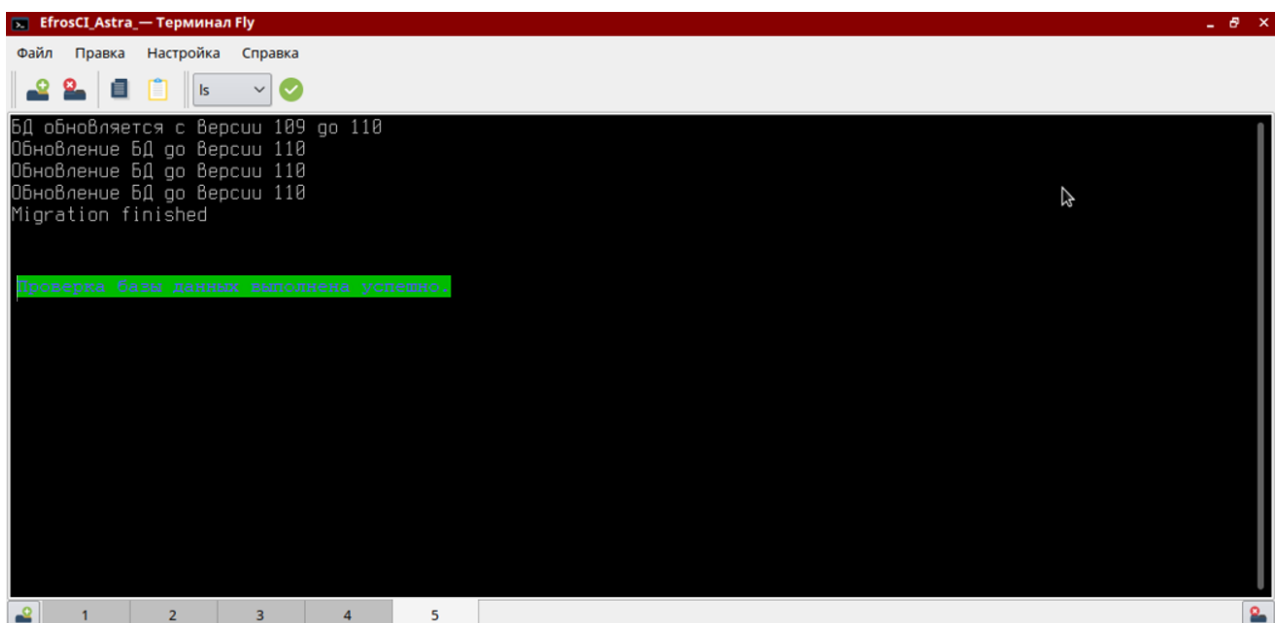


Рисунок 59 – Сообщение об успешном завершении проверки БД

3.2. Обновление внешних модулей

Для обновления внешних модулей необходимо предварительно из окна клиентской консоли комплекса загрузить на сервер ПК новую версию обновляемого модуля (подробнее о загрузке модулей см. в документе 643.72410666.00082-01 96 01-01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование»).

Затем в клиентской консоли в панели меню требуемого модуля нажать кнопку **Обновить** (↑) или нажать кнопку **Обновить все**, (↑), расположенную в форме управления внешними модулями, для обновления версий сразу всех установленных на сервере ПК внешних модулей. Начнется процесс обновления модуля, после окончания которого изменится информация о номере версии установленного модуля.

Перед обновлением внешнего модуля можно ознакомиться с информацией о внесенных в работу модуля изменениях (рис. 60) – для этого необходимо нажать кнопку **Сведения** (i), расположенную в строке с именем модуля.

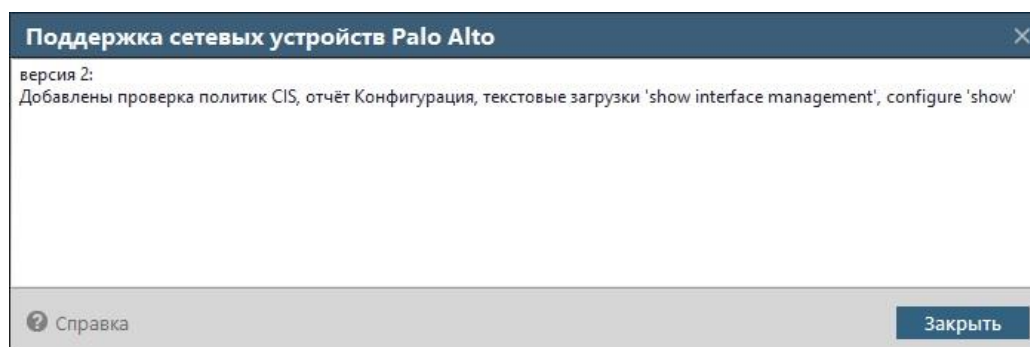


Рисунок 60 – Окно со списком внесенных в работу модуля изменений

4. Удаление программы

Для удаления установленных компонентов ПК «Efros Config Inspector» v.4 из операционной системы необходимо запустить компонент панели управления **Программы и компоненты** (**Пуск** → **Панель управления** → **Программы и компоненты**), выделить удаляемый компонент ПК «Efros Config Inspector» v.4 (серверная часть, клиентская консоль или windows-агент) и нажать кнопку **Удалить**. Далее следовать указаниям мастера удаления программы. В результате выбранный компонент комплекса будет удален из системы.

Для удаления сервера ПК, установленного на ЭВМ под управлением ОС «Astra Linux SE» необходимо использовать команду:

```
“sudo apt-get remove efrosci”
```

Для удаления сервера ПК, установленного на ЭВМ под управлением ОС «РЕД ОС», необходимо использовать команду:

```
“sudo yum remove efrosci”
```

Если в дальнейшем не планируется установка ПК «Efros Config Inspector» v.4 и пользователю для других нужд не требуется установленная СУБД, то последнюю (с соответствующими БД) можно удалить. Это можно выполнить стандартными приемами (из системного меню или из панели управления).

5. Настройка регистрации и просмотра событий

В ПК «Efros Config Inspector» v.4 реализована возможность фиксации событий, которые связаны с работой его служб и действиями пользователей (администратора и операторов) комплекса.

5.1. Просмотр журнала приложений Windows

События, связанные с запуском, остановкой служб ПК «Efros Config Inspector» v.4, автоматически фиксируются в системном журнале ОС Windows. Для их просмотра необходимо запустить консоль просмотра событий (**Панель управления** → **Администрирование** → **Просмотр событий**) и в системном журнале Windows (ветка **Журналы Windows** → **Система**) найти сообщения от источника *Service Control Manager* с кодом 7036 о запуске служб ПК «Efros Config Inspector».

Сообщения, связанные с ошибками, возникшими при запуске служб программного комплекса, фиксируются в журнале приложений ОС Windows (ветка **Журналы Windows** → **Приложение** в консоли просмотра событий), в качестве источника события в этом случае выступает служба, при запуске которой возникла ошибка (например, *Efros Config Inspector Service 4*).

В случае возникновения ошибок при запуске служб программного комплекса для определения причины ошибки необходимо в первую очередь просмотреть журнал приложений ОС Windows.

5.2. Просмотр лог-файлов

В лог-файлы, связанные с работой службы сервера программного комплекса, записывается информация о запуске и остановке службы, а также в основном отладочная информация, которая необходима для разработчиков программного комплекса.

5.2.1. Просмотр лог-файлов при установке сервера ПК на ЭВМ под управлением ОС серии Windows

Информация о запуске и остановке служб программного комплекса может записываться в лог-файлы работы соответствующей службы. Файлы аудита работы компонентов ПК «Efros Config Inspector» v.4 находятся в каталоге соответствующего компонента, который расположен в каталоге *C:\ProgramData\Efros Config Inspector4*. Так, лог-файлы работы серверной части комплекса находятся в папке *Server* вышеобозначенного каталога, внешних модулей – в папке *Server\Logs\Modules*, консоли серверной части – в папке *ServerSetup*, windows-агента комплекса – в папке *Agent*.

Для включения механизма записи событий, связанных с работой службы сервера комплекса, в лог-файлы необходимо установить соответствующий параметр на

вкладке **Службы** серверной консоли ПК «Efros Config Inspector» v.4 (см. п. 2.2.6.1 «Вкладка **Службы**» настоящего Руководства). Для регистрации событий работы серверной консоли в лог-файл необходимо установить соответствующий параметр на вкладке **Дополнительно** серверной консоли (см. п. 2.2.6.3 «Вкладка **Дополнительно**» настоящего Руководства). Для регистрации событий работы внешних модулей необходимо установить соответствующий параметр в настройках подключаемого модуля в клиентской консоли (см. документ «643.72410666.00082-01 96 01-01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование»).

5.2.2. Просмотр лог-файлов при установке сервера ПК на ЭВМ под управлением ОС «Astra Linux SE», ОС «РЕД ОС»

Информация о запуске и остановке служб программного комплекса может записываться в лог-файлы работы соответствующей службы. Файлы аудита работы компонентов комплекса находятся в каталоге соответствующего компонента, который расположен в каталоге `/var/log/efros-ci`. Так, лог-файлы работы серверной части комплекса находятся в папке `Server` вышеобозначенного каталога, внешних модулей – в папке `Server\Logs\Modules`.

Для включения механизма записи событий, связанных с работой службы сервера комплекса, в лог-файлы необходимо установить соответствующий параметр в разделе **Настройка службы сервера** серверной консоли комплекса (см. п. 2.3.2.1 «Раздел Настройка службы сервера» настоящего Руководства). Для регистрации событий работы серверной консоли в лог-файл необходимо установить соответствующий параметр в разделе **Дополнительно** серверной консоли (см. п. 2.3.2.3 «Раздел **Дополнительно**» настоящего Руководства). Для регистрации событий работы внешних модулей необходимо установить соответствующий параметр в настройках подключаемого модуля в клиентской консоли (см. документ «643.72410666.00082-01 96 01-01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование»).

5.3. Просмотр событий в клиентской консоли

Пользователь в окне клиентской консоли программного комплекса может просмотреть список всех зафиксированных событий. В разделе **События** (рис. 61) содержится список 1000 последних зафиксированных событий для всех устройств – журнал действий пользователей, в котором регистрируется информация о:

- подключении пользователей к серверной части комплекса и отключении от него;
- добавлении/изменении/удалении в списке устройств комплекса устройства/группы устройств;
- запуске заданий и результатах их выполнения на контролируемых устройствах;
- подтверждении изменений конфигурации контролируемых устройств.

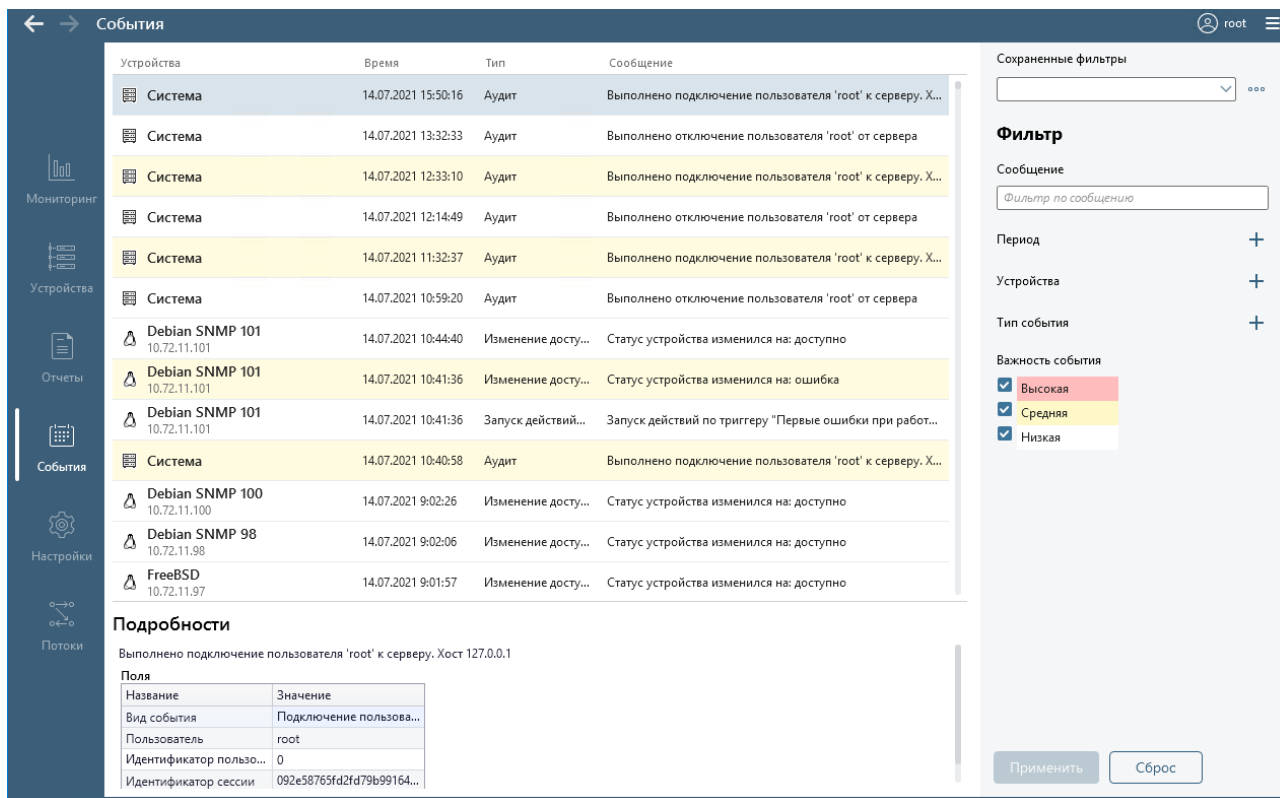


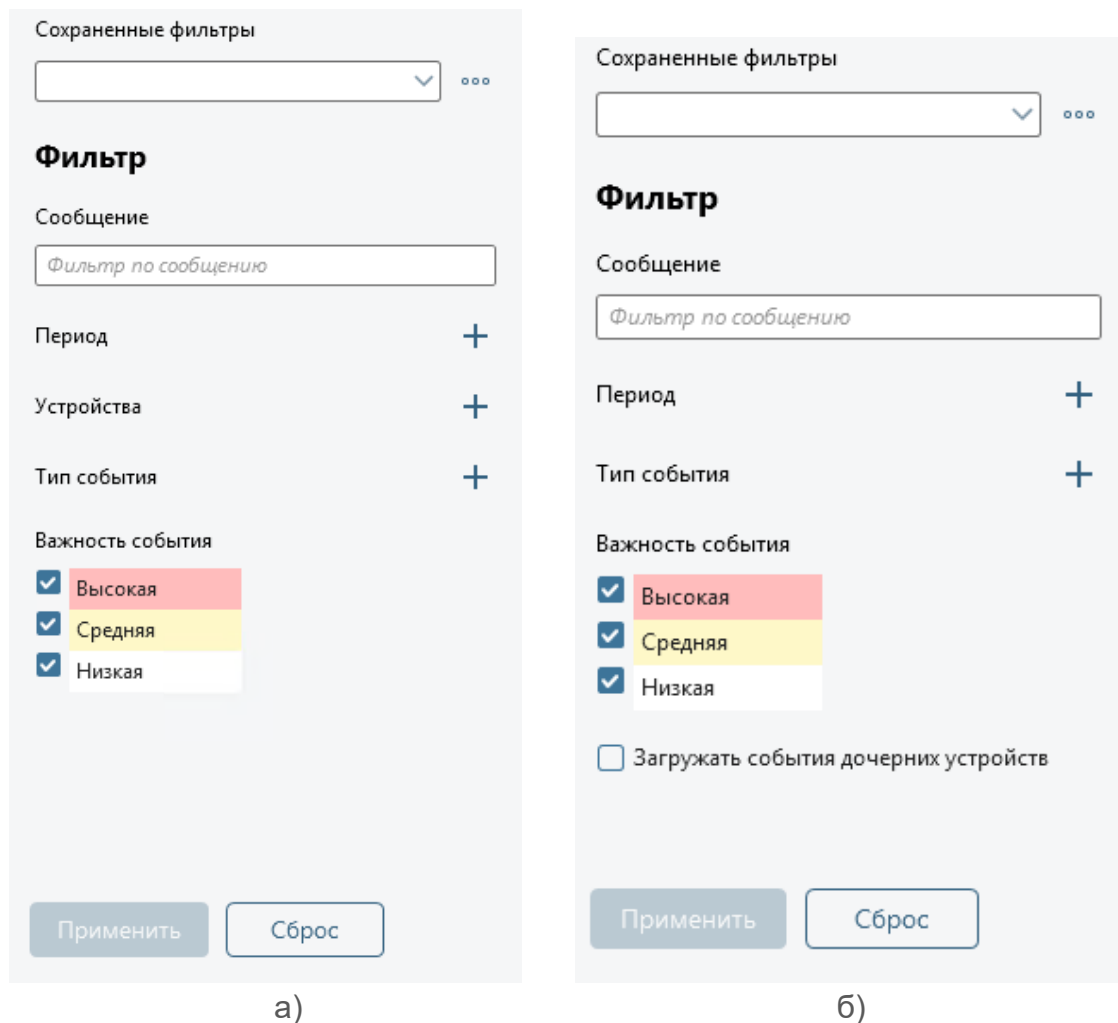
Рисунок 61 – Вкладка раздела **События**, клиентской консоли

Кроме того, во вкладке **События** раздела **Устройства** пользователю доступен для просмотра список из 1000 последних событий, которые произошли на устройстве, выбранном в панели списка устройств.

Для удобства просмотра журнала событий в разделе **События** и во вкладке **События** раздела **Устройства** пользователь может группировать записи по категориям (устройству, времени, типу события, сообщению).

Для возможности отображения в журнале событий только сообщений, которые соответствуют определенному критерию, необходимо воспользоваться фильтром сообщений в панели **Фильтр**. На рис. 62 (а) приведена панель **Фильтр** для раздела **События**, на рис. 63 (б) – для вкладки **События** раздела **Устройства**.

Существует возможность выборки событий по **Сообщению**, **Времени**, **Устройствам** (только в разделе **События**), **Типу события** и/или **Важности события**, а также включить/отключить параметр **Загружать события с дочерних устройств** (только во вкладке **События** раздела **Устройства**). Включенный параметр **Загружать события с дочерних устройств** позволяет отобразить список событий для устройств, которые входят в группу на сервере ПК (если в панели устройств выделена группа) или в состав устройства, контролируемого комплексом (например, список виртуальных машин на сервере управления VMware vCenter).

Рисунок 62 – Панель **Фильтр**

Заданные параметры фильтрации возможно сохранить для применения к другим устройствам, зарегистрированным в ПК «Efros Config Inspector» v.4. Для сохранения параметров фильтрации необходимо в поле **Сохраненные фильтры** после выбора и настройки параметров нажать кнопку (☰) и выбрать в выпадающем меню **Сохранить как**. После чего в появившемся окне **Сохранить как** ввести имя фильтра и нажать кнопку **Сохранить**. Сохраненный фильтр появится в выпадающем списке поля **Сохраненные фильтры**. После чего возможно редактирование, переименование и удаление созданного фильтра. Для редактирования или переименования сохраненного фильтра необходимо выбрать существующий фильтр в поле **Сохраненные фильтры**, изменить необходимые параметры и нажать кнопку (☰). В раскрывшемся меню выбрать соответствующее действие для сохранения внесенных изменений. Для удаления фильтра – выбрать в меню пункт **Удалить**.

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

1) В поле **Сообщение** панели **Фильтр** указать фрагмент сообщения, по которому должны быть отобраны события.

2) Нажать кнопку **Применить**.

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

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

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

Для фильтрации событий по устройствам пользователю необходимо выполнить следующие действия:

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

2) Выбрать в открывшемся окне **Выбор устройств** (рис. 63) установкой флагов требуемые устройства.

Примечание – В окне выбора устройств доступен поиск устройств и фильтрация списка по признаку *Выбрано* и типу устройств. Окно фильтрации открывается по кнопке **Фильтр (T)**. После установки в поле окна **Выбрано** флага, в списке отображаются только выбранные группы устройств/устройства. Отмена фильтрации выполняется по нажатию в окне ссылки **Сбросить фильтр**.

3) Нажать кнопку **Применить**.

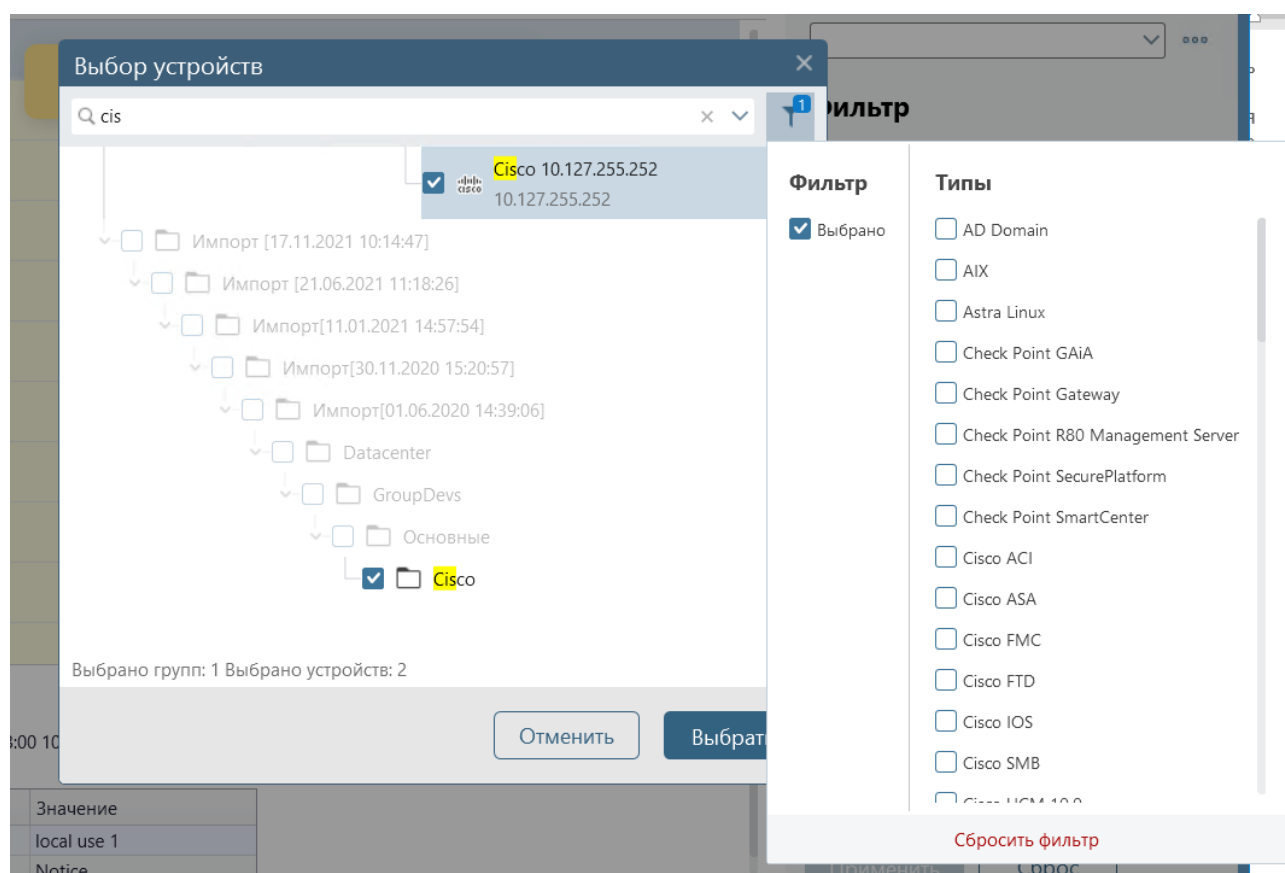


Рисунок 63 – Окно **Выбор устройств**

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

- 1) В группе полей *Тип события* фильтра нажать кнопку **Добавить** (+).
- 2) Выбрать в списке отобразившегося поля тип события, для которого задается условие фильтрации (рис. 64).

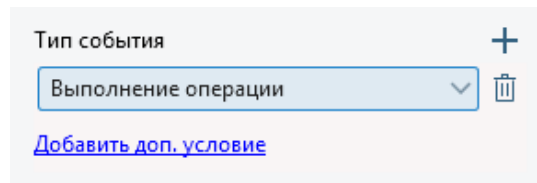
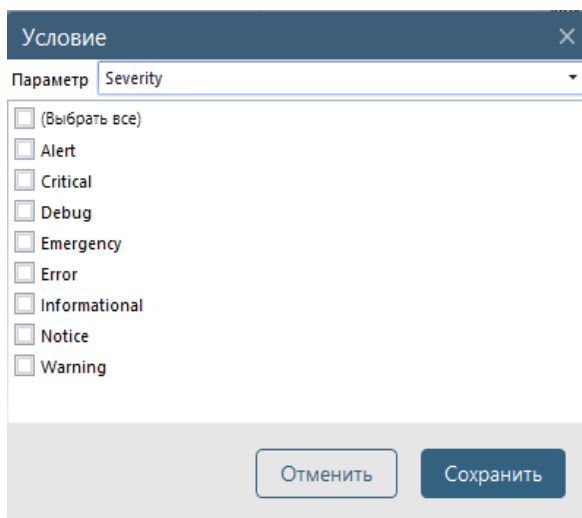


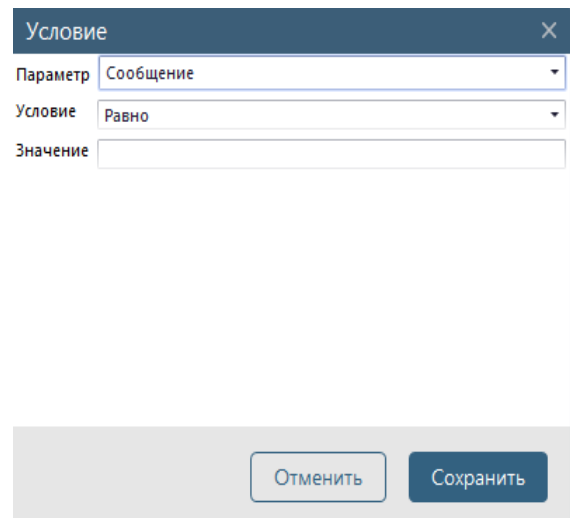
Рисунок 64 – Панель **Фильтр** с выбранным типом события

3) Задать, при необходимости, дополнительные условия отбора событий для выбранного типа:

- нажать ссылку **Добавить доп.условие**;
- в открывшемся окне **Условие** (рис. 65) из раскрывающегося списка поля **Параметр** выбрать событие, для которого задается условие фильтрации;
- в зависимости от значения выбранного события в окне **Условие** установить необходимые переключатели (рис. 66, а) или заполнить поля выбора условия и указать значения этого условия фильтрации для выбранного события (рис. 66, б);
- нажать кнопку **Сохранить**.



а)



б)

Рисунок 65 – Окно **Условие** в режиме выбора условия и задания значения условия фильтрации для выбранного параметра

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

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

- 5) При необходимости, добавить другие типы событий, повторив шаги 1 – 4.
- 6) Отменить ошибочно выбранные типы событий и заданные для них дополнительные условия, нажав соответствующие им кнопки **Удалить** (🗑️).
- 7) Нажать кнопку **Применить**.

В панели списка событий отобразится список событий, которые удовлетворяют заданным условиям фильтрации.

Для отображения в журнале сообщений только определенной степени важности необходимо установить флаги в полях группы *Важность события* и нажать кнопку **Применить**. Существует возможность фильтрации событий по трем степеням важности: **Высокая**, **Средняя** и **Низкая**.

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

6. Резервирование данных комплекса

Регулярное резервирование данных ПК «Efros Config Inspector» v.4 позволит сохранить максимум информации при возникновении внезапных сбоев в работе сервера ПК (например, при непредвиденном отключении электричества). Кроме того, резервирование необходимо выполнять перед внесением изменений в настройки программного комплекса, перед его обновлением, а также перед переносом на другой сервер.

Резервные копии программного комплекса могут понадобиться в следующих случаях:

- 1) Для восстановления работы комплекса после повреждения БД. Причинами повреждения БД могут быть:
 - аварийное отключение питания сервера БД;
 - неисправность жесткого диска и пр.
- 2) Для переноса серверной части программного комплекса на другую ЭВМ.

Для обеспечения бесперебойной работы сервера ПК «Efros Config Inspector» v.4 (быстрого восстановления работы в случае возникновения сбоев) рекомендуется осуществлять резервирование данных программного комплекса на регулярной основе.

6.1. Операции с БД

Операции резервирования и восстановления базы данных ПК «Efros Config Inspector» v.4 проводятся непосредственно на сервере баз данных с использованием встроенных средств используемой СУБД.

6.1.1. Создание резервной копии БД

Непосредственно перед резервированием используемой БД необходимо остановить службу сервера ПК «Efros Config Inspector» v.4 (*Efros Config Inspector Service 4*).

Для остановки службы сервера на ОС серии Windows необходимо открыть окно настройки серверной части комплекса с помощью меню **Пуск** на панели задач (выбрать **Все программы** → **Efros Config Inspector4** → **CIServerSetup**) и во вкладке **Службы** серверной консоли (см. рис. 18) нажать кнопку **Стоп**.

Для остановки службы сервера на ОС «Astra Linux SE», ОС «РЕД ОС» – запустить утилиту настройки сервера командой:

```
“sudo efrosci-settings”
```

Перейти в раздел **Настройки службы сервера** и остановить службу сервера командой **Стоп**. После этого выйти из утилиты настройки сервера.

Ниже будут рассмотрены способы резервирования БД ПК «Efros Config Inspector» v.4 для всех поддерживаемых СУБД.

После завершения выполнения операции резервирования – выполнить запуск службы сервера ПК «Efros Config Inspector» v.4.

СУБД MS SQL Server, функционирующая на ОС серии Windows

Для резервирования БД программного комплекса при использовании СУБД MS SQL Server необходимо запустить командную оболочку **Windows PowerShell** и выполнить команду:

```
Backup-SqlDatabase -ServerInstance <имя сервера СУБД или его ip-адрес>\<имя экземпляра СУБД> -Database <имя используемой БД> -BackupAction Database
```

В результате в директории с установленной СУБД (по умолчанию, *C:\Program Files\Microsoft SQL Server\MSSQL11.< имя экземпляра СУБД >MSSQL\Backup*) будет создана резервная копия БД программного комплекса.

СУБД MySQL, функционирующая на ОС серии Windows

Для резервирования БД программного комплекса при использовании СУБД MySQL необходимо запустить интерпретатор командной строки **cmd** и последовательно выполнить команды:

- 1) для перехода в каталог размещения утилит СУБД MySQL:

```
cd <каталог установки СУБД MySQL>
```

например:

```
cd "C:\Program Files\MySQL\MySQL Server 5.5\bin"
```

- 2) для создания резервной копии БД:

```
mysqldump --max_allowed_packet=512M -u[username] -p[password] --databases [имя базы данных] >[имя_выходного_файла.sql]
```

например, (пользователь **root**, пароль **root**, база данных **efros_4**):

```
mysqldump --max_allowed_packet=512M -uroot -proot --databases efrosci_4 > c:\efrosci.sql
```

В результате в указанном каталоге (в примере – в корне диска C:\) будет создана резервная копия БД программного комплекса с заданным именем (в примере – *efrosci.sql*).

СУБД PostgreSQL, функционирующая на ОС серии Windows

Для резервирования БД программного комплекса при использовании СУБД PostgreSQL на ЭВМ под управлением ОС серии Windows необходимо запустить интерпретатор командной строки **cmd** и последовательно выполнить команды:

- 1) Для перехода в каталог размещения утилит СУБД PostgreSQL:

```
cd <каталог установки СУБД PostgreSQL>
```

например:

```
cd "C:\Program Files\PostgreSQL\9.4\bin"
```

2) Для создания резервной копии БД:

```
pg_dump -U [username] -f <имя_выходного_файла> [имя базы данных]
```

например, (пользователь **postgres**, база данных **efros_4**):

```
pg_dump -U postgres -f c:\efrosci_4.bak efrosci_4
```

В результате в указанном каталоге (в примере – в корне диска C:\) будет создана резервная копия БД программного комплекса с заданным именем (в примере – *efrosci_4.bak*).

СУБД «Jatoba», функционирующая на ОС «Astra Linux SE», ОС «РЕД ОС»

Администратор ПК «Efros Config Inspector» v.4 осуществляет резервирование СУБД «Jatoba» путем ее выгрузки в формат скрипта. Выгрузка осуществляется при помощи терминала, вызываемого из меню **Пуск (Пуск → Системные → Терминал)** либо нажатием комбинации клавиш **ALT+T**.

Скрипт представляет собой текстовый файл, содержащий SQL-команды, необходимые для воссоздания БД до состояния на момент создания скрипта.

Все команды по резервному копированию администратор выполняет под служебной учетной записью «**Postgres**», переход к служебной учетной записи осуществляется командой:

```
"sudo su postgres"
```

Выгрузка БД «Jatoba» в формате скрипта осуществляется при помощи встроенной утилиты «**pg_dump**».

Для выгрузки СУБД «Jatoba» в формате скрипта администратору необходимо в консоли **fly** ввести команду:

```
"pg_dump «Имя БД» > BDjatoba.sql"
```

СУБД PostgreSQL, функционирующая на ОС «Astra Linux SE», ОС «РЕД ОС»

Действия администратора ПК «Efros Config Inspector» v.4 по резервированию СУБД PostgreSQL, функционирующей на ЭВМ под управлением ОС «Astra Linux SE», ОС «РЕД ОС» аналогичны действиям, приведенным по резервированию СУБД «Jatoba», функционирующей на ОС «Astra Linux SE», ОС «РЕД ОС».

6.1.2. Восстановление БД программного комплекса из резервной копии

Непосредственно перед восстановлением БД необходимо остановить службу сервера ПК «Efros Config Inspector» v.4 (*Efros Config Inspector Service 4*).

Для остановки службы сервера на ОС серии Windows необходимо открыть окно настройки серверной части комплекса с помощью меню **Пуск** на панели задач

(выбрать **Все программы** → **Efros Config Inspector4** → **CIServerSetup**) и во вкладке **Службы** серверной консоли (см. рис. 18) нажать кнопку **Стоп**.

Для остановки службы сервера на ОС «Astra Linux SE», ОС «РЕД ОС» – запустить утилиту настройки сервера командой:

```
“sudo efrosci-settings”
```

Перейти в раздел **Настройки службы сервера** и остановить службу сервера командой **Стоп**. После этого выйти из утилиты настройки сервера.

Ниже будут рассмотрены способы восстановления БД ПК «Efros Config Inspector» v.4 для всех поддерживаемых СУБД.

После завершения выполнения операции восстановления – выполнить запуск службы сервера ПК «Efros Config Inspector» v.4.

СУБД MS SQL Server, функционирующая на ОС серии Windows

Для восстановления БД комплекса при использовании СУБД MS SQL Server необходимо запустить командную оболочку **Windows PowerShell** и выполнить команду:

```
Restore-SqlDatabase -ServerInstance <имя/ip-адрес сервера СУБД>\<имя экземпляра СУБД> -Database <имя используемой БД> -BackupFile <путь к файлу резервной копии> -RestoreAction Database –ReplaceDatabase
```

В результате выполнения этой команды на сервере БД будет восстановлена БД программного комплекса из созданной ранее резервной копии.

СУБД MySQL, функционирующая на ОС серии Windows

Для восстановления БД комплекса при использовании СУБД MySQL необходимо запустить интерпретатор командной строки **cmd** и последовательно выполнить команды:

- 1) Для перехода в каталог размещения утилит СУБД MySQL:

```
cd <каталог установки СУБД MySQL>
```

например:

```
cd "C:\Program Files\MySQL\MySQL Server 5.5\bin"
```

- 2) Для восстановления БД из резервной копии:

```
mysql -u[username] -p[password] [имя базы данных]< [backup.sql]
```

например (пользователь **root**, пароль **root**, база данных **efros_4**):

```
mysql –u root –p root efrosci < c:\efrosci.sql
```

В результате выполнения этих команд на сервере БД будет восстановлена (создана) БД программного комплекса из созданной ранее резервной копии (в примере – *efrosci.sql*).

СУБД PostgreSQL, функционирующая на ОС серии Windows

Для восстановления БД комплекса при использовании СУБД PostgreSQL, функционирующей на ЭВМ под управлением ОС серии Windows, необходимо запустить интерпретатор командной строки **cmd** и последовательно выполнить команды:

- 1) Для перехода в каталог размещения утилит СУБД PostgreSQL:

```
cd <каталог установки СУБД PostgreSQL>
```

например:

```
cd "C:\Program Files\PostgreSQL\9.4\bin"
```

- 2) Для восстановления БД из резервной копии:

```
psql -U [username] [имя базы данных] < <имя_архивного_файла>
```

например, (пользователь **postgres**, база данных **efros_4**):

```
psql -U postgres -d efrosci_4_14_100 -f efrosci_4_14_100.bak
```

В результате выполнения этих команд, на сервере БД будет восстановлена БД программного комплекса из созданной ранее резервной копии (в примере – *efrosci_4.bak*).

СУБД «Jatoba», функционирующая на ОС «Astra Linux SE», ОС «РЕД ОС»

Администратор ПК «Efros Config Inspector» v.4 осуществляет восстановление СУБД «Jatoba» путем ее загрузки из созданного ранее файла формата скрипта. Восстановление осуществляется при помощи терминала, вызываемого из меню **Пуск (Пуск → Системные → Терминал)** либо нажатием комбинации клавиш **ALT+T**.

Скрипт представляет собой текстовый файл, содержащий SQL-команды, необходимые для воссоздания БД до состояния на момент создания скрипта.

Все команды по восстановлению администратор выполняет под служебной учетной записью **Postgres**, переход к служебной учетной записи осуществляется командой:

```
“sudo su postgres”
```

Для восстановления СУБД «Jatoba» из созданного ранее скрипта администратору в терминале fly необходимо:

- 1) Создать новую базу данных в СУБД командой:

```
“createdb <новое имя БД>”
```

- 2) Выполнить команду:

```
“psql -d «новое имя БД» -f BDjatoba.sql»”
```

СУБД PostgreSQL, функционирующая на ОС «Astra Linux SE», ОС «РЕД ОС»

Действия администратора ПК «Efros Config Inspector» v.4 по восстановлению СУБД PostgreSQL, функционирующей на ЭВМ под управлением ОС «Astra Linux SE», ОС «РЕД ОС» аналогичны действиям, приведенным по восстановлению СУБД «Jatoba», функционирующей на ОС «Astra Linux SE», ОС «РЕД ОС».

6.1.3. Миграция БД программного комплекса

Перенос используемой программным комплексом БД в другую СУБД либо в такую же (например, с MySQL в MySQL на том же сервере, но под другим именем, или на другом сервере с аналогичным именем) может потребоваться, например, при переходе на другой сервер БД либо по другим организационным причинам.

6.1.3.1. Перенос БД программного комплекса на ЭВМ под управлением ОС серии Windows

Для переноса используемой комплексом БД на ЭВМ под управлением ОС серии Windows администратору комплекса необходимо выполнить следующие действия:

- 1) Запустить серверную консоль ПК «Efros Config Inspector» v.4.
- 2) Перейти во вкладку **База данных** и нажать кнопку **Миграция БД**.
- 3) В открывшемся мастере переноса БД (рис. 66) проверить корректность введенных параметров и нажать кнопку **Далее**.

Перенос базы данных Efros Config Inspector (шаг 1 из 6)

Введите параметры БД, которую вы хотите перенести

Тип БД: MySQL

Адрес: localhost

Имя БД: lml11

Логин: root

Пароль: ●●●●●●

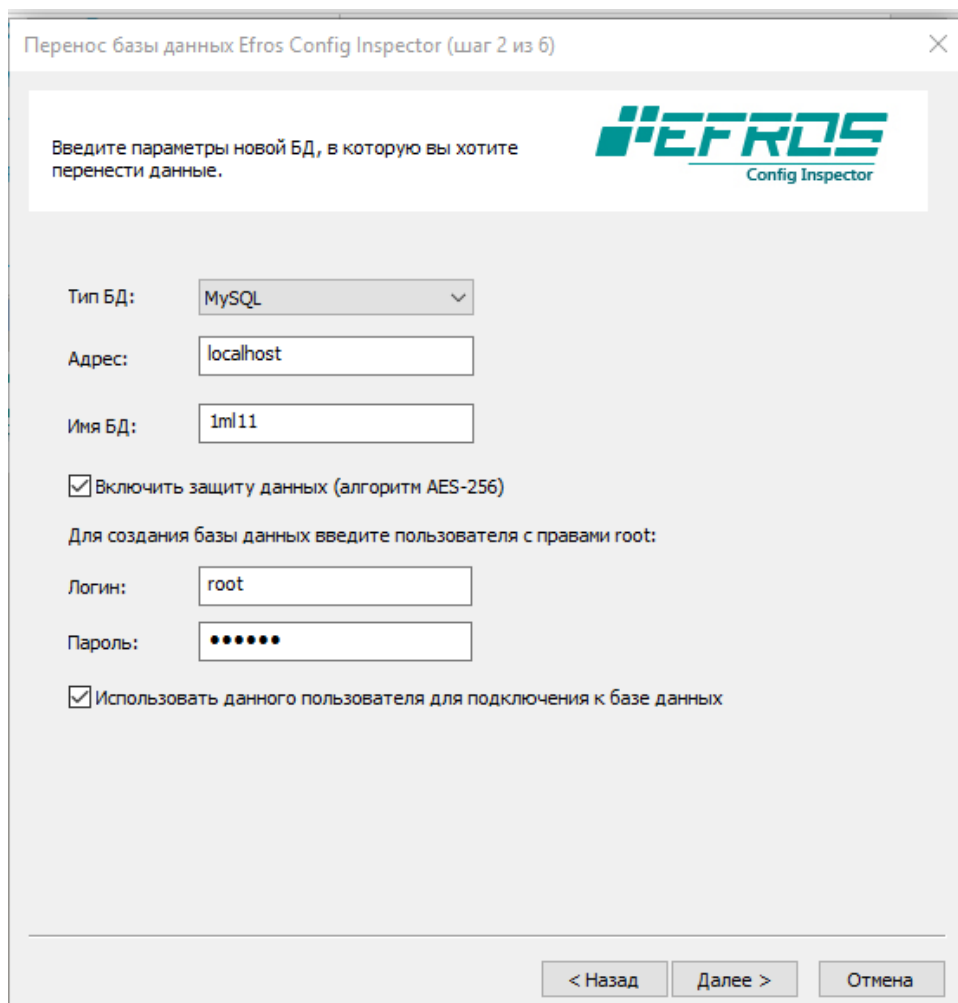
Проверка базы данных выполнена успешно.

< Назад Далее > Отмена

Рисунок 66 – Окно корректировки параметров подключения к серверу БД

4) В открывшемся окне настройки подключения сервера ПК к новому серверу БД (рис. 67) ввести в поля ввода необходимые параметры создания БД комплекса на новом сервере БД и нажать кнопку **Далее**.

Если в окно настройки подключения сервера ПК к новому серверу БД введены неверные данные, откроется окно с описанием ошибки подключения к СУБД (рис. 68). Нажмите кнопку ОК в окне с описанием ошибки и откорректируйте введенные параметры подключения сервера ПК к СУБД.



Перенос базы данных Efros Config Inspector (шаг 2 из 6)

Введите параметры новой БД, в которую вы хотите перенести данные.

Тип БД: MySQL

Адрес: localhost

Имя БД: 1ml11

Включить защиту данных (алгоритм AES-256)

Для создания базы данных введите пользователя с правами root:

Логин: root

Пароль: ●●●●●●

Использовать данного пользователя для подключения к базе данных

< Назад Далее > Отмена

Рисунок 67 – Окно ввода параметров создания новой БД

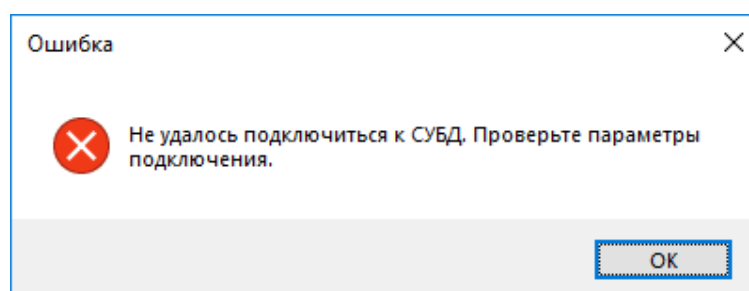


Рисунок 68 – Информационное сообщение об ошибке подключения к серверу БД

В результате откроется окно, в котором приведены параметры подключения сервера ПК к текущей и новой БД (рис. 69). Внимательно ознакомьтесь с приведенными

параметрами и, в случае их корректности, нажмите кнопку **Далее** для старта процедуры копирования текущей БД комплекса.

Если Вас не устраивает имя новой БД комплекса, нажмите кнопку **Назад** для перехода в диалоговое окно ввода параметров подключения сервера ПК к новой СУБД (см. пример на рис. 68).

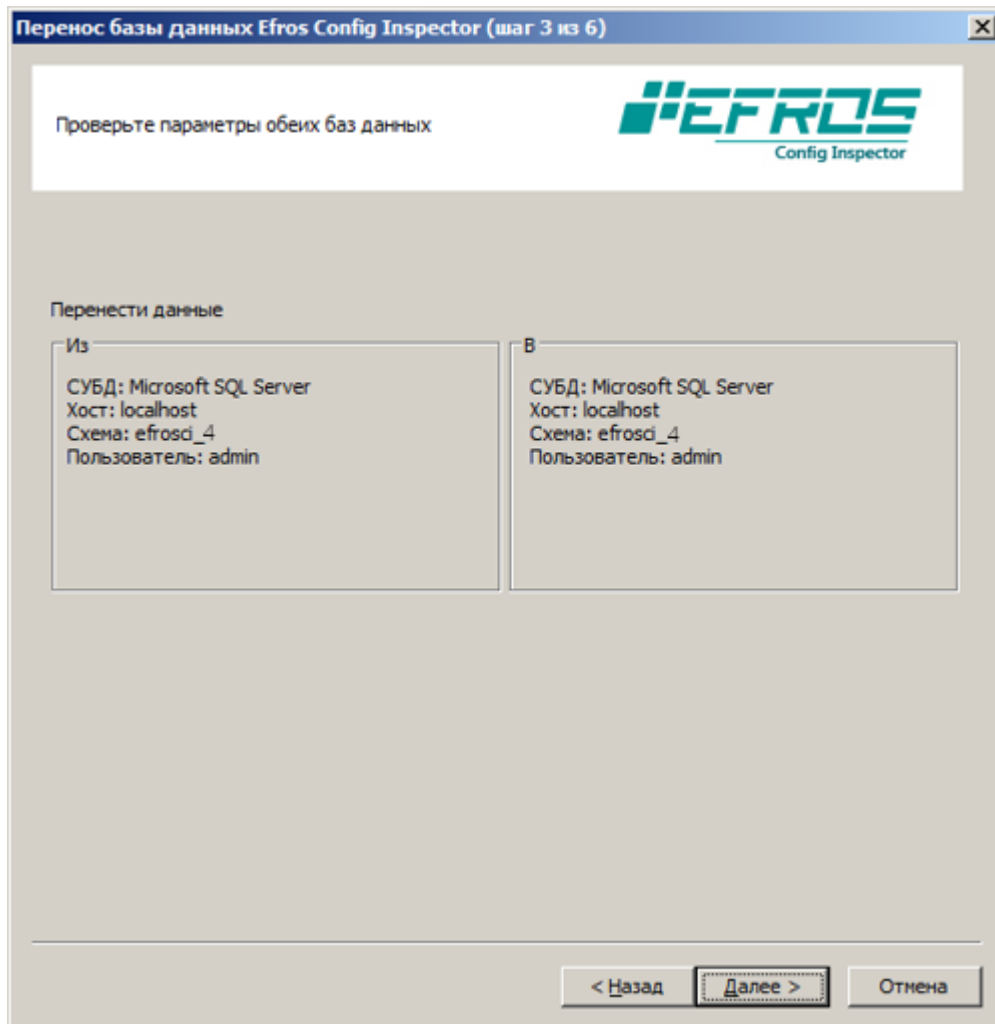


Рисунок 69 – Окно ввода параметров создания новой базы данных

5) Ход процедуры копирования БД ПК «Efros Config Inspector» v.4 будет отображаться в окне мастера переноса БД. После ее успешного окончания станет активной кнопка **Далее/Next**. При нажатии кнопки в окне (рис. 70) отобразится сводная информация по переносу и шифрованию БД, а также включенный по умолчанию параметр *Подключать Efros к новой БД*.

6) При использовании шифрования – выполнить экспорт ключа, нажав кнопку **Сохранить ключ**.

7) Нажать кнопку **Далее/Next**. В окне отобразится сообщение об успешном завершении проверки БД.

Примечание – Если одна из БД зашифрована, а шаг 6 по сохранению ключа не выполнен, то после нажатия кнопки **Далее/Next** откроется окно с предупреждением в соответствии с рис. 71. Для возврата к предыдущему окну и сохранению ключа

необходимо нажать кнопку **Нет/No**, для продолжения без сохранения ключа – нажать кнопку **Да/Yes** (ключ может быть сохранен впоследствии в утилите *CIServerSetup.exe*).

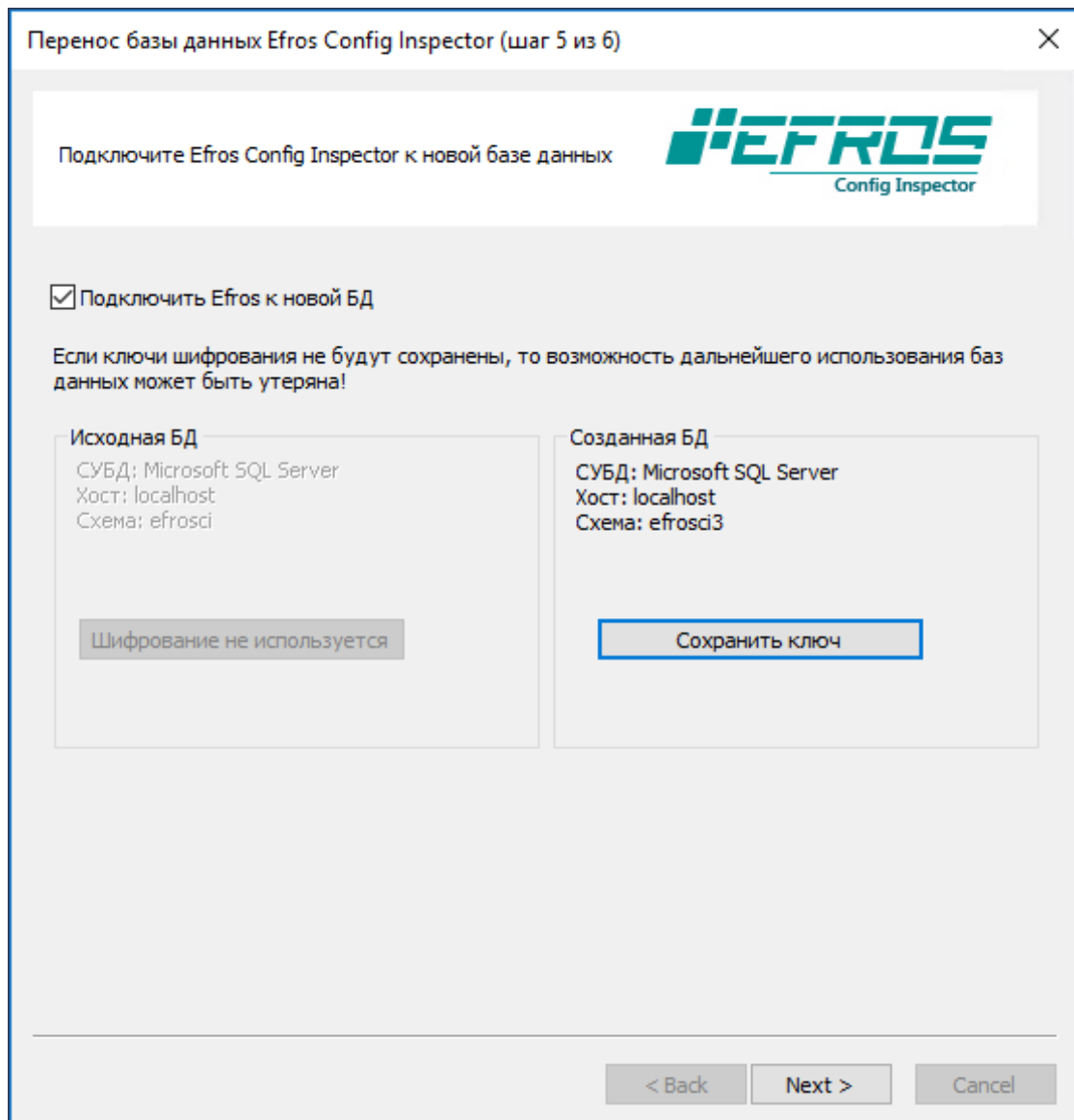


Рисунок 70 – Окно со сводной информацией по переносу и шифрованию БД

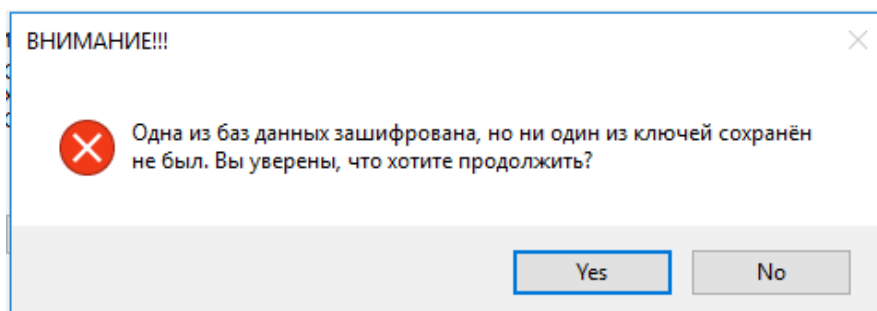


Рисунок 71 – Окно с предупреждением об отсутствии сохраненного ключа шифрования для БД

- 8) Нажать кнопку **Готово/Finish** в окне мастера переноса БД.

- 9) Закрыть серверную консоль комплекса нажатием кнопки **ОК**.
- 10) Выполнить перезапуск службы EFROS CI Service 4.

6.1.3.2. Перенос БД программного комплекса на ЭВМ под управлением ОС «Astra Linux SE», ОС «РЕД ОС»

Для переноса используемой комплексом БД на ЭВМ под управлением ОС «Astra Linux SE», ОС «РЕД ОС» администратору комплекса необходимо выполнить следующие действия:

- 1) Запустить серверную консоль комплекса командой:

```
“sudo efrosci-settings”
```

- 2) Перейти в раздел **Настройка базы данных** и выбрать пункт **Миграция БД**.
- 3) В открывшемся окне переноса БД (рис. 72) задать параметры копируемой БД и создаваемой БД.
- 4) Выбрать пункт **Начать перенос**. В окне будет отображаться ход процедуры копирования БД комплекса.

Если на шаге 3 введены неверные данные, то в окне консоли отобразится сообщение об ошибке. Откорректируйте введенные параметры и вновь выберите пункт **Начать перенос**.

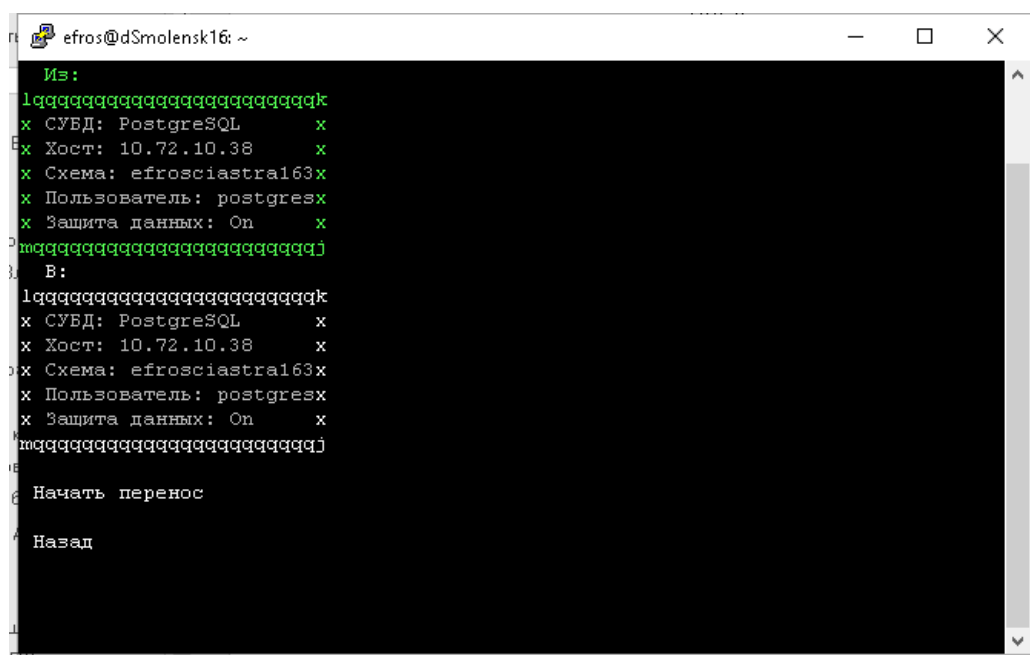


Рисунок 72 – Окно корректировки параметров подключения к серверу БД

5) После успешного окончания процедуры копирования БД комплекса в окне отобразится сообщение **Перенос БД завершен**. Нажмите ENTER.

6) Выбрать в открывшемся окне для подключения к новой БД (рис. 73) требуемый вариант и нажать ENTER.

Примечание – Если для БД задано значение **On** параметра **Включить защиту данных (алгоритм AES-256)**, то потребуется также задать параметры ключа защиты (см. п. 2.3.3 «Создание БД комплекса»).

7) Для применения внесенных изменений – выполните перезапуск службы сервера ПК.

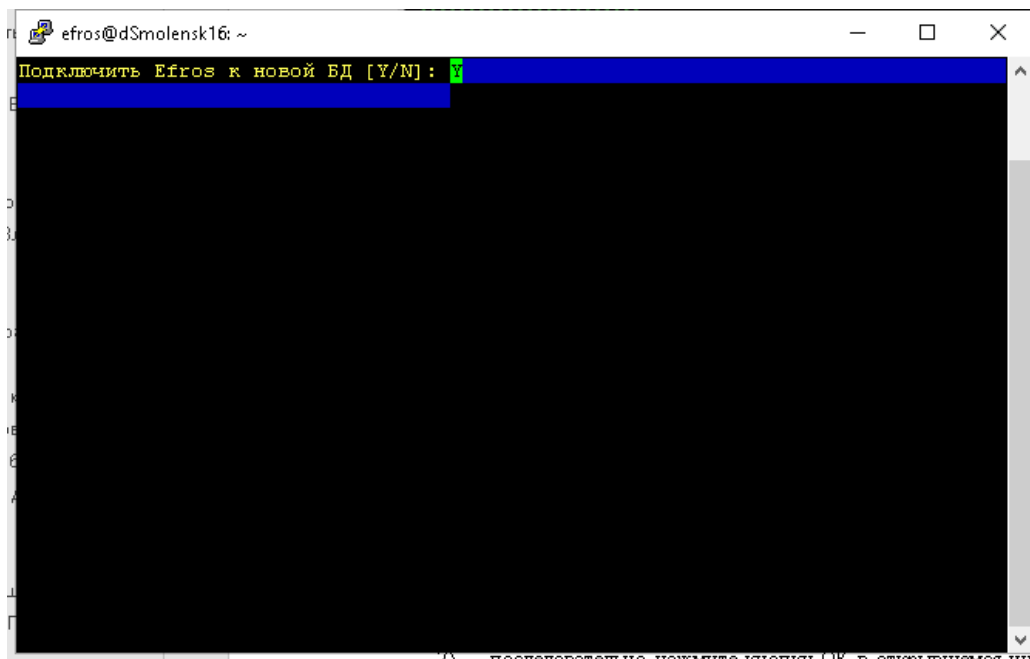


Рисунок 73 – Окно подтверждения подключения сервера ПК к новой БД

6.2. Сохранение и восстановление настроек серверной части комплекса

6.2.1. Сохранение и восстановление настроек сервера ПК на ЭВМ под управлением ОС серии Windows

Настройки серверной части ПК «Efros Config Inspector» v.4 (параметры подключения к БД, параметры аудита) хранятся в реестре ОС Windows:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Gazinformservice\EFROS Config Inspector  
Server 4
```

Для резервирования настроек серверной части комплекса необходимо сохранить данный ключ реестра.

Для сохранения ключей реестра следует ввести в эмуляторе командной строки (**cmd**) команду:

```
REG SAVE <имя раздела> <имя файла>
```

Например, в результате выполнения команды:

```
C:\>reg save "HKEY_LOCAL_MACHINE\SOFTWARE\Gazinformservice\EFROS Config  
Inspector Server 4" Device.hiv
```

в корне диска C:\ будет создан файл *Device.hiv*, в котором будут сохранены параметры серверной части программного комплекса.

Для восстановления настроек серверной части комплекса необходимо использовать файлы с сохраненными ранее ключами реестра. Для внесения изменений в реестр следует ввести в эмуляторе командной строки (**cmd**) команду:

```
REG RESTORE <имя раздела> <имя файла>
```

Например, в результате выполнения команды:

```
C:\>reg restore "HKEY_LOCAL_MACHINE\SOFTWARE\Gazinformservice\EFROS Config Inspector Server 4" Device.hiv
```

в реестре будет создан указанный раздел (если такого раздела в реестре не существовало) или его содержимое будет заменено данными содержащимися в файле C:\Device.hiv.

При восстановлении настроек серверной части ПК «Efros Config Inspector» v.4 необходимо удалить из ветки реестра *HKEY_LOCAL_MACHINE\SOFTWARE\Gazinformservice\EFROS Config Inspector Server 4\Settings* следующие параметры:

- *SQL server password protected;*
- *root password protected.*

Эти параметры защищены и привязаны к системе, на которую были установлены ранее. Заново установить пароль **root**-пользователей комплекса и используемой СУБД можно в серверной консоли на вкладках **Дополнительно** и **База данных** соответственно.

Если установленный по умолчанию пароль встроенного в БД комплекса пользователя **root** не изменялся, то параметр реестра *root password protected* будет отсутствовать.

6.2.2. Сохранение и восстановление настроек сервера ПК на ЭВМ под управлением ОС «Astra Linux SE», ОС «РЕД ОС»

Настройки сервера ПК «Efros Config Inspector» v.4 на ЭВМ под управлением ОС «Astra Linux SE», ОС «РЕД ОС» хранятся в файле */etc/efrosci/config.ini*.

Для резервирования настроек сервера ПК необходимо сохранить данный файл средствами ОС, для чего выполнить команду *cp*:

```
cp /etc/efrosci/config.ini <ПУТЬ ДЛЯ СОХРАНЕНИЯ ФАЙЛА>
```

Для восстановления настроек сервера ПК необходимо средствами ОС скопировать сохраненный ранее файл с настройками в файл */etc/efrosci/config.ini*. Сделать это можно командой *cp*:

```
sudo cp <ФАЙЛ С НАСТРОЙКАМИ> /etc/efrosci/config.ini
```

Примечание – Команды должны выполняться пользователем с правами администратора.

6.3. Резервирование ключа защиты данных БД комплекса

Информация об используемом для защиты БД ПК «Efros Config Inspector» v.4 ключе защиты данных, может понадобиться при переносе серверной части комплекса на другой компьютер или во время операции обновления версии серверной части (подробнее см. п. 2.2.4 «Подключение к существующей базе данных» настоящего Руководства).

6.3.1. Резервирование ключа защиты данных БД комплекса на ЭВМ под управлением ОС серии Windows

Для резервирования ключа защиты данных БД комплекса (если использовалась защита БД) администратору необходимо выполнить следующие действия:

- 1) Запустить серверную консоль ПК (**Пуск** → **Все программы** → **Efros Config Inspector4** → **CIServerSetup**).
- 2) В окне серверной консоли перейти на вкладку **База данных**: и нажать кнопку **Экспорт ключа**.
- 3) В открывшемся окне **Экспорт ключа защиты данных** в соответствующие поля ввода ввести пароль учетной записи администратора комплекса **root** (по умолчанию при инсталляции сервера ПК учетной записи **root** присваивается пароль **root**), пароль, с использованием которого будет модифицирован экспортируемый ключ защиты данных БД комплекса, и нажать кнопку **Сохранить ключ**.
- 4) В открывшемся диалоговом окне выбрать каталог и указать имя файла, в который будет сохранен ключ защиты данных, после чего нажать на кнопку **Сохранить**.

6.3.2. Резервирование ключа защиты данных БД комплекса на ЭВМ под управлением ОС «Astra Linux SE», ОС «РЕД ОС»

Для резервирования ключа защиты данных БД комплекса (если использовалась защита БД) администратору необходимо выполнить следующие действия:

- 1) Запустить утилиту настройки службы сервера ПК командой:

```
“sudo efrosci-settings”
```

- 2) В окне серверной консоли выбрать ссылку **Настройка базы данных**.
- 3) В открывшемся разделе **Настройка базы данных** нажать ссылку **Экспорт ключа БД**.
- 4) В открывшемся окне:
 - ввести пароль учетной записи администратора комплекса **root** (по умолчанию при инсталляции сервера ПК учетной записи **root** присваивается пароль **root**) и нажать клавишу клавиатуры **ENTER**;
 - ввести пароль, с использованием которого будет модифицирован экспортируемый ключ защиты данных БД комплекса и нажать клавишу клавиатуры **ENTER**;
 - ввести путь и имя файла, в который будет сохранен ключ защиты данных и нажать клавишу клавиатуры **ENTER**.

6.4. Перенос серверной части комплекса на другой компьютер

В зависимости от варианта установки используемой программным комплексом СУБД и серверной части комплекса существует несколько вариантов переноса серверной части на другой компьютер.

При переносе серверной части ПК «Efros Config Inspector» v.4 и используемой СУБД на другой компьютер администратор должен выполнить следующие действия:

1) Создать резервную копию БД ПК (см. п. 6.1 «Операции с БД» настоящего Руководства).

2) Зарезервировать ключ защиты данных БД комплекса, если использовалась защита БД (см. п. 6.3 «Резервирование ключа защиты данных БД комплекса» настоящего Руководства).

3) Зарезервировать настройки серверной части комплекса (см. п. 6.2 «Сохранение и восстановление настроек серверной части комплекса» настоящего Руководства).

4) Установить на новый компьютер используемую СУБД (см. п. 2.1 «Установка СУБД» настоящего Руководства).

5) Восстановить из резервной копии БД программного комплекса (см. п. 6.1.2 «Восстановление БД программного комплекса из резервной копии» настоящего Руководства).

6) Установить серверную часть программного комплекса на новый компьютер (см. п. 2.2 и 2.3 настоящего Руководства). По окончании установки серверной части программного комплекса отказаться от настройки подключения сервера ПК к БД комплекса.

7) Восстановить настройки серверной части комплекса (см. п. 6.2 «Сохранение и восстановление настроек серверной части комплекса» настоящего Руководства).

8) Выполнить настройку подключения сервера ПК к используемой БД комплекса (см. п. 2.2 и 2.3 настоящего Руководства).

При переносе на другой компьютер только серверной части ПК «Efros Config Inspector» v.4 администратор ПК должен выполнить следующие действия:

1) Зарезервировать ключ защиты данных БД комплекса, если использовалась защита БД (см. п. 6.3 «Резервирование ключа защиты данных базы данных ПК» настоящего Руководства).

2) Зарезервировать настройки серверной части комплекса (см. п. 6.2 «Сохранение и восстановление настроек серверной части комплекса» настоящего Руководства).

3) Установить серверную часть программного комплекса на новый компьютер (см. п. 2.2 и 2.3 настоящего Руководства). По окончании установки серверной части программного комплекса отказаться от настройки подключения сервера ПК к БД комплекса.

4) Восстановить настройки серверной части комплекса (см. п. 6.2 «Сохранение и восстановление настроек серверной части комплекса» настоящего Руководства).

5) Выполнить настройку подключения сервера ПК к используемой БД комплекса (см. п. 2.2 и 2.3 настоящего Руководства).

6.5. Настройка резервирования сервера комплекса

В ПК «Efros Config Inspector» v.4 при наличии в используемой лицензии ПК «Efros Config Inspector» v.4 поддержки резервирования доступна настройка резервирования сервера ПК. Просмотреть параметры лицензии можно в клиентской консоли в разделе **Настройки** (рис. 74). Резервирование поддерживается только для однотипных ОС. В случае выхода из строя основного сервера ПК, все функции переключаются на резервный.

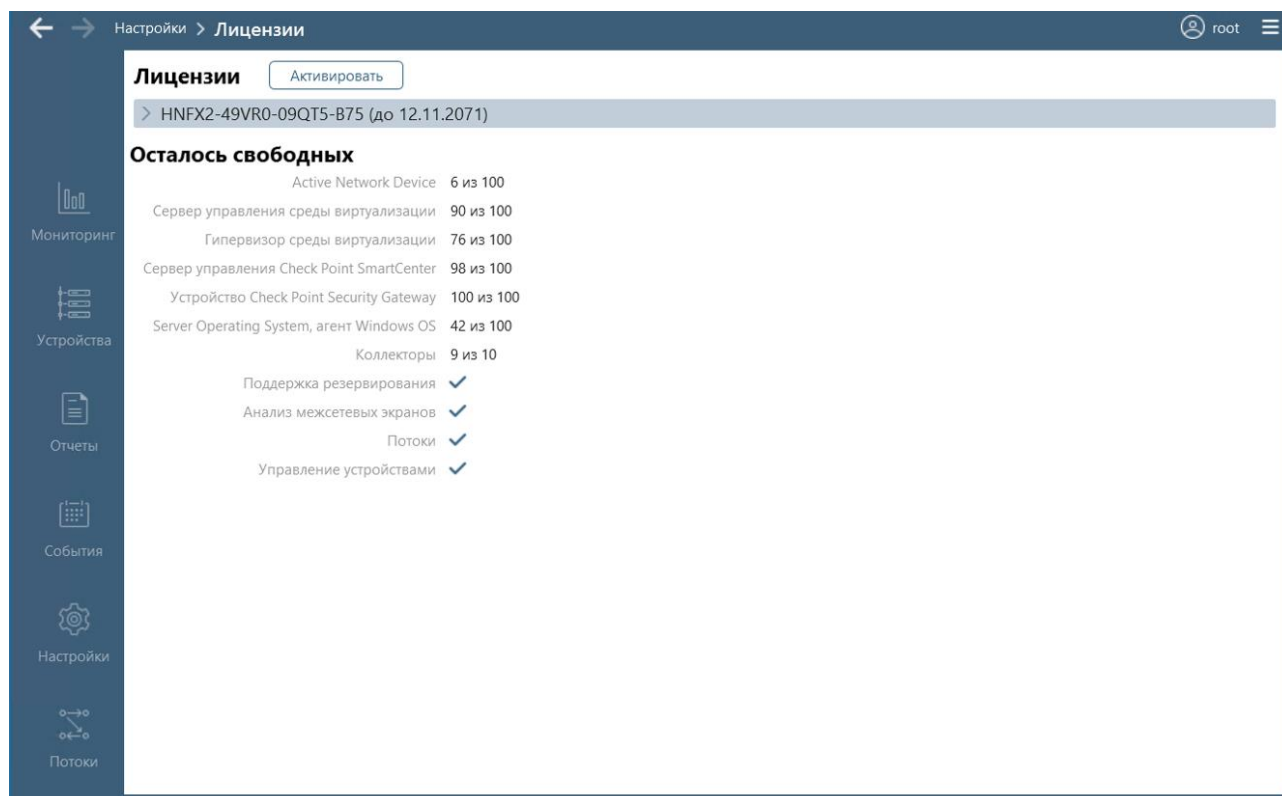


Рисунок 74 – Страница **Лицензии**

Для работы системы резервирования необходимо создание и настройка резервного сервера. Для настройки резервного сервера необходимо:

1) Установить серверную часть программного комплекса на новый компьютер (см. п. 2.2 и 2.3 настоящего Руководства), указав параметры сервера: адрес и порт подключения.

ВНИМАНИЕ: Основной и резервный серверы должны иметь одинаковую версию!

2) По окончании установки серверной части программного комплекса выполнить настройку подключения сервера ПК к используемой БД комплекса (см. п. 2.2 и 2.3 настоящего Руководства).

Просмотреть список резервных серверов ПК с активированной лицензией можно в клиентской консоли в разделе **Настройки**. Для этого необходимо в области

Администрирование под кнопкой **База данных** нажать ссылку **Резервирование**. В списке отображены наименования резервных серверов (рис. 75).

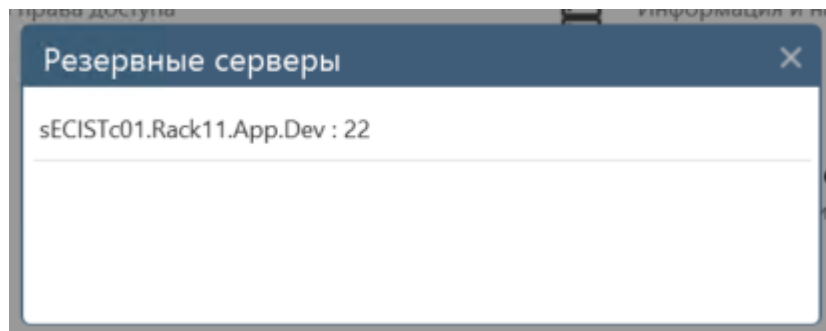


Рисунок 75 – Список резервных серверов ПК

При попытке пользователя подключиться к резервному серверу (указав адрес и порт резервного сервера при запуске клиентской консоли) автоматически будет выполнена переадресация на основной сервер ПК, на экране отобразится сообщение в соответствии с рисунком 76.

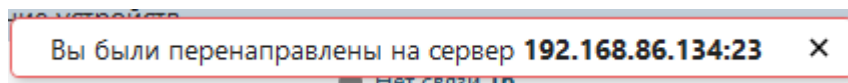


Рисунок 76 – Сообщение о переадресации подключения к серверу ПК

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

При наличии нескольких серверов ПК, основным считается тот, который был подключен к БД первым. Все последующие являются резервными.

Наименование основного сервера ПК отображено в заголовке окна консоли (рис. 77).



Рисунок 77 – Наименование основного сервера ПК

В случае нарушения работы основного сервера через определенный промежуток времени произойдет автоматическое переключение на резервный сервер. Этот параметр настраивается в БД комплекса в поле **lock_timeout_min** таблицы **efrosci_4.lockdata**. Значение параметра по умолчанию составляет 10 минут.

При наличии более одного резервного сервера ПК, переключение происходит на тот, который был раньше других подключен к БД комплекса.

При переключении на резервный сервер наименование сервера ПК в заголовке окна консоли изменится (рис. 78).

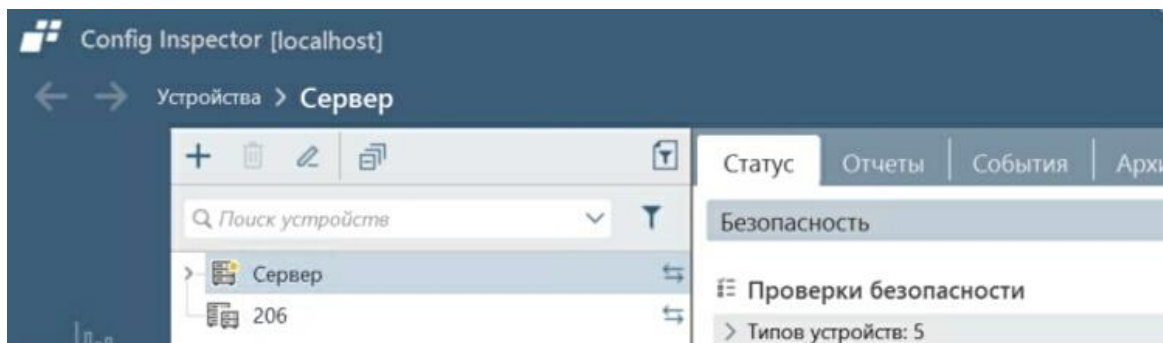


Рисунок 78 – Наименование окна после переключения

После переключения на резервный сервер изменится список резервных серверов ПК: сервер, на который произошло переключение, станет основным и не будет отображен в списке (рис. 79).

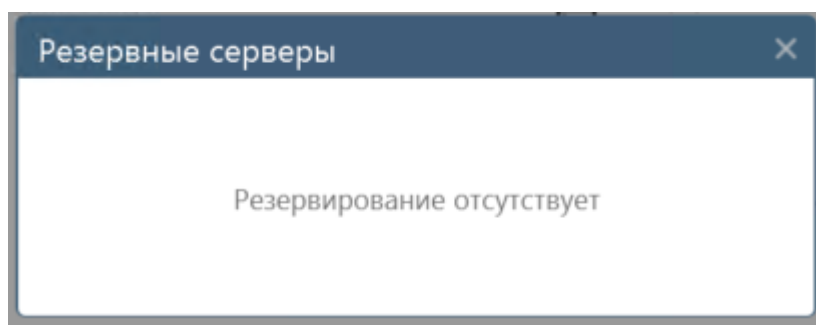


Рисунок 79 – Резервный сервер ПК стал основным

В случае восстановления работоспособности сервера ПК, вышедшего из строя, он будет иметь статус резервного (рис. 80).

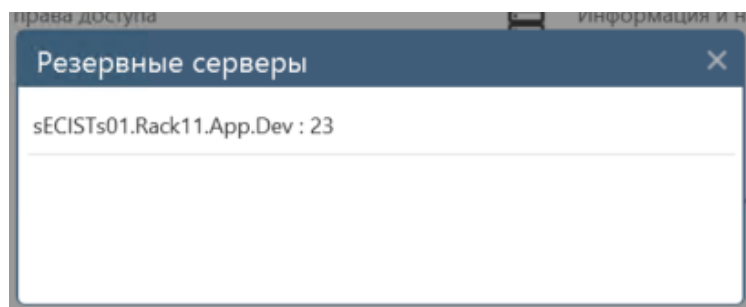


Рисунок 80 – Обновленный список резервных серверов ПК

7. Реализация функций безопасности среды функционирования

7.1. Для обеспечения безопасной эксплуатации ПК «Efros Config Inspector» v.4, после его установки при первом запуске клиентской консоли необходимо сменить пароль встроенного администратора «root».

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

- службу сервера (C:\Program Files\EFROS Config Inspector 4\Server\CIService.exe);
- клиентскую консоль (C:\Program Files (x86)\EFROS Config Inspector 4\Console\CIWPF.exe) либо (C:\Program Files\EFROS Config Inspector 4\Console\CIWPF.exe) в зависимости от разрядности используемого модуля и операционной системы;
- службу Windows-агента (C:\Program Files\EFROS Config Inspector 4\Agent\WAService.exe);
- службу коллектора задач (C:\Program Files\EFROS Config Inspector 4\Collector\CollectorService.exe).

7.3. Порядок настройки сетевого и серверного оборудования (в зависимости от производителя оборудования) для подключения его к ПК «Efros Config Inspector» v.4 по используемым протоколам указан в файле справки *Описание модулей.zip* (*Описание модулей.chm*), расположенном на дистрибутивном диске программного комплекса.

8. 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.

8.1. Сбой функционирования сетевых служб

Возможны следующие сбои функционирования сетевых служб:

1) В случае сбоя сетевого соединения между клиентской консолью и сервером ПК при попытке запуска клиентской консоли в окне подключения к серверу ПК или в процессе работы пользователя отобразится сообщение «*Связь с сервером потеряна*».

2) В случае сбоя сетевого соединения между ПК «Efros Config Inspector» v.4 и контролируемым устройством в консоли изменится статус устройства на *Нет связи*.

В обоих случаях при получении от пользователей сообщений о сбое администратору ПК «Efros Config Inspector» v.4 совместно с администратором сети необходимо выявить причину сбоя сетевого соединения и принять меры для восстановления работы сетевых служб.

8.2. Сбой после вмешательства посторонних лиц в ПК «Efros Config Inspector» v.4

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. 81). Запись об обнаружении нарушения будет также занесена в журнал событий раздела **События** клиентской консоли.

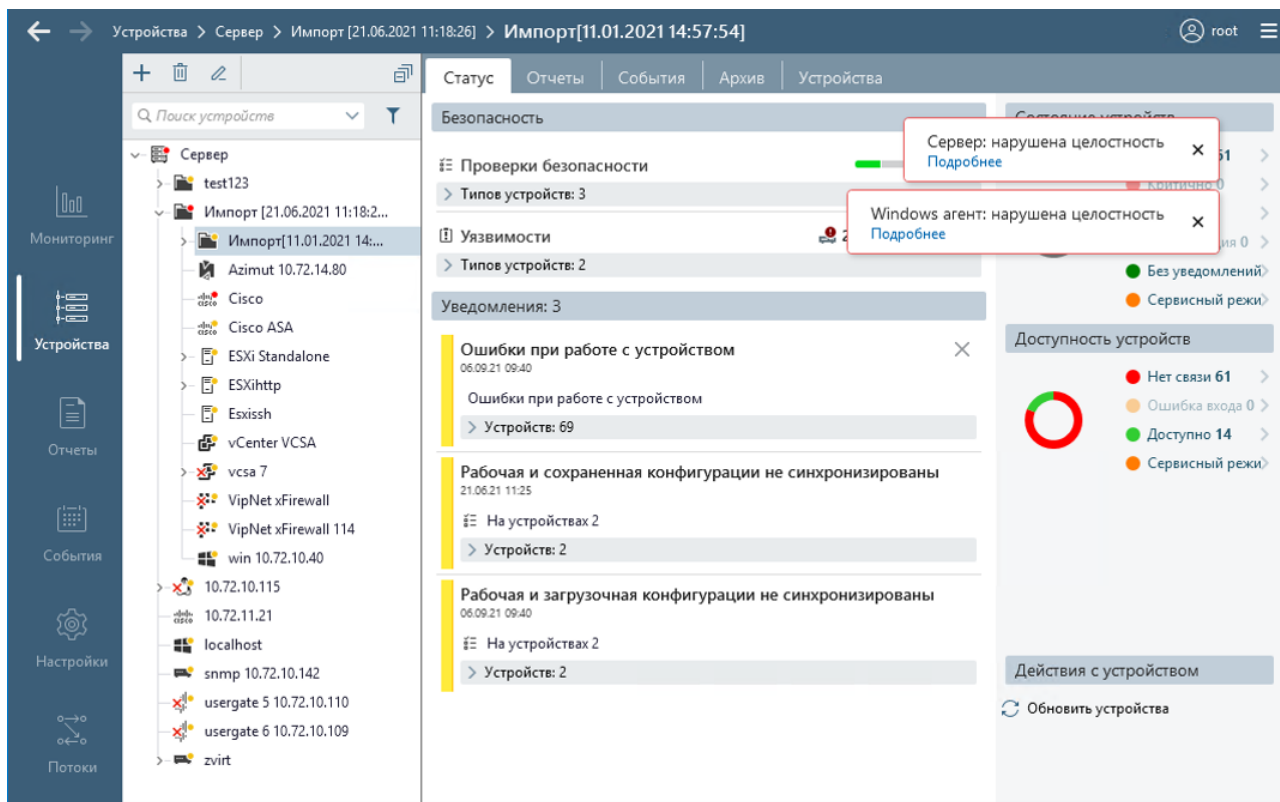


Рисунок 81 – Уведомления об обнаружении нарушения КЦ компонентов комплекса. Пользователь имеет возможность просмотреть перечень обнаруженных нарушений, нажав ссылку **Подробнее** (рис. 82). Возможные варианты нарушений: «нарушена целостность файла: <наименование файла>», «файл не найден: <наименование файла>», «неизвестный файл: <наименование файла>».

Если обнаруженные нарушения не связаны с плановыми изменениями компонентов комплекса, то администратору ПК «Efros Config Inspector» v.4 и администратору сетевой безопасности необходимо принять меры в соответствии с корпоративной политикой безопасности для устранения доступа посторонних лиц к компонентам ПК «Efros Config Inspector» v.4 и выполнить восстановление нарушенных компонентов ПК «Efros Config Inspector» v.4 путем переустановки требуемых версий компонентов комплекса.

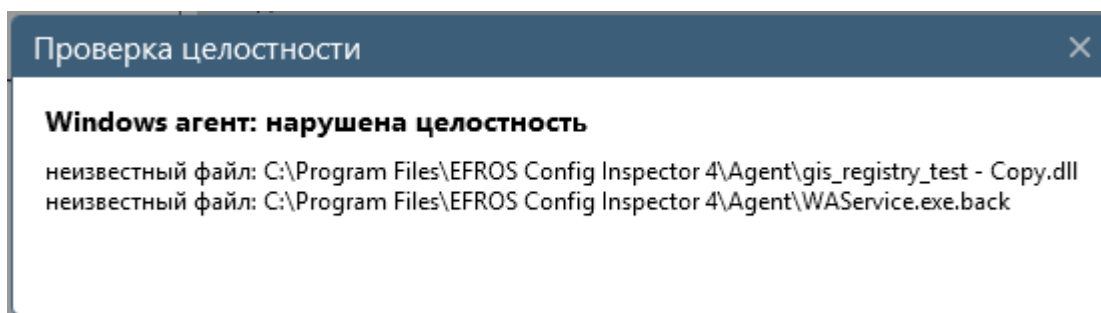


Рисунок 82 – Окно просмотра перечня обнаруженных нарушений целостности компонентов комплекса

8.3. Сбой в работе сервера ПК «Efros Config Inspector» v.4

В случае сбоя работоспособности сервера ПК «Efros Config Inspector» v.4, администратору необходимо перезапустить службу «Efros Config Inspector», для этого:

1) Открыть окно настройки сервера ПК (далее – серверная консоль) (рис. 83), для чего в меню **Пуск** рабочего стола Windows, на панели задач выбрать **Все программы** → **Efros Config Inspector4** → **CIServerSetup**.

2) В серверной консоли, на вкладке **Службы** проконтролировать состояние службы сервера «Efros Config Inspector».

3) Если служба не запущена, нажать кнопку **Пуск** (см. рис. 83). При запущенной службе сервера, нажать последовательно кнопки **Стоп** и **Пуск** для перезапуска службы сервера. Активировать функцию автоматического перезапуска службы сервера в случае возникновения отказов и сбоев и установить максимальное количество попыток перезапуска в поле *Количество попыток перезапуска*.

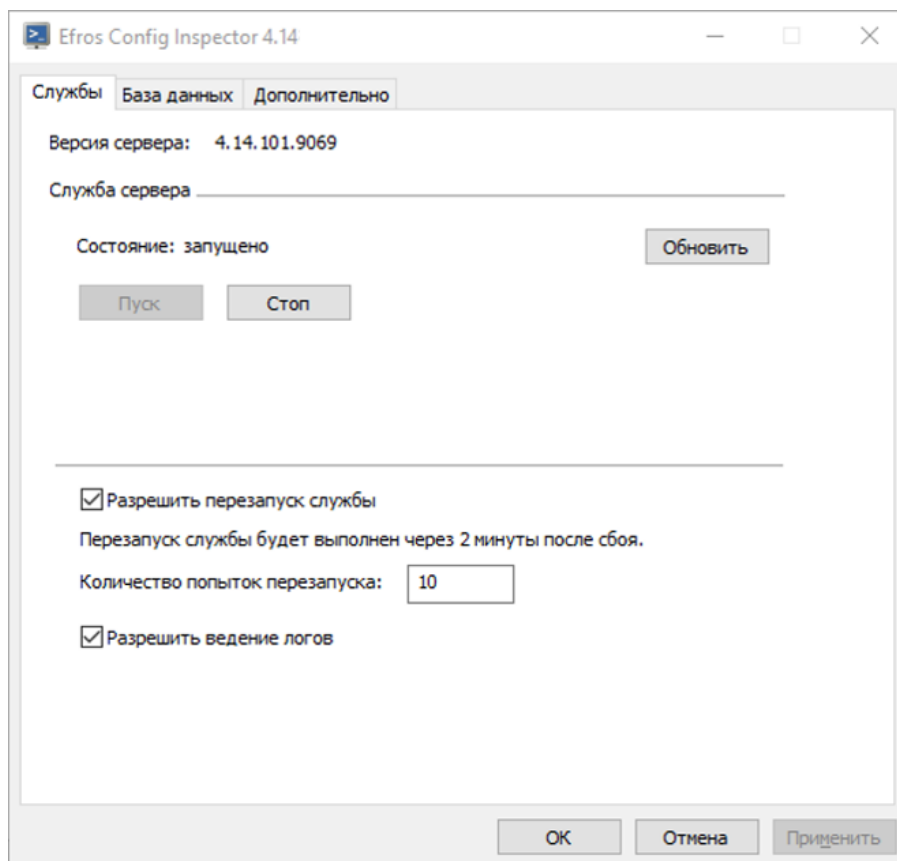


Рисунок 83 – Серверная консоль, вкладка **Службы**

Если сервер развернут на ОС «Astra Linux SE», ОС «РЕД ОС», то запустить средство настройки службы сервера командой:

```
“sudo efrosci-settings”
```

Перейти по ссылкам **Настройка службы сервера > Управление службой** (рис. 84) и последовательно нажать кнопки **Стоп** и **Пуск** (рис. 85) для перезапуска службы сервера.

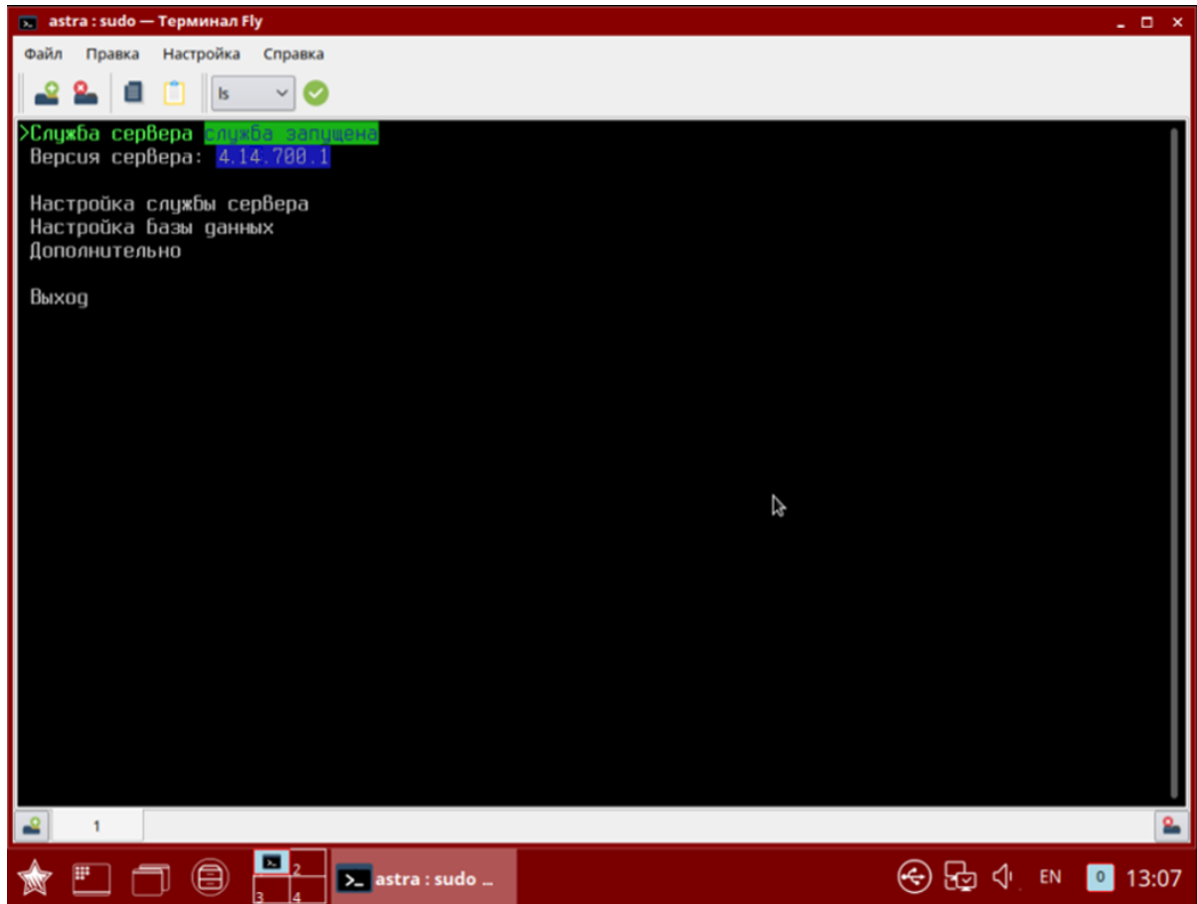


Рисунок 84 – Окно настройки службы сервера

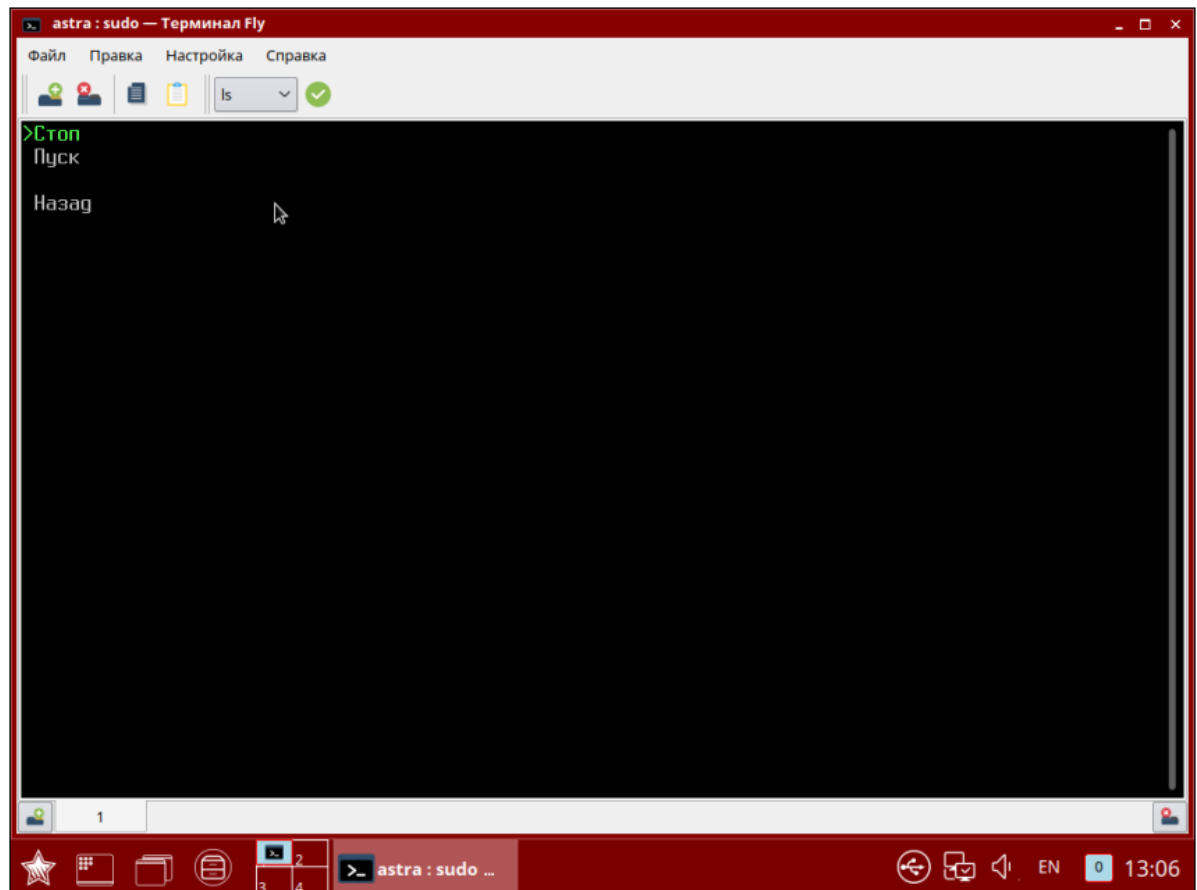


Рисунок 85 – Окно запуска (останова) службы сервера

4) При неустранении ошибки (сбоя) обратиться в службу технической поддержки организации разработчика ПК «Efros Config Inspector» v.4.

8.4. Сбой и ошибки в работе СУБД

При выходе из строя СУБД работа ПК «Efros Config Inspector» v.4 становится невозможной. Нарушение в работе СУБД возможна при следующих нарушениях:

- служба СУБД не запущена;
- версия БД отличается от версии, поддерживаемой Efros Config Inspector v.4;
- системная ошибка СУБД.

Если версия БД отличается от версии, поддерживаемой ПК «Efros Config Inspector» v.4, администратору необходимо выполнить обновление СУБД в соответствии с эксплуатационной документацией на комплекс.

В случае обнаружения системной ошибки СУБД необходимо выполнить:

- перезапуск службы СУБД;
- переустановку СУБД.

8.5. Сбой клиентской консоли ПК «Efros Config Inspector» v.4

8.5.1. Ошибки идентификации

Сообщения об ошибках идентификации будут направлены пользователю в случае отсутствия соответствующих привилегий для их выполнения:

- отказ на получение доступа к серверу.

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. 86) 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**.

Сервер: 10.72.11.134 | Порт: 20000

Вход под текущим пользователем

Логин: uzer2

Пароль: [masked] EN

Неверные логин и пароль

Подключиться

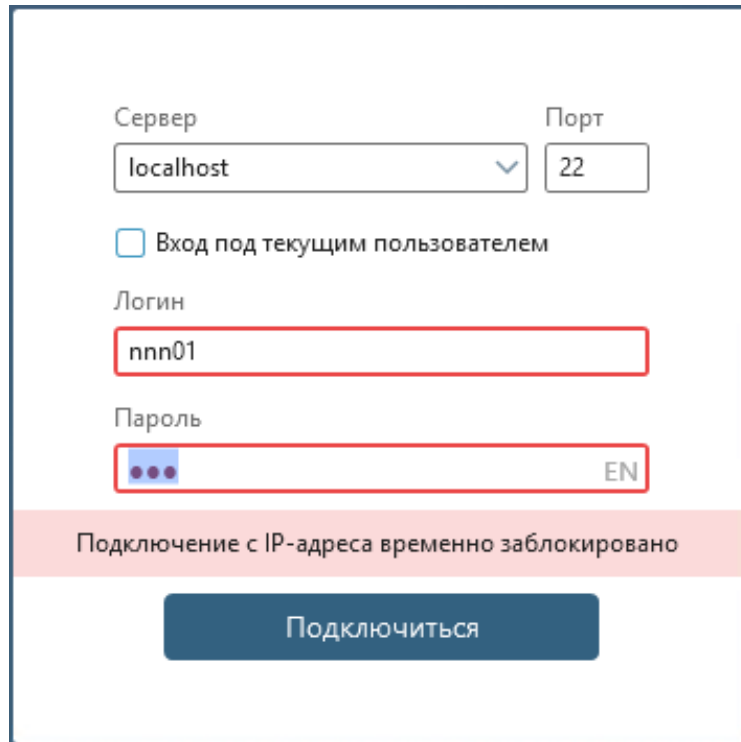
Рисунок 86 – Окно подключения к серверу ПК после ввода неверных данных пользователя

При получении сообщения о временной блокировке IP-адреса после нескольких подряд попытках (от 3 до 8) неверного ввода аутентификационных данных пользователя (рис. 87) 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. документ «643.72410666.00082-01 96 01-01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование»).

При получении сообщения о блокировке учетной записи пользователя (рис. 88) 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. документ «643.72410666.00082-01 96 01-01 «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 1. Администрирование»).



Сервер localhost Порт 22

Вход под текущим пользователем

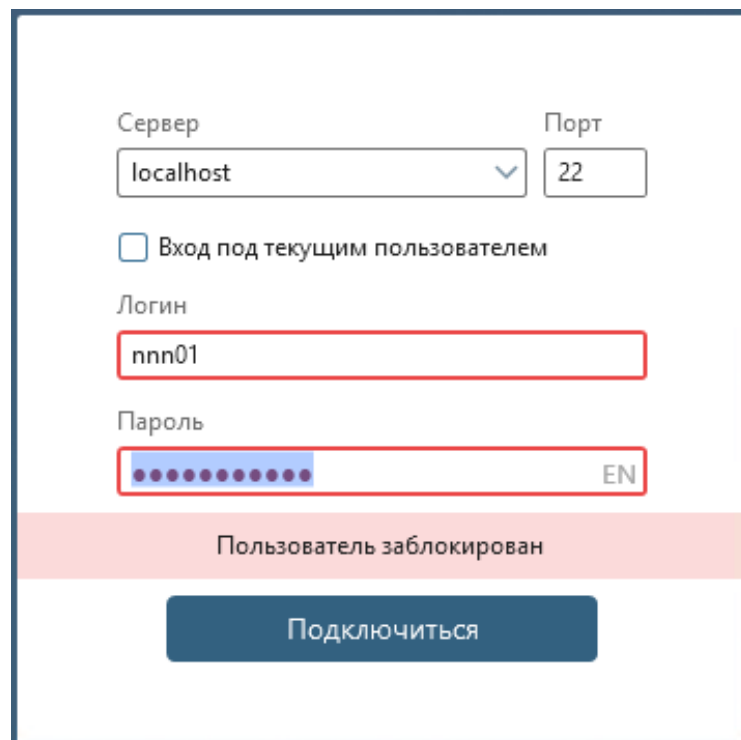
Логин nnn01

Пароль [mask] EN

Подключение с IP-адреса временно заблокировано

Подключиться

Рисунок 87 – Окно подключения к серверу ПК после превышения количества попыток неверного ввода аутентификационных данных пользователя



Сервер localhost Порт 22

Вход под текущим пользователем

Логин nnn01

Пароль [mask] EN

Пользователь заблокирован

Подключиться

Рисунок 88 – Окно подключения к серверу ПК после ввода аутентификационных данных заблокированного пользователя

8.5.2. 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.

8.5.3. 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. 2.6 настоящего Руководства.

Перечень сокращений

HTTP (HyperText Transfer Protocol)	– протокол прикладного уровня передачи данных. Основой HTTP является технология «клиент-сервер»
HTTPs (HyperText Transfer Protocol Secure)	– расширение протокола HTTP
Syslog	– стандарт отправки сообщений о происходящих в системе событиях
SSH (Secure Shell)	– сетевой протокол прикладного уровня, позволяющий производить удаленное управление и туннелирование TCP-соединений, 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
КЦ	– контроль целостности
ОЗ	– объект защиты
ОС	– операционная система
ПК	– программный комплекс
ПО	– программное обеспечение
СУБД	– система управления базами данных
ЭВМ	– электронно-вычислительная машина

Термины и определения

- Отчет** – Загружаемые с устройств данные, а также результаты обработки загруженных данных являются отчетами типа **Отчет**, **Текстовый отчет**. Результат проверки данных на соответствие заданным правилам – отчет типа **Отчет о проверке**
- Проверка** – Отчет, сформированный ПК «Efros Config Inspector» v.4 по результатам проверки загруженных или выбранных данных на соответствие заданным правилам
- Профиль** – Поименованная совокупность настроек параметров контроля устройств, отчетов и проверок, доступных для устройств
- Событие** – Зафиксированное в журнале программы действие сервера ПК или пользователей программы
- Статус** – Интерфейс, на котором отображены важные оповещения по ситуации и выведены основные операции с контролируруемыми устройствами