ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ

Dallas Lock

Инструкция по использованию

СОДЕРЖАНИЕ

ВВЕДЕНИЕ **4**

ТЕРМИНЫ **4**

СОКРАЩЕНИЯ **6**

ПРЕДСТАВЛЕНИЕ МОДУЛЕЙ В ИНТЕРФЕЙСЕ ЕЦУ **7**

1 НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ ЕЦУ DALLAS LOCK **8**

1.1 Структура ЕЦУ 8
1.2 Возможности ЕЦУ 8

2 УСТАНОВКА И УДАЛЕНИЕ ЕЦУ DALLAS LOCK **11**

2.1 Требования к аппаратному и программному обеспечению 11
2.2 Установка ЕЦУ Dallas Lock 13
2.3 Удаление ЕЦУ Dallas Lock 25
2.4 Сохранение и применение конфигурации 29
2.5 О программе 30

3 ОБЩИЕ ПРИНЦИПЫ РАБОТЫ ЕЦУ DALLAS LOCK **31**

3.1 Синхронизация 31
3.2 Репликация 31

4 АДМИНИСТРИРОВАНИЕ ЕЦУ DALLAS LOCK **32**

4.1 Запуск консоли ЕЦУ 32
4.2 Описание консоли ЕЦУ 33
4.3 Ключ доступа к ДБ 36
4.4 Настройки лицензирования 36
4.5 Параметры ЕЦУ 39

5 ДОМЕН БЕЗОПАСНОСТИ ЕЦУ **53**

5.1 Сводка для ДБ 53
5.2 Пользователи и группы ДБ 57
5.3 Ролевая модель учетных записей ДБ 78
5.4 Политики ДБ 79
5.5 Задания ДБ 112
5.6 Журнал ДБ 114

6 ГРУППЫ ДОМЕНА БЕЗОПАСНОСТИ **117**

6.1 Базовые группы 117
6.2 Настройка групп 117

7 АРМ ДОМЕНА БЕЗОПАСНОСТИ ЕЦУ **123**

7.1 Настройка АРМ 123

8 МОДУЛИ ДОМЕНА БЕЗОПАСНОСТИ ЕЦУ **126**

8.1 Настройка модуля 126

9 МОДУЛЬ СЗИ DALLAS LOCK 8.0-C/K **132**

9.1 Ввод модуля в ДБ 132
9.2 Вывод модуля из ДБ 134
9.3 Удаленное развертывание СЗИ Dallas Lock 8.0 135
9.4 Настройка модуля СЗИ Dallas Lock 8.0 151

10 МОДУЛЬ СЗИ НСД DALLAS LOCK LINUX **156**

10.1 Ввод модуля в ДБ 156

10.2 Вывод модуля из ДБ 157
10.3 Удаленное развертывание СЗИ НСД Dallas Lock Linux 158
10.4 Настройка модуля СЗИ НСД Dallas Lock Linux 165

11 МОДУЛЬ СЗИ ВИ DALLAS LOCK 171

11.1 Ввод модуля в ДБ 171
11.2 Вывод модуля из ДБ 172
11.3 Настройка СЗИ ВИ Dallas Lock 173

12 МОДУЛЬ СДЗ DALLAS LOCK 178

12.1 Ввод модуля в ДБ 178
12.2 Вывод модуля из ДБ 180
12.3 Настройка модуля СДЗ Dallas Lock 180

13 МОДУЛЬ WAF DALLAS LOCK 184

13.1 Ввод модуля в ДБ 184
13.2 Вывод модуля из ДБ 185
13.3 Настройка модуля WAF Dallas Lock 186

14 АГЕНТ ЕЦУ 191

14.1 Требования к аппаратному и программному обеспечению 191
14.2 Установка и удаление Агента ЕЦУ 191
14.3 Регистрация Агента ЕЦУ в ДБ 202
14.4 Настройка модуля Агент ЕЦУ 202

15 KASPERSKY SECURITY CENTER 209

15.1 Подключение к Kaspersky Security Center 209
15.2 Отключение Kaspersky Security Center 210
15.3 Настройка Kaspersky Security Center 211
15.4 Настройка модуля Kaspersky Endpoint Security 215

16 СЕТЕВОЕ ОБОРУДОВАНИЕ 218

16.1 Регистрация сетевого устройства в ДБ 218
16.2 Удаление сетевого устройства из ДБ 222
16.3 Настройка сетевого устройства 223

17 ПОДЧИНЕННЫЙ ДОМЕН БЕЗОПАСНОСТИ 228

17.1 Ввод ДБ в подчинение 228
17.2 Вывод ДБ из подчинения 230
17.3 Настройка подчиненного домена безопасности 232

ВВЕДЕНИЕ

Данная инструкция предназначена для администратора программного продукта «Единый центр управления Dallas Lock».

В инструкции содержатся сведения, необходимые для получения общего представления о программном изделии, его функциональных возможностях, а также для установки, настройки и управления работой в соответствии с требованиями безопасности.

Единый центр управления Dallas Lock — кроссплатформенное изделие в продуктовой линейке Dallas Lock, предназначенное для решения следующих задач:

- создание иерархической инфраструктуры домена безопасности с наследованием значений параметров безопасности;
- контроль сетевой инфраструктуры;
- удаленный сбор и удобное отображение настроек текущей и эталонной конфигураций (контроль целостности) сетевых устройств с целью дальнейшей проверки на соответствие требованиям стандартов и выявления несанкционированных изменений;
- использование единой системы управления учетными записями;
- интеграция списка учетных записей и групп пользователей с Active Directory;
- организация централизованного управления решениями продуктовой линейки ООО «Конфидент»:
  - СЗИ Dallas Lock 8.0 редакций «К» и «С» (включая компоненты МЭ, СОВ);
  - СЗИ НСД Dallas Lock Linux;
  - СЗИ ВИ Dallas Lock;
  - СДЗ Dallas Lock;
  - Агент ЕЦУ;
- удаленное развертывание модулей СЗИ Dallas Lock 8.0, СЗИ НСД Dallas Lock Linux, а также Агента ЕЦУ (для Windows и Linux);
- сбор журналов с модулей и сетевых устройств (по протоколу Syslog), зарегистрированных в домене безопасности;
- интеграция со сторонними продуктами (Антивирус Kaspersky, SIEM-системы).

Сайт компании-разработчика единого центра управления Dallas Lock ООО «Конфидент» доступен по ссылке: www.confident.ru.

Информация о продуктах линейки Dallas Lock представлена на странице сайта www.dallaslock.ru. На данном сайте можно заказать комплекс услуг по проектированию, внедрению и сопровождению продукта. Также при необходимости можно обратиться в службу технической поддержки по электронному адресу: helpdesk@confident.ru.

ТЕРМИНЫ

Некоторые термины и сокращения, содержащиеся в тексте инструкции, уникальны для продуктовой линейки ООО «Конфидент», другие являются общепринятыми и используются из соображения краткости и удобства.

Термин	Определение
Автоматизированное рабочее место	виртуальная или физическая рабочая станция, используемая в ЕЦУ как способ представления совокупности нескольких модулей в качестве единой машины
Группа	логическое объединение нескольких объектов ДБ (например, подгрупп, АРМ, модулей WAF Dallas Lock и сетевых устройств). Модули ЕЦУ в составе АРМ удобно объединять в группы если у них совпадают параметры безопасности. Допускается создание любого числа вложенных групп
Доверенный домен безопасности	Домен безопасности, находящийся с ДБ в доверительных отношениях
Домен безопасности ЕЦУ	совокупность (кластер) одного или нескольких серверов в режиме репликации конфигурации. Представляет собой корневой уровень

	организации логической группировки модулей, сетевых устройств и подчиненных доменов безопасности ЕЦУ, предназначенный для осуществления централизованного управления всеми подчиненными объектами
Дерево домена безопасности	структурированное отображение объектов домена безопасности в виде иерархии в консоли ЕЦУ
Задание	некоторое действие, назначенное администратором для модуля ЕЦУ, которое модуль должен выполнить при первой же возможности. Тип заданий: получить отчет, создать файл конфигурации, обновить какое-либо программное обеспечение и т.д.
Модуль	представление отдельного продукта производства ООО «Конфидент»: • СЗИ Dallas Lock 8.0 редакции «К» и «С» (включая компоненты МЭ, СОВ); • СЗИ НСД Dallas Lock Linux; • СЗИ ВИ Dallas Lock; • СДЗ Dallas Lock; • шлюз безопасности WAF Dallas Lock; • Агент ЕЦУ. Каждый модуль может использоваться независимо от других
Консоль ЕЦУ	приложение, предназначенное для управления ЕЦУ Dallas Lock и доменом безопасности ЕЦУ
Кластер серверов ДБ	работа ДБ может обеспечиваться как одним сервером ЕЦУ Dallas Lock, так и несколькими. В последнем случае говорят о кластере серверов ДБ. Преимущество Кластера серверов ДБ в репликации конфигурации серверов, распределении нагрузки и отказоустойчивости
Локальное/Удаленное администрирование модуля	настройка, просмотр всех параметров модуля. Подключение производится через сеть. Для локального администрирования используется подключение по зарезервированному локальному IP-адресу *127.0.0.1* или доменному имени *localhost*
Оперативное управление	процесс управления модулем путем отправки команд, выполняемых на стороне модуля, и не требующих передачи результатов на ЕЦУ. Например, команда на выключение модуля
Подчиненный домен безопасности	домен безопасности, входящий в ДБ на более низком уровне иерархии
Репликация конфигурации	повторение функциональности серверов ЕЦУ для обеспечения отказоустойчивости и распределения нагрузки по возможности наиболее оптимальным образом
Синхронизация	процесс, в котором участвует сервер ЕЦУ Dallas Lock и модуль ЕЦУ. Заключается в приведении в соответствие параметров модуля ЕЦУ (списки пользователей, политики, и т.д.) параметрам, заданным в ДБ
Субъект доступа	сотрудник предприятия, у которого есть учетная запись. Учетная запись характеризуется логином, паролем, аппаратным идентификатором (АИ), расписанием, группой и т.д. Учетная запись должна быть единой для всех модулей ЕЦУ

Централизованное управление	совокупность таких функциональных возможностей ЕЦУ Dallas Lock, как: • отслеживание статуса модулей; • удаленное развертывание модулей на АРМ; • управление учетными записями, политиками и параметрами безопасности (включая синхронизацию); • сбор, хранение, анализ журналов; • оперативное управление; • выполнение заданий на модулях; • сигнализация

СОКРАЩЕНИЯ

Сокращение	Полная формулировка
АИ	аппаратный идентификатор
АИБ	администратор информационной безопасности
АРМ	автоматизированное рабочее место
ДБ	домен безопасности ЕЦУ
ДВК	датчик вскрытия корпуса
ДСЧ	датчик случайных чисел
ЕЦУ	Единый центр управления Dallas Lock
ЗПС	замкнутая программная среда
МЭ	межсетевой экран
НСД	несанкционированный доступ
ОС	операционная система
ПК	персональный компьютер
ПО	программное обеспечение
СДЗ	средство доверенной загрузки Dallas Lock
СЗИ	средство защиты информации
СЗИ ВИ	система защиты информации в виртуальных инфраструктурах
СОВ	система обнаружения вторжений
СУ	сетевое устройство
Сервер УД	сервер управления доступом
ТС	техническое средство
ФС	файловая система
ШОС	штатная операционная система
ЦУ СЗИ ВИ	Центр управления СЗИ ВИ Dallas Lock
AD	Active Directory
DL8.0	СЗИ Dallas Lock 8.0
SP (Service Pack)	пакет обновлений для ОС
WAF	web application firewall

ПРЕДСТАВЛЕНИЕ МОДУЛЕЙ В ИНТЕРФЕЙСЕ ЕЦУ

Модуль — представление отдельного продукта производства ООО «Конфидент», включающее обозначение итерации продукта (ИК) с порядковым номером (соответствует порядковому номеру очередной процедуры прохождения испытаний продуктом, вызванных внесением изменений в сертифицированное средство защиты информации).

Продукты производства ООО «Конфидент» полноценно взаимодействуют с ЕЦУ Dallas Lock в соответствии с настоящей инструкцией, начиная с версий, указанных в таблице.

Продукт	Наименование модуля	
	Основное обозначение	Поддерживается с версии (итерации)
СЗИ Dallas Lock 8.0 редакции «К» и «С» (включая компоненты МЭ, СОВ)	Dallas Lock 8.0	версия 8.0.689.0 (ИК8) и выше
СЗИ НСД Dallas Lock Linux	Dallas Lock Linux	версия 3807 (ИК2) и выше
СЗИ ВИ Dallas Lock	СЗИ ВИ Dallas Lock	версия 3.50 (ИК3) и выше
СДЗ Dallas Lock	СДЗ Dallas Lock	версии выше 222 (ИК4)
шлюз безопасности WAF Dallas Lock	по умолчанию соответствует системному имени хоста, может быть задано АИБ вручную	все версии
Агент ЕЦУ	Агент ЕЦУ	все версии

1 НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ ЕЦУ DALLAS LOCK

ЕЦУ Dallas Lock — единый кроссплатформенный центр управления, предназначенный для контроля целостности настроек сетевого оборудования и решения задач организации централизованного управления продуктами линейки ООО «Конфидент» (СЗИ Dallas Lock 8.0 редакции «К» и «С» (включая компоненты МЭ, СОВ), СЗИ НСД Dallas Lock Linux, СЗИ ВИ Dallas Lock редакции «Стандартная» и «Расширенная», СДЗ Dallas Lock, шлюз безопасности WAF Dallas Lock, Агент ЕЦУ), а также интеграция со сторонними продуктами (Антивирус Kaspersky, SIEM-системы).

1.1 Структура ЕЦУ

ЕЦУ Dallas Lock состоит из следующих основных компонентов:

1. **Серверный компонент ЕЦУ (Служба ЕЦУ).** Выполняет основные функции ЕЦУ:
   - обеспечивает централизованное оперативное управление и аудит модулей;
   - обеспечивает контроль и управление сетевыми устройствами;
   - позволяет объединять несколько серверов ЕЦУ в единую логическую единицу — кластер Домена безопасности;
   - обеспечивает работу механизма репликации конфигурации в рамках одного кластера ДБ;
   - позволяет объединять несколько ДБ в единую логическую единицу, имеющую структуру вложенности со связями типа «родитель-потомок».
2. **Консоль ЕЦУ.** Пользовательский интерфейс, предназначенный для управления настройками службы ЕЦУ, а также для отображения на экране информации о работе службы.

1.2 Возможности ЕЦУ

При работе с сетевым оборудованием доступны следующие возможности:

- сканирование сети для обнаружения SNMP- и SSH-клиентов;
- ввод/вывод сетевого оборудования в/из ДБ;
- выключение и перезагрузка сетевого оборудования;
- настройка контролируемых параметров;
- получение отчета о конфигурации сетевого оборудования;
- контроль изменений конфигурации сетевого оборудования;
- сигнализация о нарушении целостности.

При работе с модулями **СЗИ Dallas Lock 8.0 редакций «К» и «С»** доступны следующие возможности:

- завершение работы и перезагрузка модуля;
- отображение информации о состоянии модуля;
- синхронизация политик/пользователей;
- удаленное развертывание модуля на АРМ;
- управление пользователями и группами пользователей на модуле;
- управление политиками безопасности;
- управление заданиями на:
  - получение конфигурации;
  - применение конфигурации;
  - изменение параметров лицензии и технической поддержки;
  - проверку целостности контролируемых объектов;
- сбор журналов модуля;
- отправка сигнализации об инцидентах безопасности;
- включение неактивного режима работы модуля или компонентов;
- управление мандатными метками (только для Dallas Lock 8.0 редакции «С»);
- настройка аппаратных идентификаторов.

При работе с модулями **СЗИ НСД Dallas Lock Linux** доступны следующие возможности:

- завершение работы и перезагрузка модуля;
- отображение информации о состоянии модуля;
- синхронизация политик/пользователей;
- удаленное развертывание модуля на АРМ;

- управление пользователями и группами пользователей на модуле;
- управление политиками безопасности;
- управление заданиями на изменение параметров лицензии и технической поддержки;
- сбор журналов модуля;
- отправка сигнализации об инцидентах безопасности;
- настройка аппаратных идентификаторов.

При работе с модулями **СЗИ ВИ Dallas Lock** доступны следующие возможности:

- отображение информации о состоянии модуля;
- синхронизация политик/пользователей;
- управление пользователями и группами пользователей на модуле;
- управление политиками безопасности;
- настройка неактивного режима работы модуля;
- управление заданиями на:
  - проверка обновлений;
  - изменение параметров лицензии и технической поддержки;
  - получение конфигурации;
  - применение конфигурации;
  - получение отчета о конфигурации;
- сбор журналов модуля;
- отправка сигнализации об инцидентах безопасности.

При работе с модулем **СДЗ Dallas Lock** доступны следующие возможности:

- завершение работы и перезагрузка модуля;
- отображение информации о состоянии модуля (процент заполнения журнала, отслеживание событий ДВК, контроль версии установленной сборки, информация о модели платы и т. д.);
- синхронизация политик/пользователей;
- управление пользователями и группами пользователей на модуле;
- управление политиками безопасности;
- управление заданиями на:
  - очистку журнала;
  - получение конфигурации;
  - применение конфигурации;
  - получение отчета об аппаратном обеспечении;
  - получение отчета о конфигурации;
- сбор журналов модуля;
- отправка сигнализации об инцидентах безопасности;
- взаимодействие с агентом ШОС;
- настройка аппаратных идентификаторов.

При работе со шлюзом безопасности **WAF Dallas Lock** доступны следующие возможности:

- завершение работы и перезагрузка модуля;
- отображение информации о состоянии модуля (состояние подключения, режим работы, имя шлюза безопасности, IP-адрес шлюза безопасности, MAC-адрес подключения шлюза безопасности, данные об аппаратном обеспечении, версия ПО, версия базы решающих правил, объем свободного места на диске, номер лицензии, код технической поддержки);
- сброс временных блокировок;
- включение аварийного режима;
- включение штатного режима;
- открытие веб-интерфейса управления;
- управление заданиями на:
  - обновление базы решающих правил;
  - получение конфигурации;
  - применение конфигурации;
  - получение логов;
  - получение отчета об аппаратном обеспечении;
  - получение отчета о конфигурации;

    - сброс к заводским настройкам;
- сбор журналов модуля;
- отправка сигнализации об инцидентах безопасности.

При работе с модулем **Агент ЕЦУ** доступны следующие возможности:

- завершение работы и перезагрузка удаленной рабочей станции с установленным Агентом ЕЦУ;
- удаленное развертывание модуля на АРМ;
- удаленное подключение к рабочей станции с установленным Агентом ЕЦУ;
- управление заданиями на:
    - получение отчета об аппаратном обеспечении;
    - получение отчета о программном обеспечении;
    - удаление Агента ЕЦУ;
- сбор журналов с рабочей станции с установленным Агентом ЕЦУ;
- сбор отчетов об аппаратном и программном обеспечении с рабочей станции с установленным Агентом ЕЦУ;
- аудит подключений Агента ЕЦУ.

При работе с **Kaspersky Security Center** доступны следующие возможности:

- получение сведений о состоянии Антивируса Kaspersky на клиентских АРМ (версия, включен/выключен, статус обновления антивирусных баз);
- получение журналов Антивируса Kaspersky;
- получение информации об инцидентах (срабатываниях антивируса) на клиентских АРМ;
- запуск процесса обновления антивирусных баз данных на клиентских АРМ;
- выполнение принудительного сканирования (полной проверки) клиентских АРМ.

2 УСТАНОВКА И УДАЛЕНИЕ ЕЦУ DALLAS LOCK

2.1 Требования к аппаратному и программному обеспечению

ЕЦУ предназначен для использования на ТС, таких как: персональные компьютеры, портативные компьютеры (ноутбуки, планшеты), серверы и ТС с поддержкой виртуальных сред (по технологии VMware и пр.) и технологии Windows To Go[1], работающих на 64-битной архитектуре процессоров под управлением операционных систем семейства Windows (x64):

- Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
- Windows 8.1 (Core, Pro, Enterprise);
- Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
- Windows Server 2012 R2 (Foundation, Essentials, Standard, Datacenter);
- Windows 10 (Enterprise, Education, Pro, Home);
- Windows Server 2016 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server);
- Windows Server 2019 (Essentials, Standard, Datacenter);
- Windows 11 (Enterprise, Education, Pro, Home);
- Windows Server 2022 (Standard, Datacenter);

и семейства GNU Linux[2] (x64):

- Debian 10;
- Debian 11;
- CentOS 7;
- Red Hat Enterprise Linux Server 7;
- Ubuntu 18.04 LTS;
- Ubuntu 20.04 LTS;
- Astra Linux Common Edition (Орел) 2.12;
- Astra Linux Special Edition (Смоленск) 1.6;
- Astra Linux Special Edition (Смоленск) 1.7;
- Альт Сервер 9;
- Альт Сервер 10;
- Альт Сервер 10.1;
- Альт Рабочая Станция 9.0;
- Альт Рабочая Станция 9.1;
- Альт Рабочая Станция 9.2;
- Альт Рабочая Станция 10.0;
- Альт Рабочая Станция 10.1;
- Альт Рабочая Станция К 10.0;
- Альт Рабочая Станция К 10.1;
- РЕД ОС 7.3 Муром.

Установка ЕЦУ невозможна на операционные системы без графического интерфейса. На ОС должны быть установлены все актуальные обновления. В противном случае может появиться ошибка с просьбой установить обновления и повторить установку ЕЦУ.

Требуемый объем свободного дискового пространства для установки ЕЦУ: 1 Гб.

Для ОС семейства Linux необходимо наличие свободного места в разделе /opt.

Внимание! Сама программа занимает достаточно мало места на диске, но необходимо заранее дополнительно зарезервировать место на диске для организации хранения журналов.

[1] Поддержка технологии Windows To Go осуществляется только для Консоли ЕЦУ Dallas Lock.

[2] Для инсталляции и работы с ЕЦУ под ОС семейства Linux требуется графическая оболочка.

Примечание. Для хранения журналов во внешней базе данных необходимо использовать PostgreSQL версии 13 или выше.

ЕЦУ Dallas Lock позволяет в качестве средства опознавания пользователей использовать следующие аппаратные идентификаторы:

- электронные ключи Touch Memory (iButton)[3]:
  - DS-1992;
  - DS-1993;
  - DS-1995;
  - DS-1996.
- USB-ключи Aladdin eToken[4];
  - Pro/Java;
  - 72K;
- смарт-карты Aladdin eToken Pro/SC;
- USB-ключи и смарт-карты Рутокен (Rutoken):
  - Рутокен (Rutoken);
  - Рутокен (Lite);
  - Рутокен ЭЦП;
  - Рутокен ЭЦП 2.0;
  - Рутокен ЭЦП 3.0;
  - Рутокен ЭЦП PKI;
  - Рутокен S[5]
- USB-ключи и смарт-карты JaCarta:
  - JaCarta SF/ГОСТ;
  - JaCarta ГОСТ;
  - JaCarta PKI;
  - JaCarta PKI/Flash;
  - JaCarta LT;
  - JaCarta PRO;
  - JaCarta-2 PKI/ГОСТ;
  - JaCarta-2 ГОСТ;
- USB-ключи и смарт-карты ESMART:
  - ESMART Token;
  - ESMART Token ГОСТ;
  - ESMART 64K.

При настройке аппаратного идентификатора рекомендуется устанавливать драйверы, поставляемые в комплекте с идентификатором, или скачать их с сайта производителя.

Примечание. Для работы электронных ключей Touch Memory (iButton) на APMax с ОС Windows необходимы драйверы «Prolific USB-to-Serial Common Port» (данные драйверы уже могут быть в составе ОС, или их можно скачать с сайта производителя драйверов Prolific).

---

[3] Для ОС Linux электронный ключ Touch Memory (iButton) поддерживается только для чтения, то есть можно только назначить пользователю. Запись учетных данных пользователя на такой идентификатор не производится.

[4] Для USB-ключа eToken 32Кб обеспечивается только возможность усиления механизма аутентификации. Запись учетных данных пользователя на такой идентификатор не производится в силу ограниченного объема доступной памяти аппаратного идентификатора.

[5] Для ОС Linux недоступно форматирование ключа.

Примечание. Для работы электронных ключей Touch Memory (iButton) на АРМах с ОС Linux (кроме ALT Linux), необходимо разрешить обычному пользователю работать с COM-портами. Для этого достаточно поместить пользователя в группу *dialout,* с помощью команды *sudo usermod -a -G dialout $USER*, затем перезагрузить АРМ.

Примечание. Для корректной работы аппаратных идентификаторов eToken необходимо использовать драйверы SafeNet. Версия драйвера SafeNet для работы с аппаратными идентификаторами eToken в операционных системах семейства Windows должна быть не выше 10.0.43. Для операционных систем семейства GNU Linux следует использовать версию драйвера SafeNet — 10.0.37.

Примечание. В связи с особенностью устройства JaCarta-2 ГОСТ, операция форматирования аппаратных идентификаторов данного типа должна выполняться только с использованием ПО «Единый Клиент JaCarta».

2.2 Установка ЕЦУ Dallas Lock

Для одной Службы ЕЦУ можно установить несколько Консолей ЕЦУ на другие АРМ сети. Таким образом, можно будет управлять Доменом безопасности ЕЦУ с разных устройств.

Внимание! В DNS-сервере должна быть только одна запись об АРМ, на котором будет развернут сервер ЕЦУ.

Внимание! Для идентификации сервера ЕЦУ в сети по умолчанию используется имя ПК, на который он был установлен:

1. Изменение имени ПК после установки на него службы ЕЦУ не допускается.
2. Для корректного подключения к серверу ЕЦУ модулей, установленных на ПК с ОС Windows и ОС Linux, службу ЕЦУ рекомендуется устанавливать на ПК, имя которого соответствует кодировке ASCII. В противном случае потребуется внесение изменений на стороне используемого DNS-сервера. Например, если в корпоративной сети используется DNS-сервер Microsoft, то для корректного разрешения имен со стороны модулей на ПК с ОС Linux, необходимо добавить A-запись с именем сервера ЕЦУ, закодированным в пьюникоде (punycode).

Примечание. Перед установкой ЕЦУ требуется проверить, что происходит получение IP-адреса компьютера по сетевому имени данного ПК. Для этого необходимо выполнить следующие действия:

1. Получить сетевое имя сервера, для этого запустить терминал и выполнить команду «*hostname*».
2. Проверить доступность по сетевому имени, выполнив команду «*ping <сетевое имя ПК>*».
3. Выполнить команду «*traceroute <IP-адрес ПК>*» (для ОС семейства Linux) или «*tracert <IP-адрес ПК>*» (для ОС семейства Windows) и проверить, что полученное имя совпадает с выводом команды «*hostname*» на шаге 1.

В случае несовпадения имен следует откорректировать переменную *hostname*, для этого:

1. Для Linux: выполнить команду «*hostnamectl set-hostname <сетевое имя ПК>*».
2. Для Windows: переименовать имя компьютера с помощью панели управления.

Примечание. Способ хранения журналов допускается выбрать в процессе установки ЕЦУ Dallas Lock, так и после его установки.

В ЕЦУ Dallas Lock реализованы следующие варианты смены места хранения журналов:

1. С Внутренней системы хранения на внешний/локальный PostgreSQL-сервер (доступно только для одиночного сервера ЕЦУ);
2. С хранения на внешнем/локальном PostgreSQL-сервере на Внутреннюю систему хранения (доступно только для одиночного сервера ЕЦУ);
3. Менять БД в рамках одного PostgreSQL-сервера;
4. Менять один PostgreSQL-сервер на другой;
5. Возвращаться на используемые ранее БД (на внешнем/локальном PostgreSQL-сервере).

Подробнее о настройке способа хранения журналов описано в разделе «Параметры хранения журналов»

Примечание. Для подключения внешнего сервера с базой данных PostgreSQL, на стороне внешнего сервера должно быть настроено разрешающее правило фильтрации на входящее соединение. Необходимо открыть TCP-порт 5432.

2.2.1 Порядок установки ЕЦУ Dallas Lock в ОС семейства Windows

Внимание! Устанавливать ЕЦУ Dallas Lock может только пользователь, обладающий правами администратора на данном компьютере. Это может быть локальный или доменный пользователь.

Локальную установку необходимо выполнять только из-под сессии текущего авторизованного пользователя. Запуск установки от имени другого пользователя (Run as) не допускается.

Примечание. В процессе установки ЕЦУ Dallas Lock будет произведена автоматическая настройка брандмауэра Windows (Windows Firewall).

Для серверных версий Windows при включенном Windows Firewall требуется дополнительная настройка правил для обеспечения корректного взаимодействия службы и консоли ЕЦУ. Для выполнения настройки необходимо:

1. Запустить оболочку Windows PowerShell с повышающими привилегиями от учетной записи администратора ОС.
2. Выполнить следующие команды в консоли:
   - «*New-NetFirewallRule -DisplayName "Dallas Lock: сервер ЕЦУ - входящие TCP" -Direction Inbound -Program "C:\Program Files\UCC\UcMainCore.exe" -Protocol TCP -Action Allow*»;
   - *«New-NetFirewallRule -DisplayName "Dallas Lock: сервер ЕЦУ - входящие UDP" -Direction Inbound -Program "C:\Program Files\UCC\UcMainCore.exe" -Protocol UDP -Action Allow»;*
   - *«New-NetFirewallRule -DisplayName "Dallas Lock: сервер ЕЦУ - исходящие TCP" -Direction Outbound -Program "C:\Program Files\UCC\UcMainCore.exe" -Protocol TCP -Action Allow»;*
   - *«New-NetFirewallRule -DisplayName "Dallas Lock: сервер ЕЦУ - исходящие UDP" -Direction Outbound -Program "C:\Program Files\UCC\UcMainCore.exe" -Protocol UDP -Action Allow»;*
   - *«New-NetFirewallRule -DisplayName "Dallas Lock: консоль ЕЦУ - входящие TCP" -Direction Inbound -Program "C:\Program Files\UCC\UcConsole.exe" -Protocol TCP -Action Allow»;*
   - *«New-NetFirewallRule -DisplayName "Dallas Lock: консоль ЕЦУ - входящие UDP" -Direction Inbound -Program "C:\Program Files\UCC\UcConsole.exe" -Protocol UDP -Action Allow»;*
   - *«New-NetFirewallRule -DisplayName "Dallas Lock: консоль ЕЦУ - исходящие TCP" -Direction Outbound -Program "C:\Program Files\UCC\UcConsole.exe" -Protocol TCP -Action Allow»;*
   - *«New-NetFirewallRule -DisplayName "Dallas Lock: консоль ЕЦУ - исходящие UDP" -Direction Outbound -Program "C:\Program Files\UCC\UcConsole.exe" -Protocol UDP -Action Allow».*

Примечание. Если в процессе установки ЕЦУ Dallas Lock планируется использовать лицензию, записанную на АИ Rutoken Lite, то необходимо перед установкой заранее установить драйверы производителя.

Для установки ЕЦУ Dallas Lock в ОС семейства Windows необходимо:

1. Запустить установочный файл *«uccInst.exe»*, который находится в корневой директории дистрибутива (или выбрать данное действие в меню окна *autorun*).

   Если ЕЦУ Dallas Lock устанавливается на ПК, не оснащенный приводом компакт-дисков, а дистрибутив поставляется именно на CD-диске, то можно скопировать с диска необходимый установочный файл на данный ПК любым удобным способом: через ЛВС, USB-Flash накопитель и др.

   После запуска программы установки необходимо выполнять действия по подсказкам программы. Выполнение следующего шага установки выполняется с помощью кнопки «Далее». На каждом шаге установки предоставляется возможность отмены установки с возвратом произведенных изменений. Для этого служит кнопка «Отмена».

Примечание. Если ранее была установлена отдельная Консоль ЕЦУ, то ее надо удалить (см. «Порядок удаления ЕЦУ Dallas Lock в ОС семейства Windows») и поставить заново вместе с установкой службы ЕЦУ.

Примечание. Возможно подключение между Консолью ЕЦУ и Службой ЕЦУ разных версий.

2. После запуска приложения на экране будет выведено окно для подтверждения операции. После подтверждения запустится мастер установки ЕЦУ Dallas Lock (рис. 1).

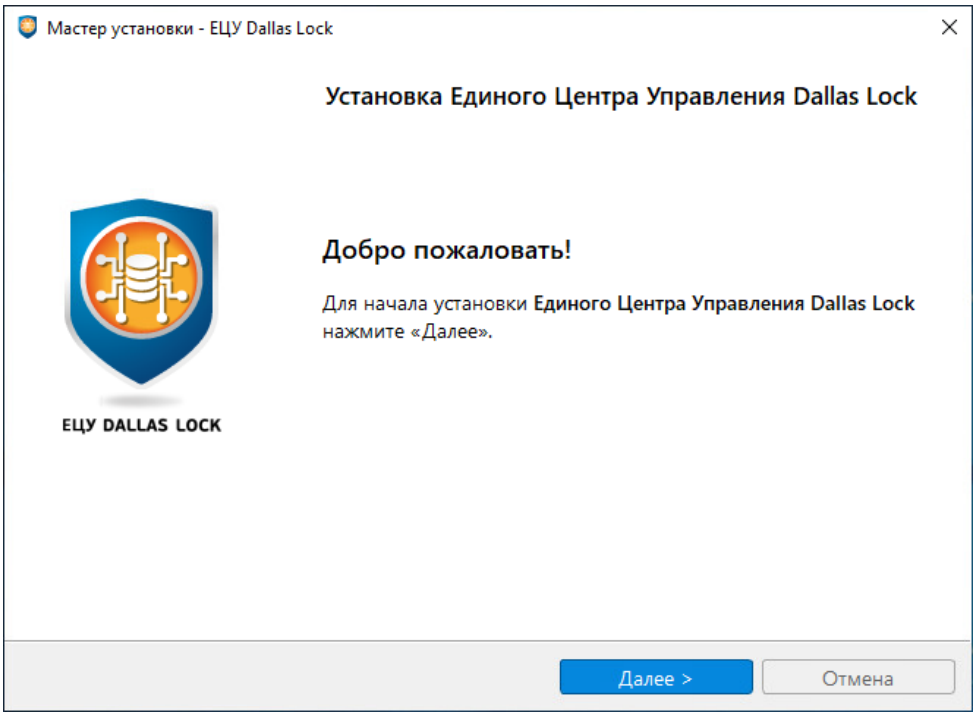

Рис. 1. Окно начала установки ЕЦУ Dallas Lock

Для продолжения установки нажать кнопку «Далее».

3. Выбрать компоненты, которые будут установлены (рис. 2).

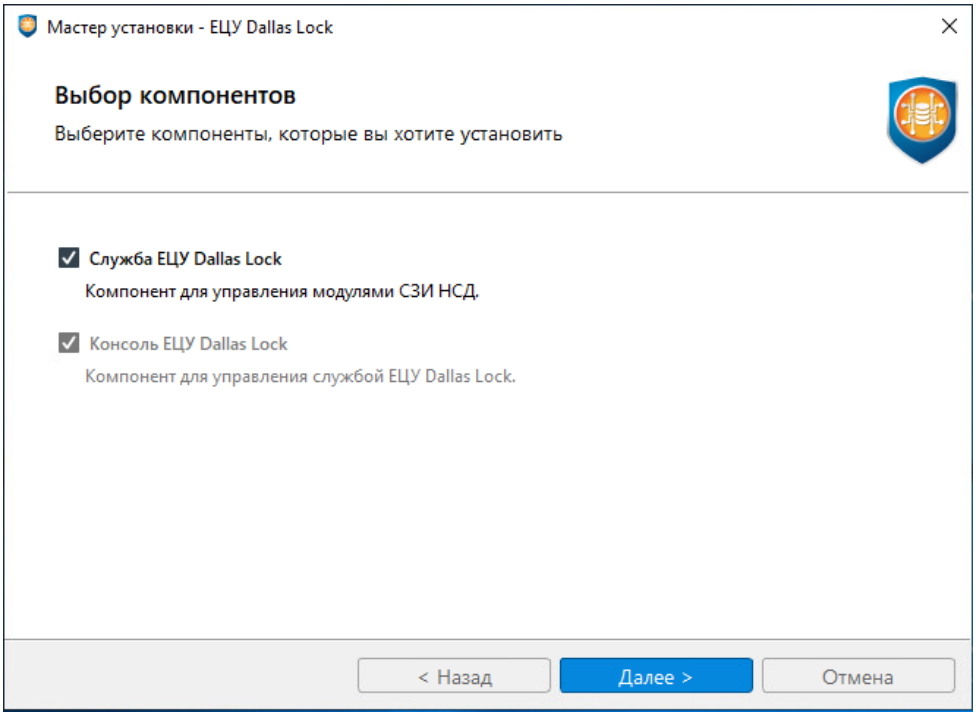

Рис. 2. Выбор компонентов для установки ЕЦУ Dallas Lock

Примечание. Служба ЕЦУ использует подключение TCP/IP по порту 17900. Установка нескольких экземпляров Службы ЕЦУ на одном ПК не допускается.

4. На следующем шаге установки необходимо предъявить аппаратный ключ, входящий в комплект поставки, для применения лицензии на устанавливаемый сервер (рис. 3).

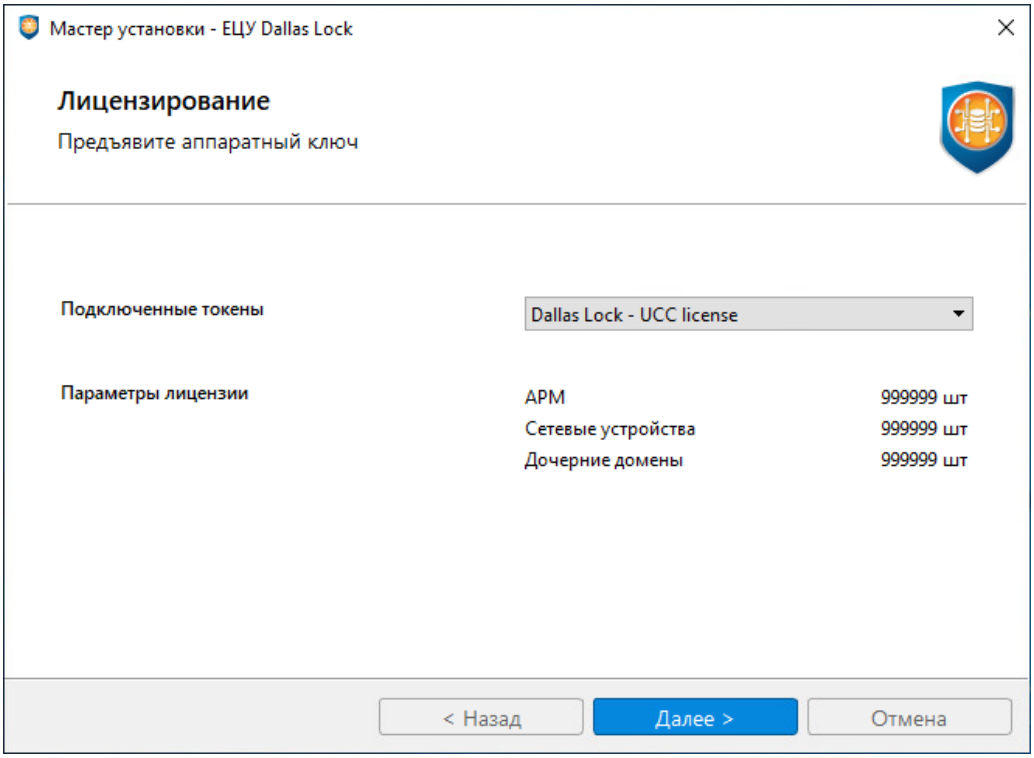

Рис. 3. Предъявление аппаратного ключа

5. Выбрать тип создаваемого домена в зависимости от цели установки ЕЦУ Dallas Lock (рис. 4). Описание установки подчиненного Домена безопасности и сервера репликации см. в разделах «Ввод ДБ в подчинение в процессе установки» и «Параметры кластера ДБ» соответственно.

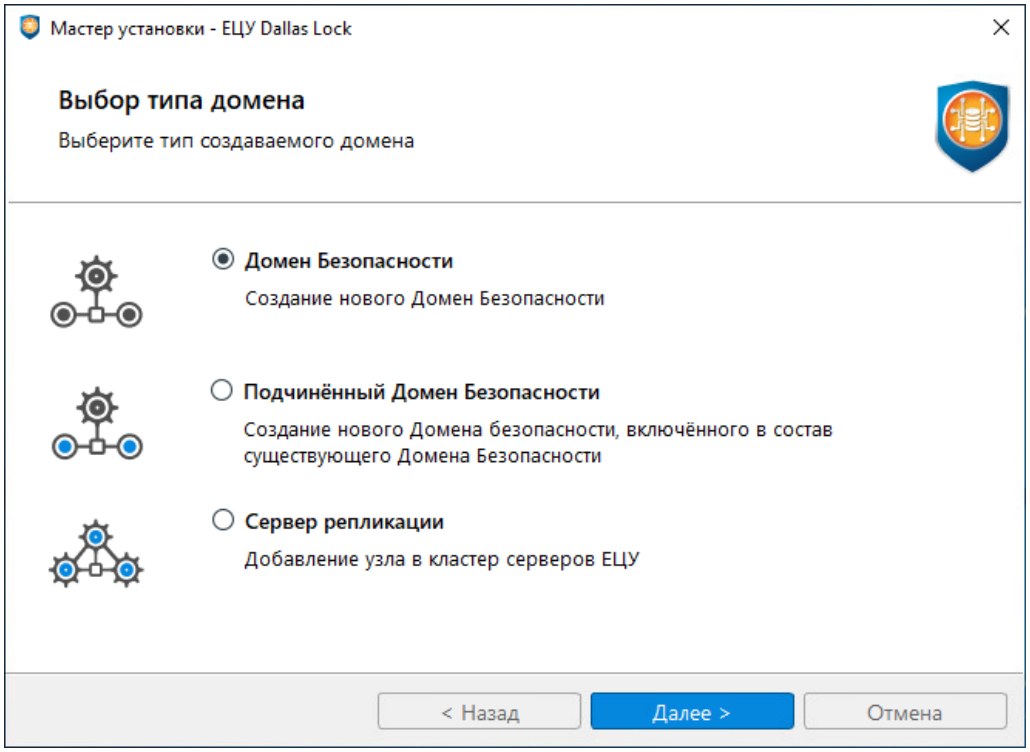

Рис. 4. Выбор типа создаваемого домена

6. Задать параметры ДБ (рис. 5):

- в поле «Название ДБ» указать имя ДБ;
- в поля «Ключ доступа» и «Подтвердите ключ доступа» ввести ключ доступа.

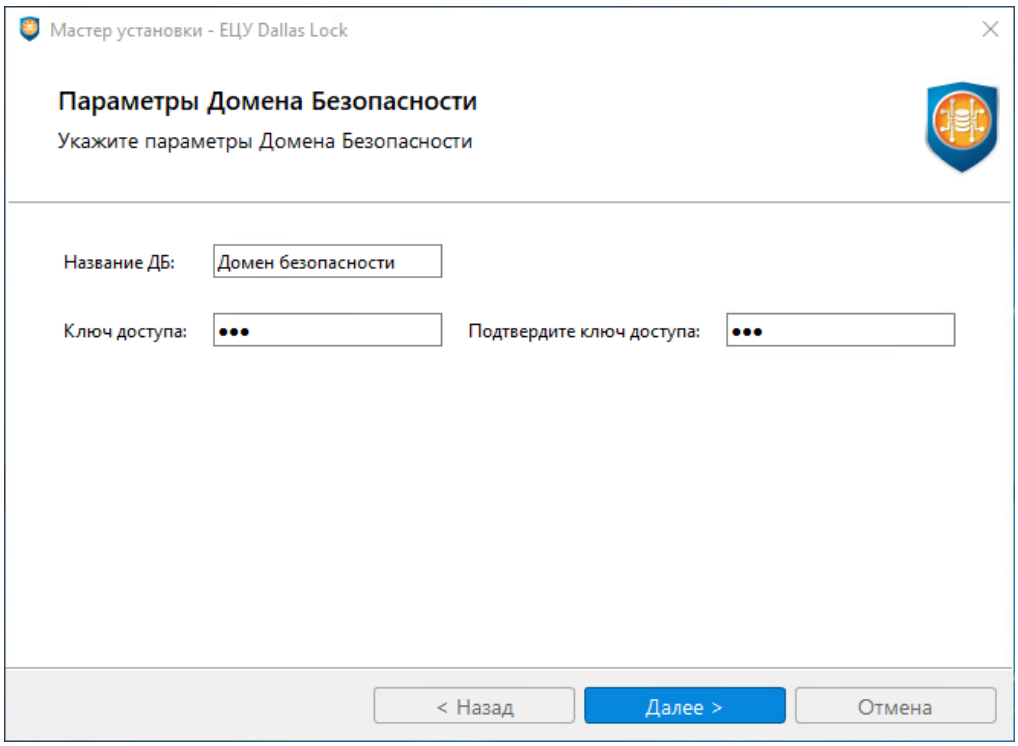

Рис. 5. Настройка параметров ДБ

Примечание. Ключ доступа к ДБ предназначен для ввода новых объектов в ДБ.

7. Задать параметры учетной записи администратора ДБ (рис. 6).

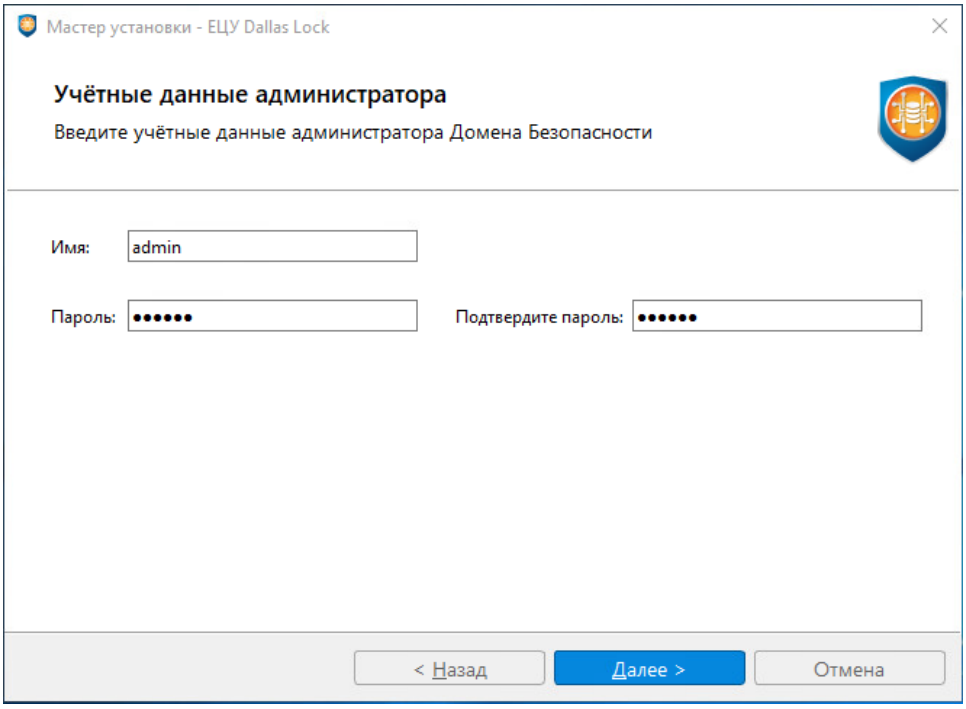

Рис. 6. Настройка параметров учетной записи администратора ДБ

8. Опционально поставить флаг и заполнить поля для использования базы данных PostgreSQL (рис. 7). Если используется внешний сервер с базой данных PostgreSQL, на его стороне должно быть настроено разрешающее правило фильтрации на входящее соединение. Необходимо открыть TCP-порт 5432.

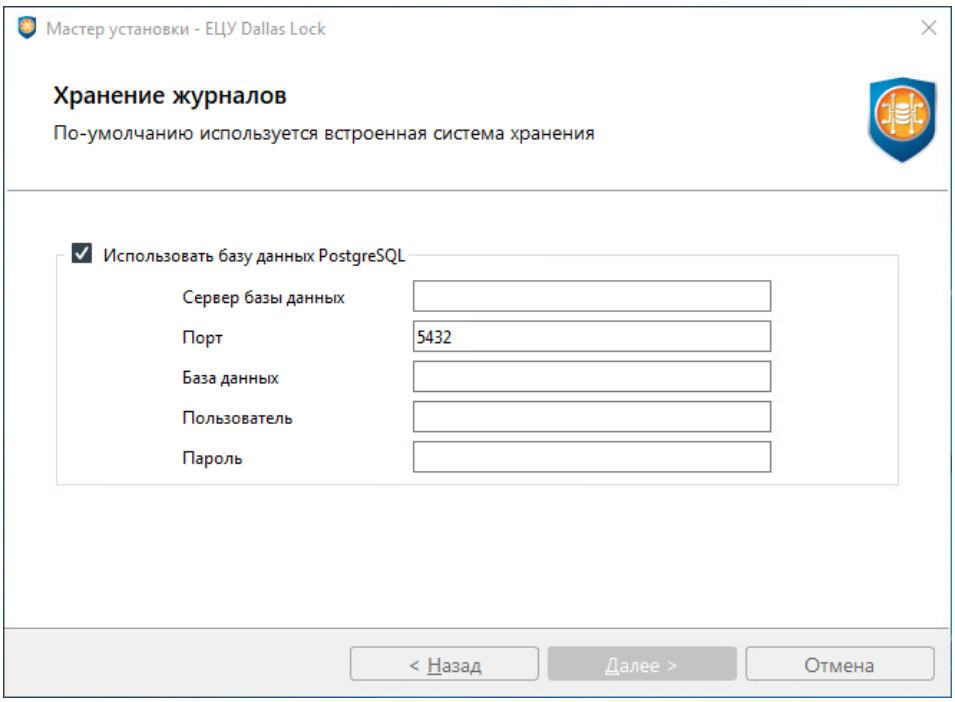

Рис. 7 Настройка базы данных PostgreSQL

Внимание! Пользователь, который указывается при подключении базы данных PostgreSQL, должен обладать полными правами на используемую БД. Сделать это можно следующей командой:

- *«GRANT ALL PRIVILEGES ON DATABASE <database_name> TO <user_name>».*

Примечание. Если при попытке установить ЕЦУ Dallas Lock с выбранной опцией «Использовать базу данных PostgreSQL» появляются нечитаемые ошибки, то в ОС с помощью панели управления следует установить русский язык для параметра «Язык программ, неподдерживаемых Юникод».

9. Проверить параметры установки и нажать кнопку «Установить» (рис. 8).

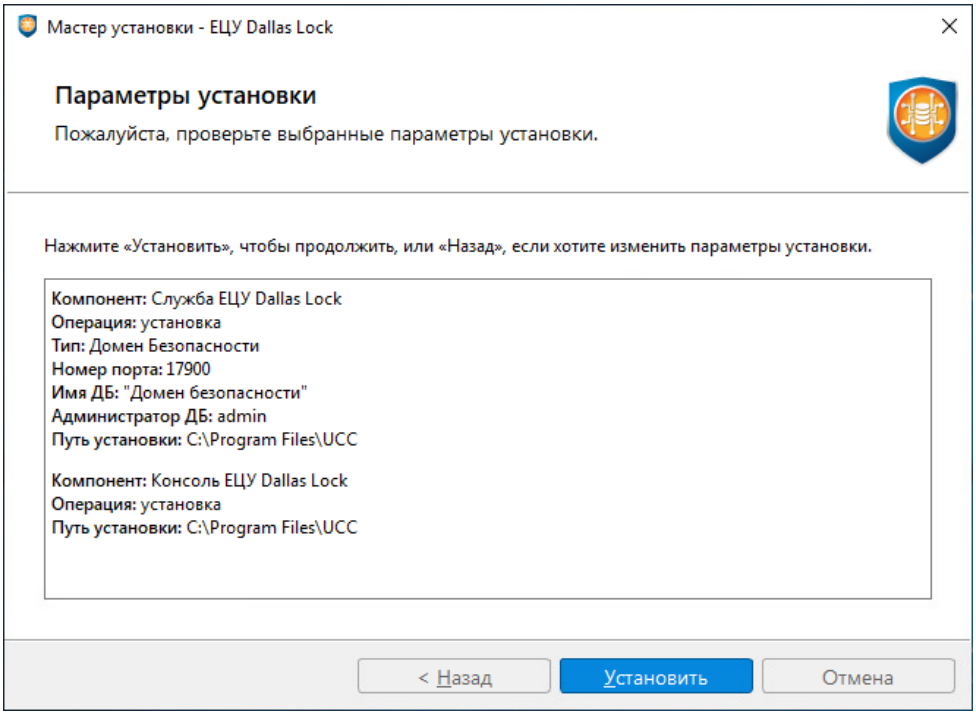

Рис. 8. Проверка параметров установки

10. Далее возможно наблюдать за процессом установки (рис. 9). Если процесс прошел без ошибок, необходимо нажать кнопку «Далее», чтобы перейти к окну завершения процесса установки.

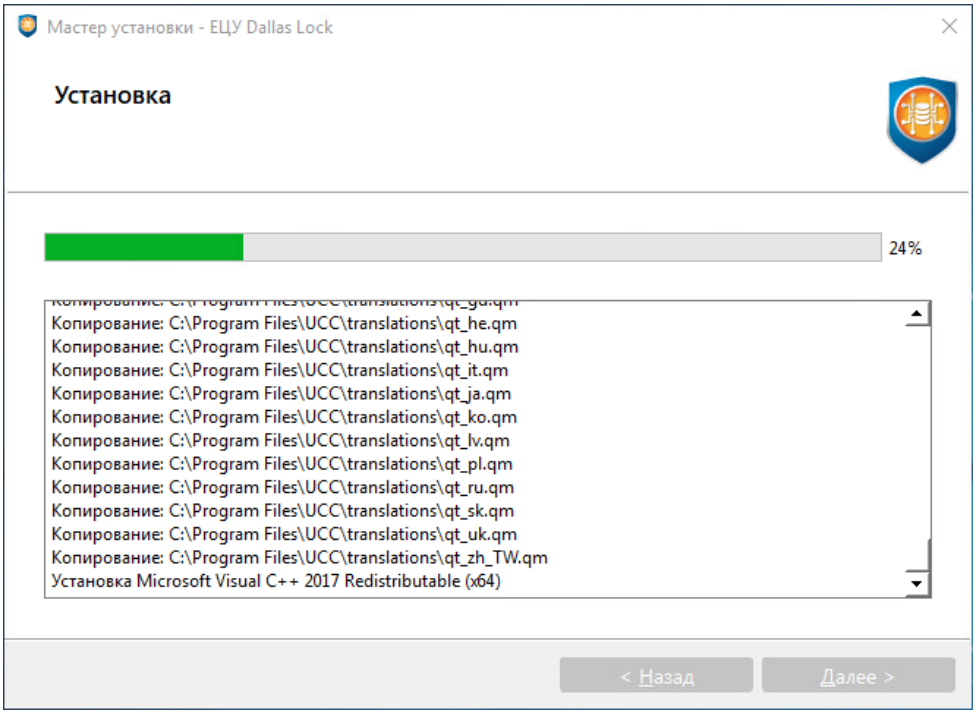

Рис. 9. Процесс установки ЕЦУ Dallas Lock

11.Нажать кнопку «Завершить» (рис. 10).

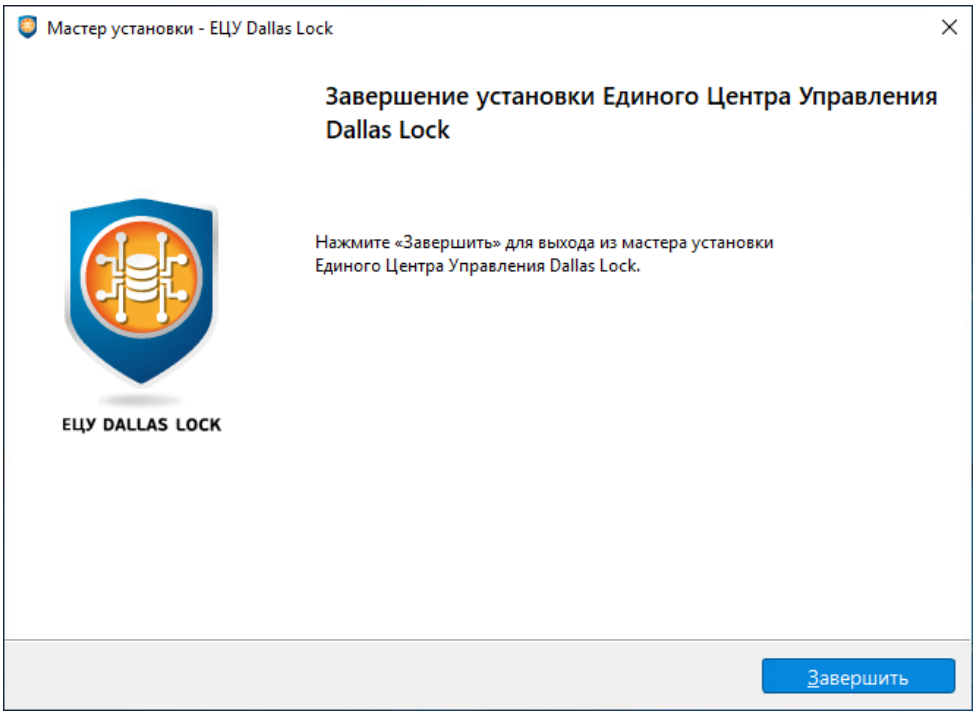

Рис. 10. Завершение процесса установки

После завершения процесса установки ЕЦУ Dallas Lock на рабочем столе и в меню «Пуск» появится ярлык Консоли ЕЦУ Dallas Lock (рис. 11).

Рис. 11. Ярлык консоли ЕЦУ Dallas Lock

2.2.2 Порядок установки ЕЦУ Dallas Lock в ОС семейства Linux

Примечание. Если ранее была установлена отдельная Консоль ЕЦУ, то ее нужно удалить (см. «Порядок удаления ЕЦУ Dallas Lock в ОС семейства Linux») и поставить заново вместе с установкой службы ЕЦУ.

Примечание. Если ЕЦУ Dallas Lock устанавливается на ТС, на котором также используется СЗИ НСД Dallas Lock Linux, то в настройках межсетевого экрана необходимо открыть TCP-порт 17900.

Примечание. Если в процессе установки ЕЦУ Dallas Lock планируется использовать лицензию, записанную на АИ Rutoken Lite, то необходимо перед установкой заранее установить драйверы производителя[6]. Для этого:

1. Скачать и установить драйверы с сайта производителя.
2. Установить соответствующие библиотеки *PKCS#11* (без этого действия мастер установки не сможет считать лицензию с АИ).

Внимание! При установке ЕЦУ Dallas Lock на АРМ с ОС «Astra SE» для разделов, которые ЕЦУ Dallas Lock использует для функционирования, необходимо отключить такие опции монтирования как: *noexec*, *nodev*, *nosuid*. В противном случае установка ЕЦУ Dallas Lock будет завершаться с ошибкой.

Для установки ЕЦУ Dallas Lock в ОС семейства Linux необходимо:

1. Скопировать в домашний каталог пользователя установочный файл «uccInst», который находится в корневой директории дистрибутива.

   Если ЕЦУ Dallas Lock устанавливается на ПК, не оснащенный приводом компакт-дисков, а дистрибутив поставляется именно на CD-диске, то можно скопировать с диска необходимый установочный файл на данный ПК любым удобным способом: через ЛВС, USB-Flash накопитель и др.
2. Проверить, является ли файл «*uccInst*» исполняемым:
   - либо с помощью команды *ls –l.*

     Пример:

     ls -l <enter>

     rw-rw---- отображаются последовательно без пробелов флаги владельца, флаги группы, флаги всех остальных пользователей. В данном примере файл не является исполняемым ни для владельца, ни для группы, ни для всех остальных пользователей.
   - Либо, можно открыть свойства файла, перейти на вкладку «Права» и убедиться, что в поле «Выполнение» поставлен флаг (рис. 12).

   Если файл не является исполняемым, необходимо поставить флаг в поле «Выполнение».

[6] Для работы ЕЦУ Dallas Lock на Astra Special Edition (Смоленск) 1.6 и Astra Special Edition (Смоленск) 1.7 в режиме ЗПС необходимо использовать драйверы производителя версии 2.4.0.0.

Или использовать команду *chmod a+x <путь к файлу>.run.*

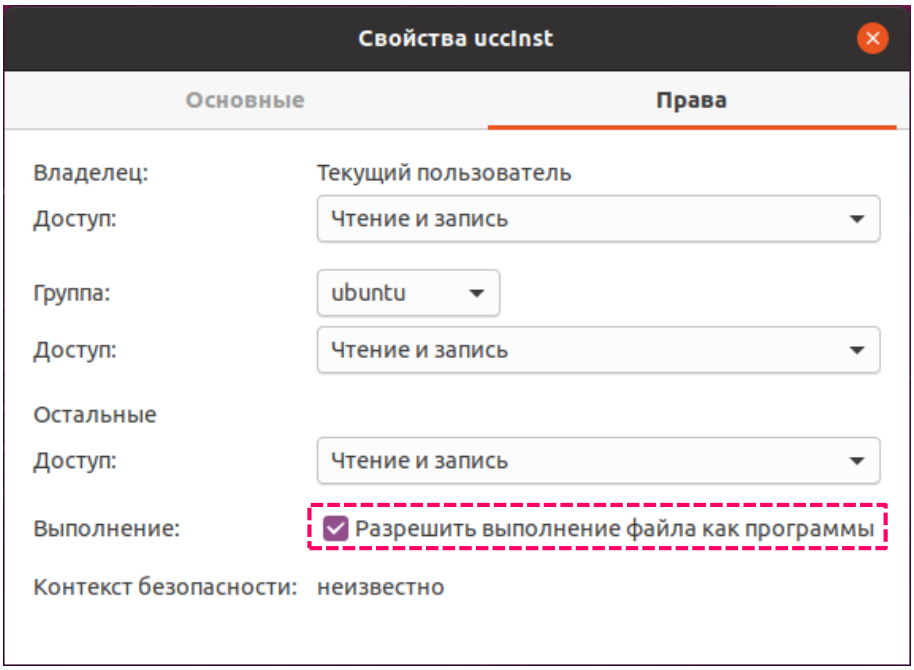

Рис. 12. Добавление прав на выполнение файла программы

3. Запустить файл дистрибутива.
4. После запуска приложения на экране будет выведено окно, в котором необходимо указать пароль пользователя (рис. 13).

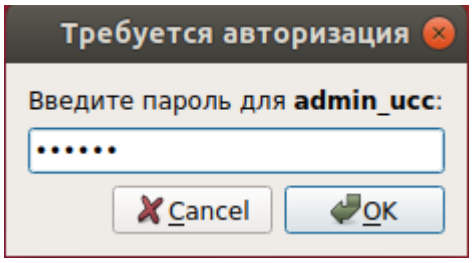

Рис. 13. Запуск программы установки

После нажатия кнопки «ОК» запустится мастер установки ЕЦУ Dallas Lock (рис. 14).

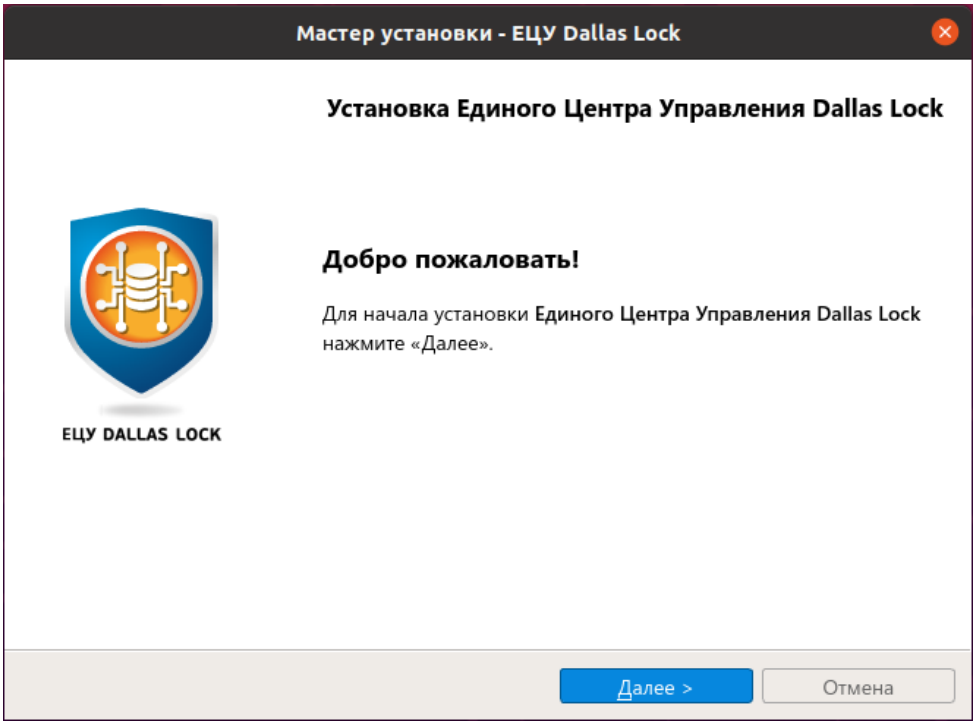

Рис. 14. Окно начала установки ЕЦУ Dallas Lock

Далее порядок установки ЕЦУ Dallas Lock аналогичен порядку установки данной программы в ОС семейства Windows (см. «Порядок установки ЕЦУ Dallas Lock в ОС семейства Windows»).

Примечание. Возможно подключение между Консолью ЕЦУ и Службой ЕЦУ разных версий.

После завершения процесса установки ЕЦУ Dallas Lock в списке приложений появится ярлык Консоли ЕЦУ Dallas Lock «Консоль ЕЦУ» (рис. 15).

Рис. 15. Ярлык консоли ЕЦУ Dallas Lock

Примечание. 1) Если на АРМ с Linux уже установлены сторонние СЗИ или драйверы на другие аппаратные идентификаторы, и при этом в процессе установки ЕЦУ произошла ошибка установки, которая связана с пакетным менеджером, то может помочь команда *sudo apt --fix-broken install*.
2) Если в процессе установки ЕЦУ на Linux возникает ошибка вида: "...error whiel loading shared libaries: libxcb-xkb.so.1: cannot open shared object file: No such file or directory", то необходимо перед установкой вручную установить пакет "libxcb-xkb1.

2.3 Удаление ЕЦУ Dallas Lock

Примечание. Удаление сервера ЕЦУ Dallas Lock, являющегося членом кластера репликации или состоящего в подчинении у другого Домена, не допускается. Перед удалением сервер ЕЦУ Dallas Lock необходимо вывести из кластера/подчинения соответственно.

2.3.1 Порядок удаления ЕЦУ Dallas Lock в ОС семейства Windows

Правом на удаление ЕЦУ Dallas Lock обладает пользователь с правами администратора ДБ.
В ОС Windows необходимо открыть «Пуск» → «Панель управления» → «Программы и компоненты». В появившемся окне из списка выбрать программу «ЕЦУ Dallas Lock», нажать «Удалить» и подтвердить удаление (рис. 16).

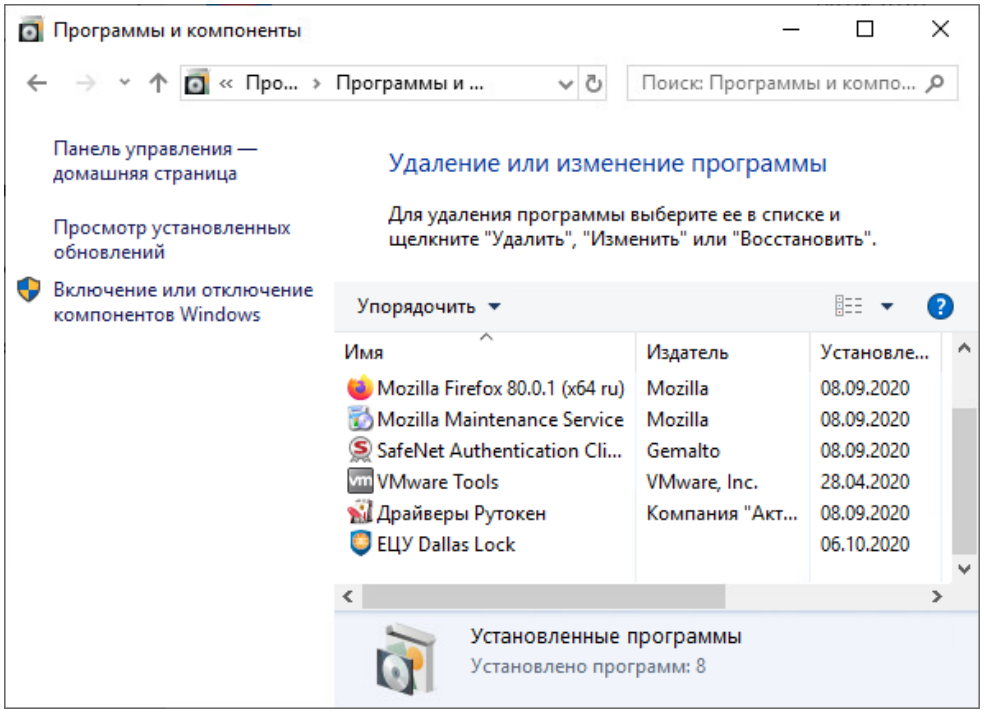

Рис. 16. Удаление ЕЦУ Dallas Lock

1. После подтверждения запустится мастер удаления ЕЦУ Dallas Lock (рис. 17). Для продолжения удаления нажать кнопку «Далее».

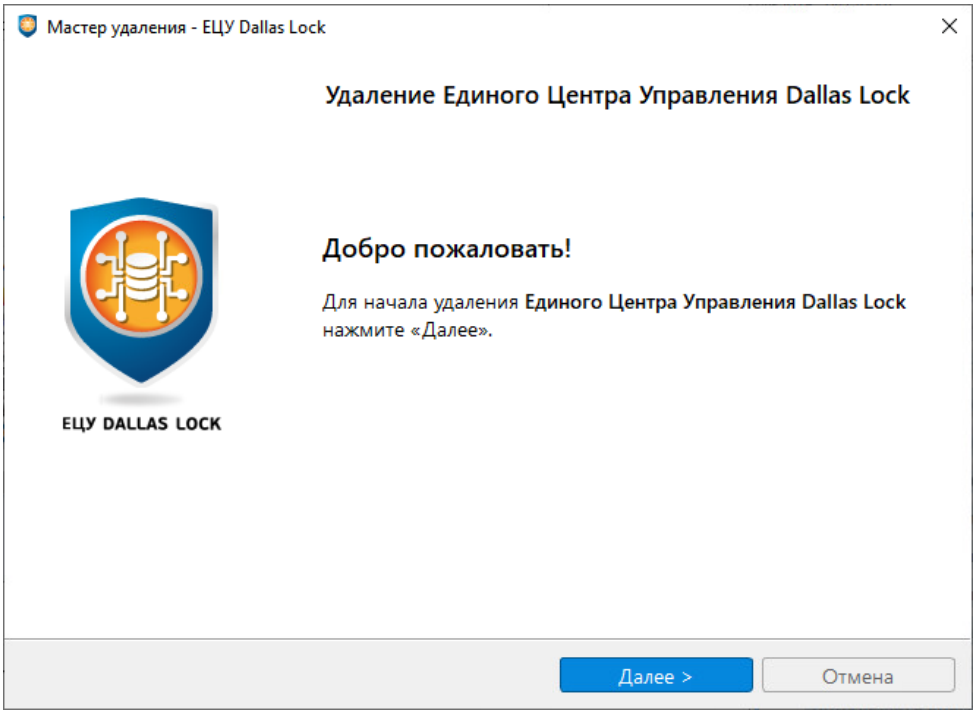

Рис. 17. Окно начала удаления ЕЦУ Dallas Lock

2. Выбрать компоненты, которые будут удалены (рис. 18).

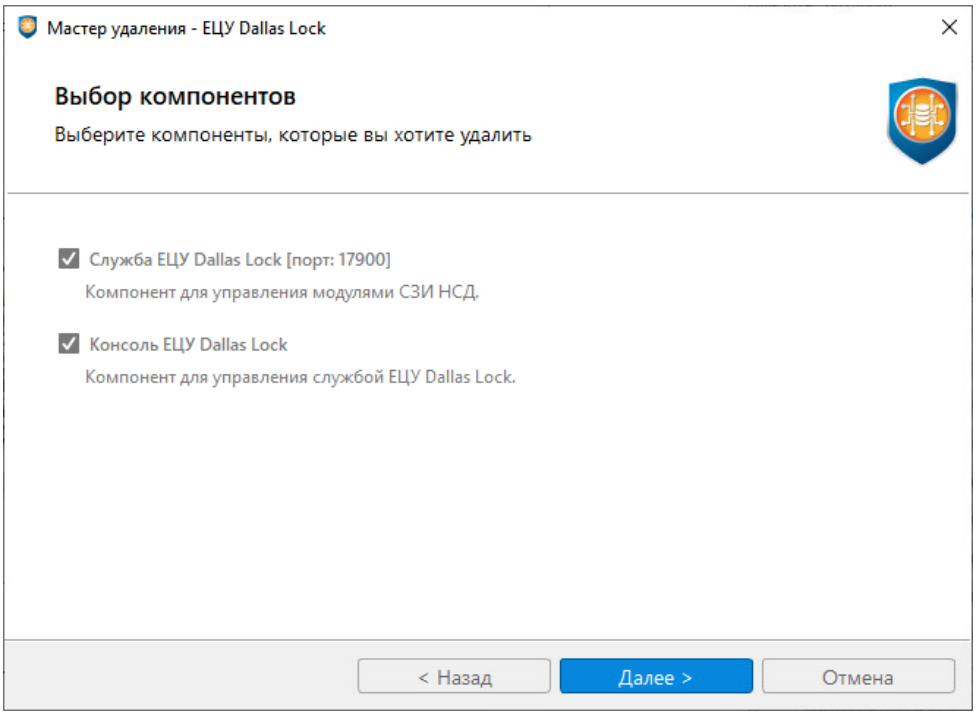

Рис. 18. Выбор компонентов для удаления ЕЦУ Dallas Lock

3. Подтвердить удаление конфигурационных файлов (рис. 19).

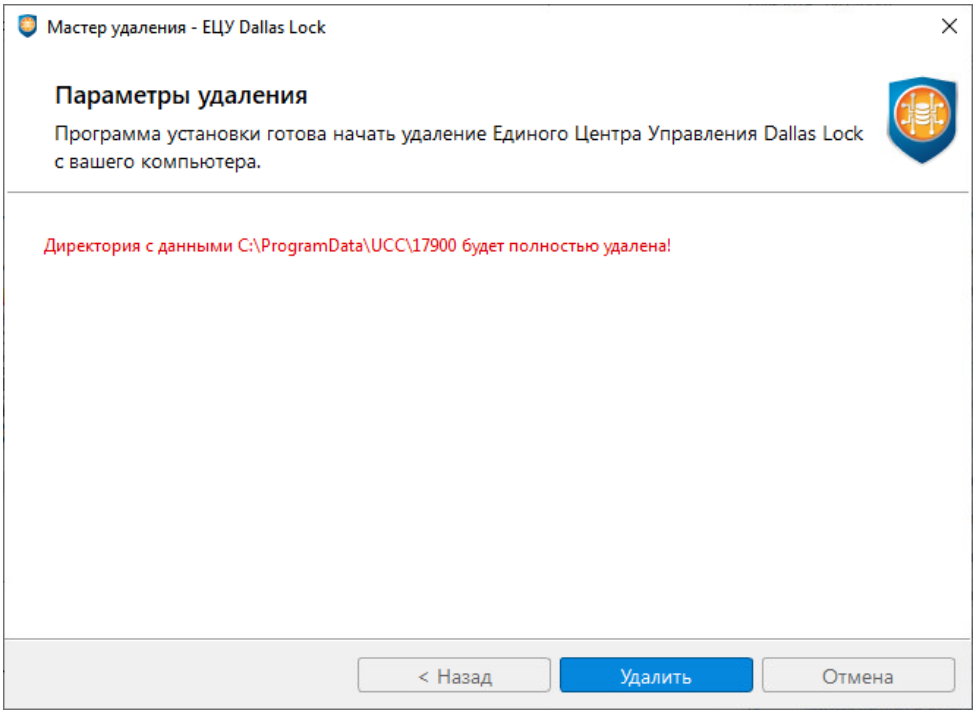

Рис. 19. Параметры удаления

4. Далее возможно наблюдать за процессом удаления (рис. 20). Если процесс прошел без ошибок, необходимо нажать кнопку «Далее», чтобы перейти к окну завершения процесса удаления.

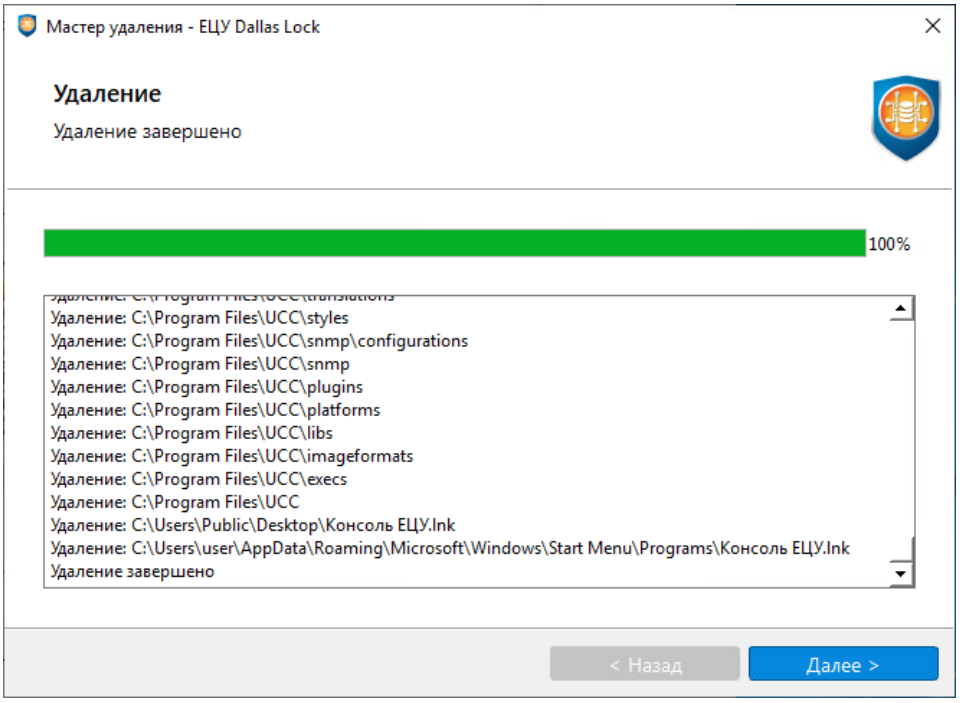

Рис. 20. Процесс удаления ЕЦУ Dallas Lock

5. Нажать кнопку «Завершить» (рис. 21).

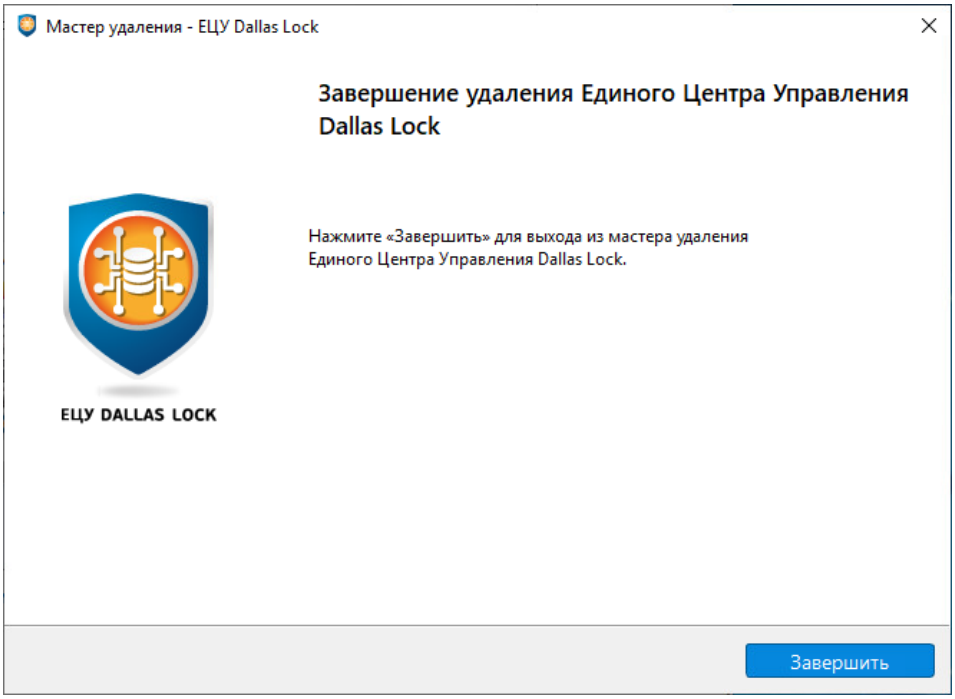

Рис. 21. Завершение процесса удаления

2.3.2 Порядок удаления ЕЦУ Dallas Lock в ОС семейства Linux

Для удаления ЕЦУ Dallas Lock необходимо обладать правами администратора операционной системы (root) на данном ПК.

1. Для удаления ЕЦУ Dallas Lock необходимо запустить исполняемый файл *uccUninst*, который расположен в директории */opt/UCC/bin/uccUninst* в терминале. Для этого необходимо выполнить в терминале команду:
   sudo /opt/UCC/ bin/uccUninst
2. После выполнения команды запустится окно мастера удаления ЕЦУ Dallas Lock (рис. 22).

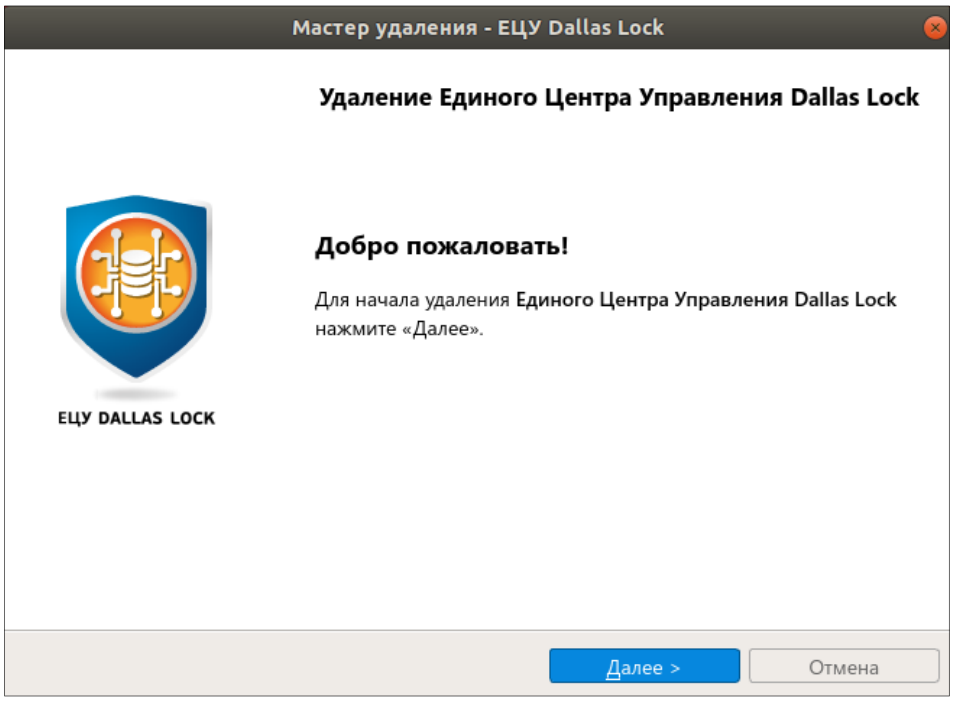

Рис. 22. Окно начала удаления ЕЦУ Dallas Lock

Далее порядок удаления ЕЦУ Dallas Lock аналогичен порядку удаления данной программы в ОС семейства Windows (см. «Порядок удаления ЕЦУ Dallas Lock в ОС семейства Windows»).

2.4 Сохранение и применение конфигурации

В ЕЦУ Dallas Lock существует возможность сохранить текущую конфигурацию сервера для применения на новом сервере после установки.

2.4.1 Сохранение конфигурации ЕЦУ

Для сохранения конфигурации ЕЦУ Dallas Lock в ОС семейства Windows или Linux необходимо открыть главное меню Консоли ЕЦУ и выбрать пункт → «Сохранить конфигурацию…».

Появится окно «Сохранение конфигурации» (рис. 23), где нужно задать путь к файлу конфигурации с помощью кнопки «…».

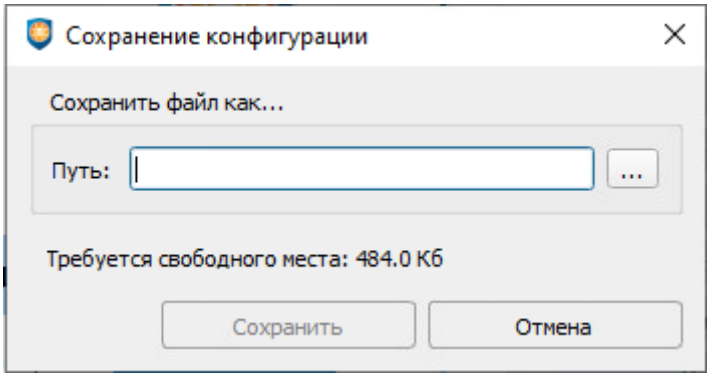

Рис. 23. Сохранение конфигурации

Примечание. Количество свободного места, которое необходимо для сохранения конфигурации указано в окне «Сохранение конфигурации» под полем «Путь к файлу конфигурации…» (рис. 23).

2.4.2 Применение конфигурации ЕЦУ

Внимание! Применение конфигурации приведет к удалению всех данных домена безопасности.

Для применения конфигурации ЕЦУ Dallas Lock в ОС семейства Windows или Linux необходимо открыть главное меню Консоли ЕЦУ и выбрать пункт → «Применить конфигурацию…».

Появится окно «Применение конфигурации» (рис. 24). Далее необходимо указать путь к файлу конфигурации, для этого нужно:

- нажать кнопку «Выбрать…»;
- найти и выбрать сохраненный ранее файл конфигурации ЕЦУ *(*.uconf)*;
- нажать кнопку «Применить».

В случае, если при сохранении конфигурации (см. «Сохранение конфигурации ЕЦУ») также были сохранены и журналы, можно установить их вместе с конфигурацией. Для этого в окне «Применение конфигурации» (рис.24), нужно установить флаг напротив пункта «Журналы».

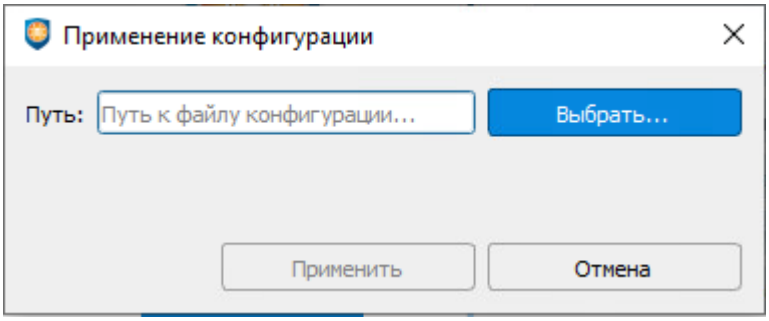

Рис. 24. Применение конфигурации

2.5 О программе

Информационное окно «О программе» (Рис. 25), вызывается пунктом главного меню в Консоли ЕЦУ и содержит следующие данные:

- полное наименование программы;
- номер сборки консоли;
- дата сборки консоли;
- номер сборки службы ЕЦУ;
- дата сборки службы ЕЦУ;
- контакты разработчика и технической поддержки.

Рис. 25 Окно «О программе»

3 ОБЩИЕ ПРИНЦИПЫ РАБОТЫ ЕЦУ DALLAS LOCK

3.1 Синхронизация

Синхронизация — это ключевое понятие в идеологии ЕЦУ Dallas Lock. Под синхронизацией понимается процесс сверки соответствия параметров с внутренней базой данных Домена безопасности ЕЦУ Dallas Lock и, при обнаружении несоответствия, модификации параметров подчиненного объекта.

Что бы ни происходило на подчиненном объекте, какие бы настройки параметров умышленные или злоумышленные не производились, при синхронизации все настраивается согласно записям Домена безопасности ЕЦУ Dallas Lock. Если параметры оставались без изменения (например, список пользователей), синхронизация этих параметров не происходит. Факты и результаты синхронизации фиксируются в журналах подчиненных объектов. Но если в процессе синхронизации на подчиненном объекте не было изменений, то запись в журнал не заносится.

Синхронизация модулей СДЗ происходит при каждом включении модуля СДЗ до момента авторизации пользователя.

Синхронизировать остальные модули с ЕЦУ Dallas Lock можно следующими способами:

1. Периодически из Консоли ЕЦУ. Необходимо настроить периодичность синхронизации с модулями.
2. По команде АИБ из Консоли ЕЦУ. Необходимо использовать кнопку «Синхронизировать», которая расположена на панели инструментов «Оперативное управление» вкладки «Сводка».
3. Из оболочки администрирования модуля.

3.2 Репликация

Под репликацией понимается процесс дублирования конфигурации (списка подчиненных объектов, значений политик, списка пользователей и групп, записей журналов и т.д.) серверов в кластере ЕЦУ Dallas Lock с целью повышения отказоустойчивости системы и повышения производительности за счет горизонтального масштабирования.

Распределение нагрузки реализуется за счет равномерного распределения модулей между серверами кластера (модуль подключается к серверу выбранному случайным образом).

Примечание. Серверы в кластере репликации практически по всем задачам распределяют нагрузку (это одна из задач, решаемых при построении кластера). В том числе это касается анализа состояния объектов в сети. Поэтому, если объект становится недоступным для какого-либо сервера, эта информация может быть синхронизирована с другими серверами в кластере. При обнаружении несоответствий фактической доступности объектов с диагностируемой следует убедиться, что в репликации нет сервера, который не может установить с объектом сетевое соединение.

В случае отказа одного из серверов в кластере работа подчиненных объектов не будет нарушена так как все настройки, сделанные для одного сервера, применяются на все серверы кластера, введенные в домен.

Реализовано динамическое применение изменений настроек на сторонние серверы.

Реализована функция дублирования журнала ЕЦУ Dallas Lock и собранных с модулей журналов на все серверы кластера. Синхронизация журналов между серверами кластера осуществляется в двух режимах:

1. Обмен информацией, по которой можно определить недостающие данные, и передача данных пакетами размером до 2 Мб (или одной записью, если она больше 2 Мб).
2. Обмен новыми данными, полученными от подчиненных объектов, между серверами.

При вводе нового сервера в существующий кластер (см. «Параметры кластера ДБ»), все серверы в кластере ЕЦУ, в том числе не участвующие в непосредственной регистрации нового сервера, автоматически оповещаются о новом «участнике».

4 АДМИНИСТРИРОВАНИЕ ЕЦУ DALLAS LOCK

4.1 Запуск консоли ЕЦУ

Запуск Консоли ЕЦУ осуществляется при условии, что компьютер, на котором расположена служба ЕЦУ, включен и доступен по сети.
Для запуска Консоли ЕЦУ необходимо запустить ярлык консоли, который появился после установки на рабочем столе ПК.

При первом запуске Консоли ЕЦУ необходимо выполнить регистрацию экземпляра Консоли в ЕЦУ. Для этого необходимо указать сетевое имя ПК, на котором установлена служба ЕЦУ и ключ доступа к Домену безопасности (рис. 26).

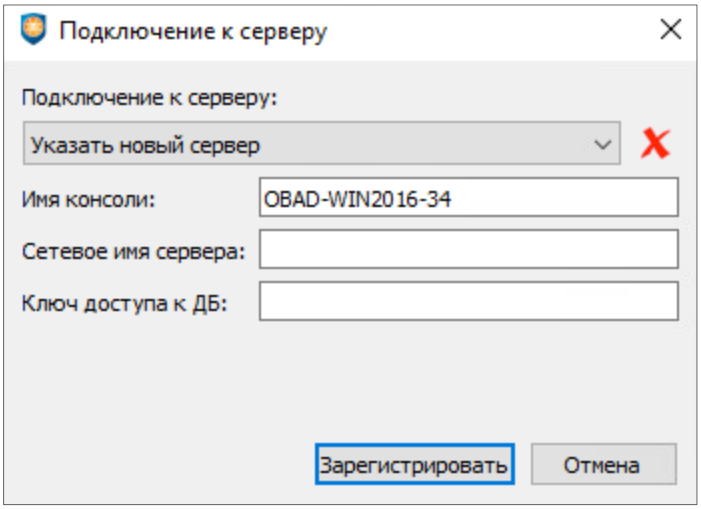

Рис. 26. Регистрация консоли ЕЦУ в Домене безопасности

В качестве имени консоли по умолчанию будет использоваться имя ПК, на котором она зарегистрирована.

Далее в окне подключения к серверу требуется заполнить поля (рис. 27):

- **Подключение к серверу.** Из списка выбрать доступный сервер, к которому необходимо выполнить подключение.
- **Имя пользователя.** Указать имя пользователя ДБ.
- **Пароль.** Ввести пароль учетной записи пользователя ДБ.
- **Аппаратный идентификатор.** Предъявить и выбрать из списка аппаратный идентификатор (если настроено использование средств аппаратной идентификации).

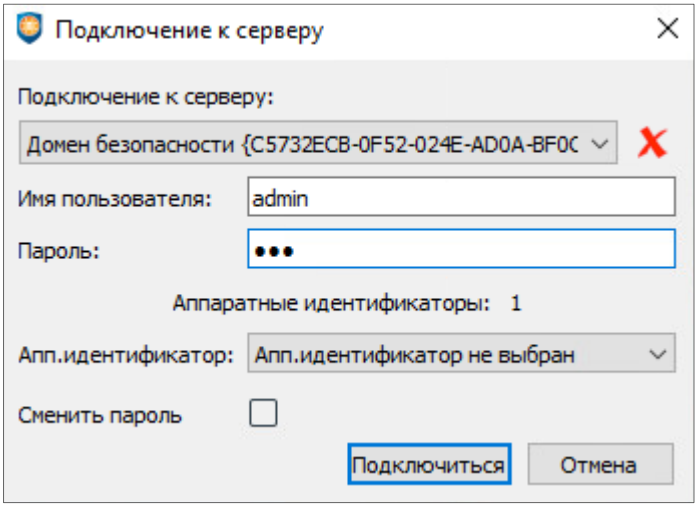

Рис. 27. Ввод пароля учетной записи для входа в Консоль ЕЦУ

При необходимости сменить пароль для указанной учетной записи, можно поставив флаг в поле «Сменить пароль» до нажатия кнопки «Продолжить» (рис. 27). Затем ввести новый пароль и подтверждение пароля (рис. 28).

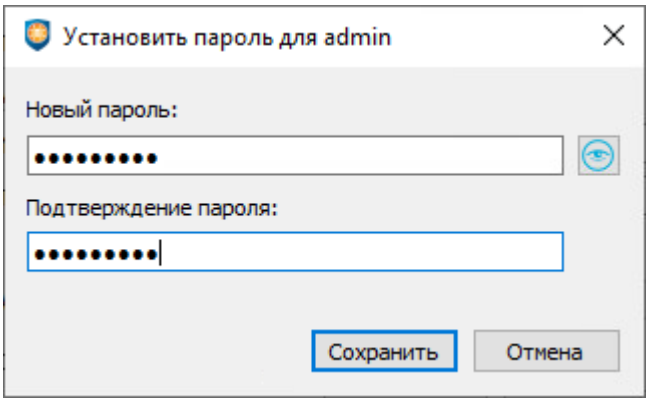

Рис. 28. Установка нового пароля пользователя

4.2 Описание консоли ЕЦУ

Главное окно Консоли ЕЦУ содержит следующие рабочие области (рис. 29):

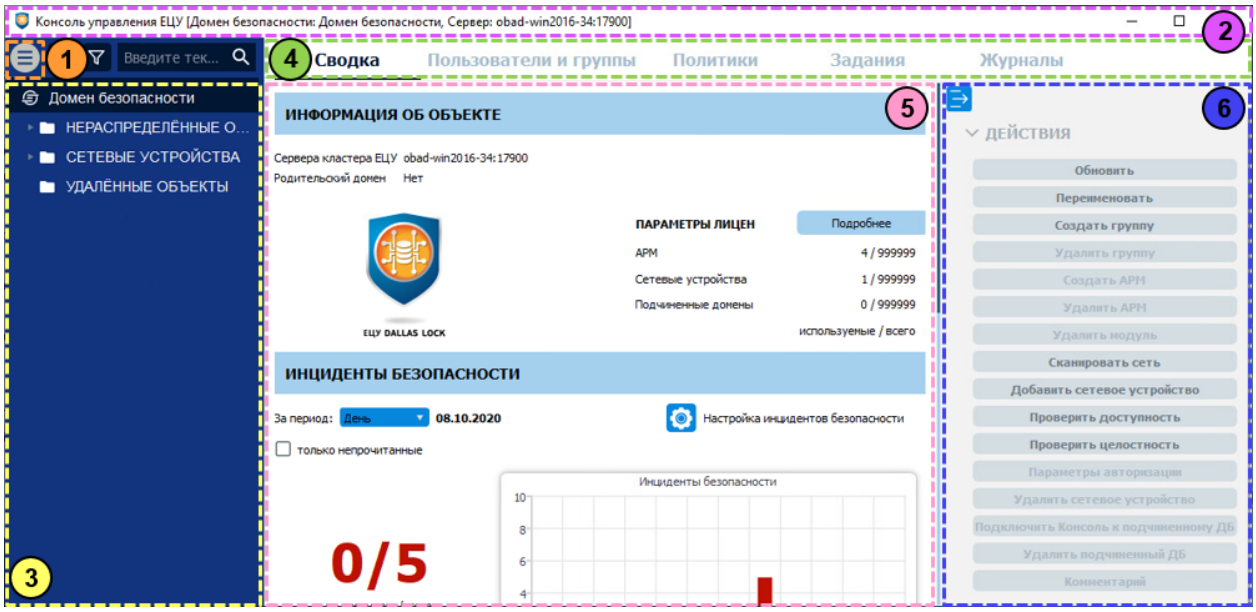

Рис. 29. Главное окно консоли ЕЦУ

1. Кнопка главного меню ЕЦУ Dallas Lock.
2. Заголовок окна (верхняя строка), содержащий имя программы, имя Домена безопасности и имя сервера.
3. Дерево Домена безопасности.
4. Вкладки для управления объектом дерева ЕЦУ Dallas Lock.
5. Содержание рабочей области вкладки управления объектом ЕЦУ Dallas Lock.
6. Панель инструментов.

Кнопка главного меню Консоли ЕЦУ содержит следующие пункты (рис. 30):

- «Ввод/Вывод в подчинение» (см. «Ввод ДБ в подчинение после установки» и «Вывод ДБ из подчинения из собственной консоли»);
- «Параметры кластера ДБ» (см. «Параметры кластера ДБ»);
- «Подключение к Kaspersky Security Center» (см. «Подключение к Kaspersky Security Center»);
- «Экспорт ИБ» (см. «Экспорт инцидентов безопасности»);
- «Настройка конфигурационных файлов» (см. «Настройка конфигурационных файлов»);

- «Установка ключа доступа» (см. «Ключ доступа к ДБ»);
- «Принадлежность к домену Active Directory» (см. «Принадлежность к домену Active Directory»);
- «Параметры…» (см. «Параметры работы»);
- «Утилиты»:
  - см. «Удаленное развертывание СЗИ Dallas Lock 8.0»;
  - см. «Подготовка msi-дистрибутива DL8.0 для AD»;
  - см. «Удаленное развертывание СЗИ НСД Dallas Lock Linux» ;
  - см. «Удаленная установка Агента ЕЦУ Windows»;
  - см. «Удаленная установка Агента ЕЦУ Linux»;
- «Сохранить конфигурацию…» (см. Сохранение конфигурации ЕЦУ);
- «Применить конфигурацию…» (см. Применение конфигурации ЕЦУ);
- «О программе» (см. «О программе»);
- «Выход».

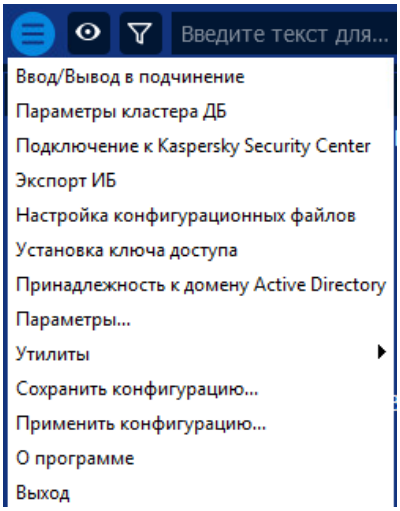

Рис. 30. Пункты главного меню

С помощью Консоли ЕЦУ можно настроить параметры для следующих объектов ДБ:

- для всего Домена безопасности, определив настройки при выборе объекта, обозначающего текущий Домен безопасности в дереве;
- для группы, определив настройки при выборе объекта, обозначающего группу в дереве;
- для АРМ, определив настройки при выборе объекта, обозначающего АРМ в дереве;
- для отдельного модуля, выбрав его в дереве;
- для сетевого устройства, выбрав его в дереве;
- для подчиненного ДБ, определив настройки при выборе объекта, обозначающего группу в дереве.

Для объектов дерева ДБ, можно настроить сортировку и фильтрацию:

— Сортировка. При нажатии на кнопку появляется меню с возможными вариантами сортировки:

- группы по умолчанию вверху;
- сортировка в алфавитном порядке;
- сортировка в обратном алфавитном порядке;
- сортировка по возрастанию инцидентов безопасности;
- сортировка по убыванию инцидентов безопасности.

— Фильтрация. При нажатии на кнопку можно выбрать один из вариантов фильтрации:

- фильтрация по типу АРМ;
- фильтрация по модулям;
- фильтрация по сетевым устройствам;
- фильтрация по поддоменам;
- фильтрация по включенным объектам;

- фильтрация по выключенным объектам;
- фильтрация объектов, давно не выходивших на связь;
- фильтрация объектов с непрочитанными инцидентами безопасности.

Для сброса всех фильтров, нужно нажать «Сбросить фильтры».

Для поиска конкретного объекта в дереве ДБ, можно воспользоваться поисковой строкой, расположенной правее кнопки фильтрации.

Для каждого из объектов в верхней части дополнительного меню консоли формируется список вкладок для управления объектом дерева. Список вкладок меняется в зависимости от типа выбранного объекта. При выборе вкладки в рабочей области открывается страница с соответствующими параметрами и меню.

Значки объектов, обозначающие группы, в зависимости от состояния могут принимать следующий вид:

— список вложенных объектов группы скрыт;

— список вложенных объектов группы отображается в дереве.

Контекстное меню объектов дерева консоли позволяет добавлять/удалять/переименовывать группы, создавать АРМ в группе, перемещать объекты из группы в группу и другие операции.

В ЕЦУ Dallas Lock предусмотрены 3 базовые группы, предназначенные для обеспечения состояния защищенности объектов Домена безопасности:

- нераспределенные объекты;
- сетевые устройства;
- удаленные объекты.

Удаление и переименование базовых групп недоступно.

Значки объектов, обозначающих модули, зависят от типа и состояния модуля.
Так как АРМ представляет собой совокупность модулей, состояние АРМ зависит от состояния модулей. Эта связь описывается следующим образом:

— если хотя бы один из модулей в составе АРМ находится в состоянии «Подключен», состояние АРМ — «включен»;

— если все модули в составе АРМ не подключены, состояние АРМ — «выключен»;

— если ни один из модулей в составе АРМ не выходил на связь с ЕЦУ свыше установленного параметром «Оповещения при отсутствии связи с объектом (в днях)» времени (при условии, что настроено письмо об отсутствии связи с объектом), состояние АРМ — «долго не выходил на связь».

В целях оптимизации производительности ЕЦУ проверяет АРМы на долгое отсутствие связи не чаще, чем раз в час. Если в рамках данной проверки связь отсутствует, то в Консоли управления ЕЦУ появится инцидент безопасности с результатом «Продолжительное отсутствие связи».

В дереве напротив объекта, на котором произошли инциденты безопасности индицируется их количество (рис. 31).

Рис. 31. Индикация инцидентов безопасности в дереве

При этом для уровня выше по иерархии ДБ суммируется количество инцидентов на всех вложенных объектах. Например, на уровне АРМ отображается сумма количества инцидентов на модулях, входящих в его состав.

4.3 Ключ доступа к ДБ

Консоль позволяет установить ключ доступа к ДБ, который нужен для ввода модулей и подчиненных доменов в текущий ДБ. По умолчанию ключ доступа — пустой.

Для изменения ключа доступа к ДБ необходимо открыть главное меню Консоли ЕЦУ → «Установка ключа доступа».
Появится окно «Смена ключа доступа к ДБ», где необходимо заполнить требуемые поля (рис. 32).

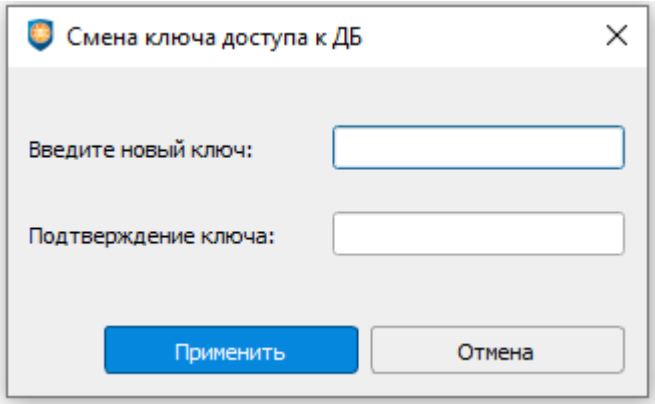

Рис. 32. Ключ доступа к ДБ

Примечание. Политики сложности паролей в ЕЦУ Dallas Lock распространяются на установку значений ключа доступа к ДБ. Чтобы была возможность задать пустое значение доступа к ДБ, необходимо, чтобы в Консоли ЕЦУ политика «Минимальная длина пароля» из категории «Политики паролей» имела значение «Не используется».

Примечание. Действие политики сложности пароля «Необходимо изменение пароля не меньше чем в» не распространяется на ключ доступа к ДБ.

4.4 Настройки лицензирования

Лицензия на ЕЦУ Dallas Lock устанавливает количественные ограничения по следующим подчиненным объектам:

- защищаемые АРМ;
- сетевые устройства;
- подчиненные домены.

Управление лицензией на ЕЦУ Dallas Lock осуществляет пользователь с ролью «Администратор», назначенной на уровне ДБ (см. «Ролевая модель учетных записей ДБ»).

Информация о параметрах текущей лицензии доступна на уровне Домена безопасности на вкладке «Сводка» → «Информация об объекте» (рис. 33).

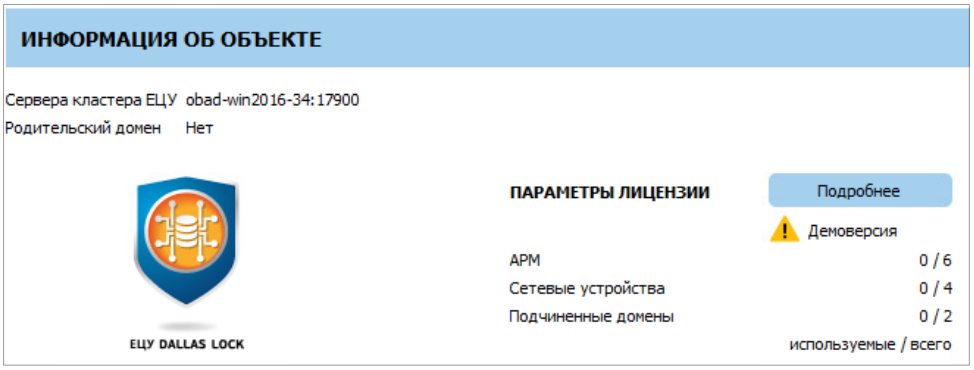

Рис. 33. Информация о параметрах лицензии

При нажатии кнопки «Подробнее» появляется окно «Состояние лицензии» (рис. 34), которое содержит информации о состоянии лицензии для данного сервера, а также для каждого сервера в кластере ДБ.

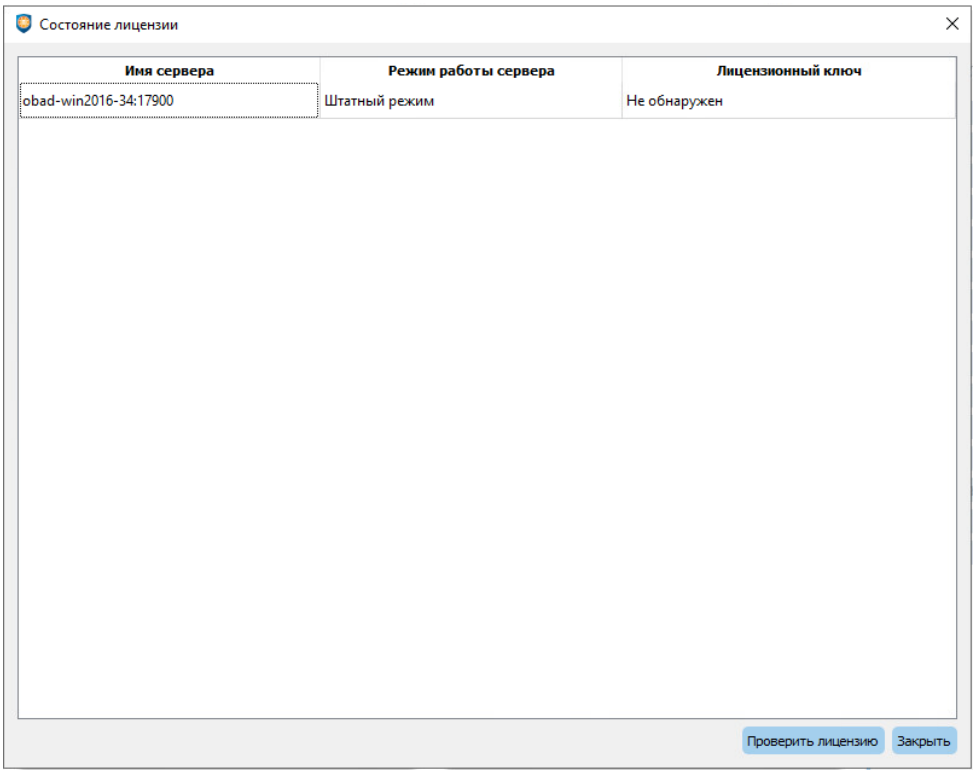

Рис. 34. Окно «Состояние лицензии»

Для добавления\обновления лицензии на сервер ЕЦУ Dallas Lock необходимо предъявить аппаратный ключ и нажать кнопку «Проверить лицензию», либо перезагрузить сервер. В случае успешного применения, в столбце «Лицензионный ключ» появится соответствующая надпись с установленными количественными ограничениями по подчиненным объектам. Также на вкладке «Сводка» изменится информация о параметрах текущей лицензии (рис. 35).

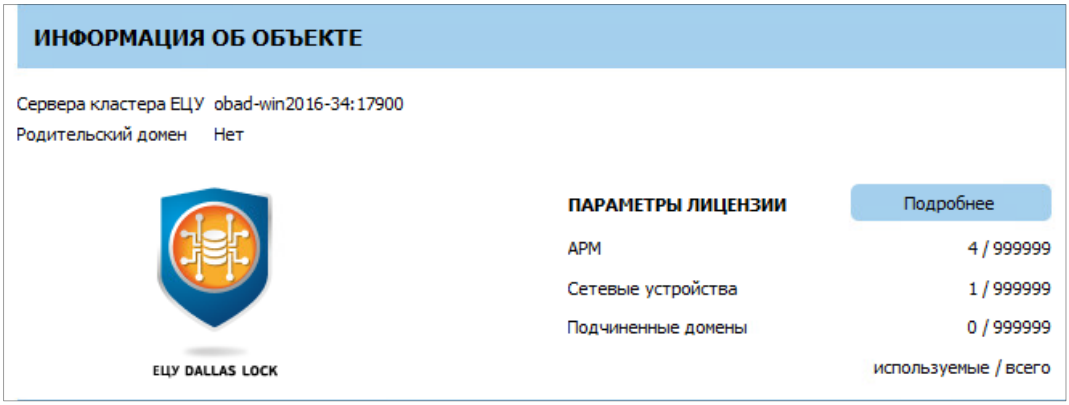

Рис. 35. Информация о параметрах лицензии

Если предъявлено более одного аппаратного идентификатора, то применяется аппаратный ключ с максимальными ограничениями. Так как лицензионные ключи хранятся на АИ и не сохраняются на сервер ЕЦУ, то удалять неактуальные лицензии не нужно.

Процедура проверки параметров лицензии дополнительно осуществляется при каждом старте службы ЕЦУ.

4.4.1 Особенности лицензирования кластера ДБ

При организации работы Домена безопасности в режиме кластера (см. раздел «Параметры кластера ДБ») следует обратить внимание на особенности распределения лицензионных ограничений: в кластере применяются максимальные ограничения из предъявленных на аппаратных ключах. Эти ограничения распределяются между серверами в составе кластера (путем назначения «квот» для домена). Все сервера в составе одного кластера ДБ имеют равные квоты.

Например, имеется конфигурация из *M* реплицированных серверов. Количественные ограничения в аппаратных ключах кластера обозначены следующим образом:

- *N* — количество защищаемых АРМ;
- *K* — количество сетевых устройств;
- *L* — количество подчиненных доменов безопасности.

В данном случае квота кластера рассчитывается следующим образом:

- MAX(*N*)/*M* = квота на защищаемые АРМ;
- MAX(*K*)/*M* = квота на сетевые устройства;
- MAX(*L*)/*M* = квота на подчиненные ДБ.

Соответственно, чем больше реплицированных серверов, тем быстрее расходуются квоты для ДБ.

Примечание. Если в результате деления получается дробное число, которое:

- >1, то округление осуществляется в меньшую сторону;
- <1, то округление производится до единицы.

При каждом запуске службы ЕЦУ осуществляется проверка назначенных квот для домена.

Например, имеется следующая конфигурация:

- *X* — количество реплицированных серверов;
- *Y* — количественные ограничения по подчиненным объектам в аппаратном ключе, примененном в запускаемом сервере;
- MAX(*Z*)/*X* — количественные ограничения по подчиненным объектам, действующие в кластере ЕЦУ.

1. Если по итогам проверки параметров лицензии обнаружен корректно работающий ключ, при этом (MAX(*Z*)/*X* ≥ *Y*/*X*) — служба ЕЦУ запускается в штатном режиме с назначенными в домене квотами.
2. Если по итогам проверки параметров лицензии обнаружен корректно работающий ключ, при этом (MAX(*Z*)/*X* < *Y*/*X*) — происходит перераспределение квот между серверами кластера, служба ЕЦУ запускается в штатном режиме на данном сервере.
3. Если по итогам проверки сервером ЕЦУ не обнаружен ключ или ключ работает некорректно — текущий сервер в ДБ переводится в режим ограниченной функциональности до предъявления корректно работающего аппаратного ключа. Режим ограниченной функциональности («ограниченный режим») — это режим работы сервера ЕЦУ, при котором:
   - аудит, управление и синхронизация с модулями, сетевыми устройствами и подчиненными (дочерними) доменами не осуществляется;
   - аудит и администрирование ДБ кластера из консоли ЕЦУ не осуществляется;
   - репликация и обмен данными между серверами в рамках кластера продолжает функционировать.

   На уровне ДБ на вкладке «Сводка» выводится предупреждение об ошибке с лицензией на сервере.

Инициация новой проверки лицензии осуществляется повторной попыткой запуска службы ЕЦУ.

4.5 Параметры ЕЦУ

4.5.1 Настройка инцидентов безопасности

Примечание. Настройка инцидентов безопасности доступна на разных уровнях дерева Домена безопасности. При изменении настройки отображения на любом уровне ДБ, изменения распространятся на отображение всех уровней ДБ.

В ЕЦУ Dallas Lock предусмотрена возможность пользовательской настройки визуализации диаграмм инцидентов безопасности и управления оповещениями в зависимости от приоритета и типа события, а также реализована возможность экспорта инцидентов безопасности в файл по кнопке «Экспорт» (рис. 36).
Для настройки и управления оповещениями, необходимо нажать на соответствующую кнопку на вкладке «Сводка» → «Настройка инцидентов безопасности» (рис. 36).

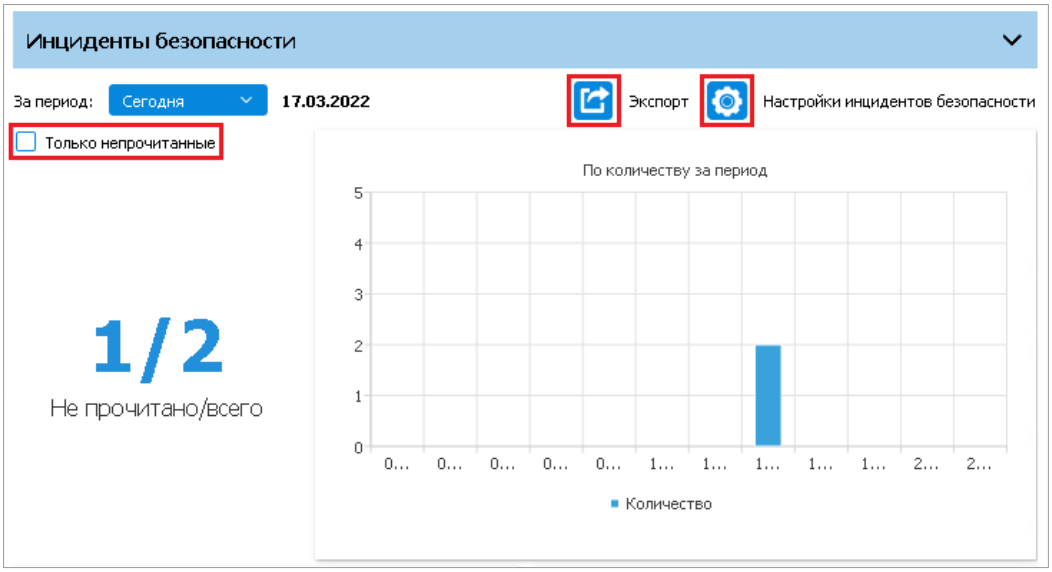

Рис. 36. Настройка инцидентов безопасности

При нажатии кнопки, появляется окно «Настройки инцидентов безопасности» (рис. 37).

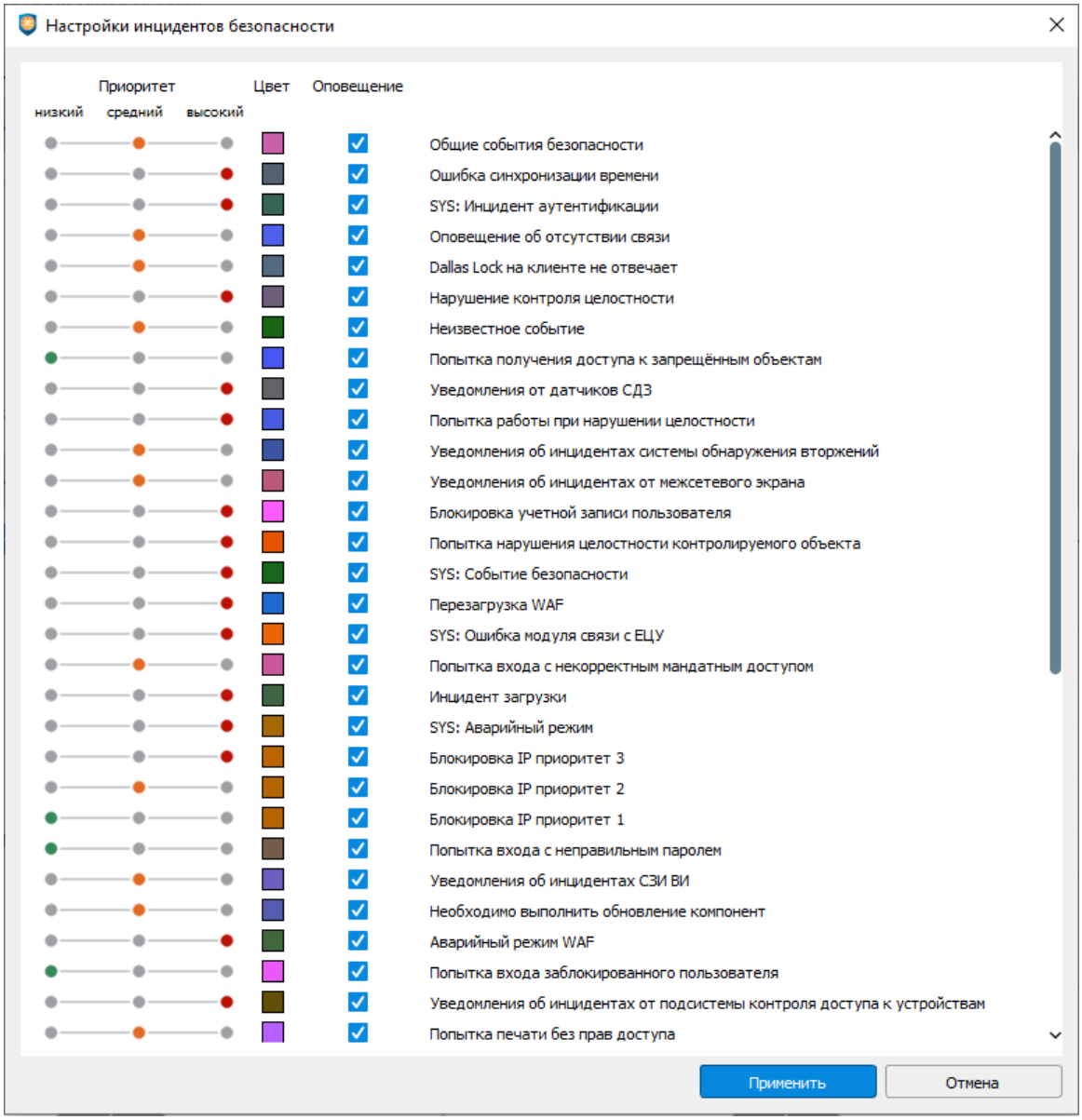

Рис. 37. Окно «Настройки инцидентов безопасности»

В окне расположена таблица, состоящая из четырех столбцов. *В правом столбце* приведен *список доступных инцидентов безопасности*, для которых осуществляется настройка.
В левом столбце производится *настройка приоритетов* правил контроля приложений. Для каждого инцидента безопасности можно изменить приоритет выбором одного из значений. Доступны приоритеты событий: «Низкий», «Средний» и «Высокий».
Настройки приоритетов влияют на внешний вид диаграммы «По приоритету» (вкладка «Сводка» → «Инциденты безопасности»).

В столбце «Цвет» производится *настройка цвета сегментов диаграммы* «По типу» (отображается на вкладке «Сводка» → «Инциденты безопасности»). Для смены цвета инцидента безопасности нужно нажать левой кнопкой мыши по навигатору цвета и выбрать цвет из палитры (рис. 38).

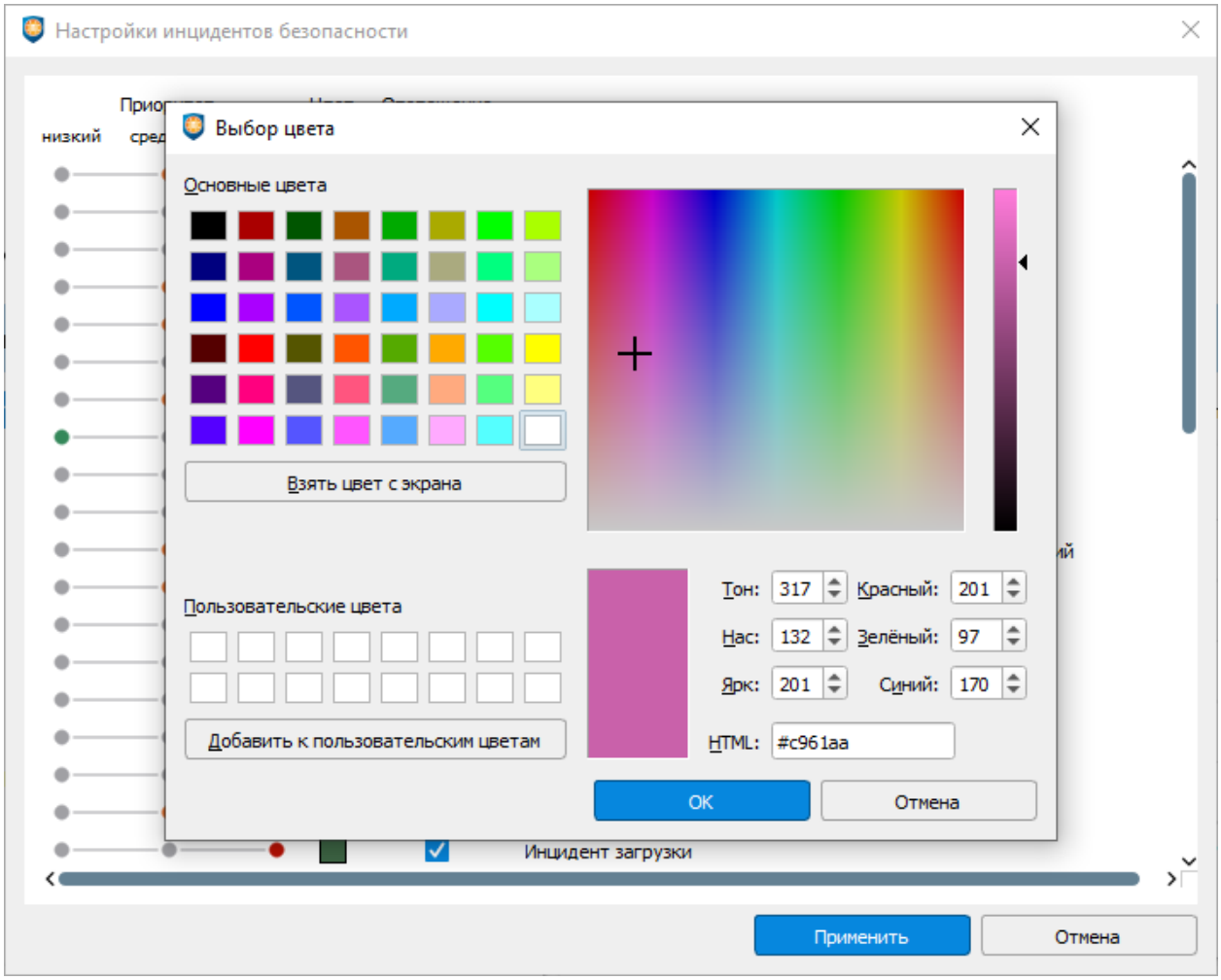

Рис. 38. Выбор цвета инцидента безопасности

Инциденты безопасности на модулях отслеживаются и сопровождаются сигнализацией на ЕЦУ Dallas Lock. На ПК с запущенной Консолью ЕЦУ воспроизводится звуковой сигнал о событии безопасности и выводится всплывающее сообщение в области уведомлений (рис. 39).

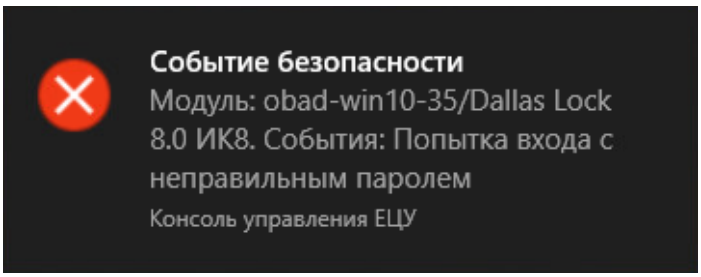

Рис. 39. Уведомление о событии безопасности на модуле

Для включения сообщения, в строке, относящейся к данному типу событий, нужно поставить флаг в столбце *«Оповещение»* (окно «Настройки инцидентов безопасности»). *Для отключения* сообщения необходимо *убрать флаг.*

4.5.2 Параметры кластера ДБ

Перед тем, как создавать кластер серверов ДБ, АИБ необходимо произвести подготовительные действия:

1. Убедиться, что на всех будущих серверах кластера правильно настроено подключение к DNS-серверу.

2. Корректно настроить DNS-сервер — на каждом будущем сервере кластера должно возвращаться корректное полностью определенное имя домена (FQDN) каждого сервера, по которому потом будут вводиться и работать модули DL.
3. Рекомендуется произвести синхронизацию времени серверов кластера (вручную или при использовании серверов NTP).
4. Настроить базу данных PostgreSQL на внешние подключения, а также настроить связь между БД и всеми АРМ, которые будут входить в кластер. Для этого необходимо:
   - добавить в файл *pg_hba.conf* (который находится в одном из каталогов, куда установлена база данных) следующую строку:

     «*# IPv4 local connections:*
     host all all 0.0.0.0/0 password»

     Это позволит разрешить подключение к PostgreSQL с любого адреса, для подключения с IPv4 адресов к любой БД, любым пользователем (или настроить ограниченный доступ только с серверов ЕЦУ Dallas Lock);
   - раскомментировать в файле *postgresql.conf* следующую строку:

     «*listen_addresses = '*'*»

     Это позволит PostgreSQL отвечать на любом интерфейсе сервера (или настроить работу на определенном сетевом интерфейсе, доступном по сети с сервера ЕЦУ Dallas Lock);
   - создать отдельную базу данных и учетную запись в PostgreSQL для ЕЦУ Dallas Lock, выполнив команды:
     «*postgres=# create database <база_данных>*»;
     «*postgres=# create role <admin_базы_данных> with login*»;
     «*postgres=# \password <admin_базы_данных>*»;
     «*postgres=# grant connect, create on database <база_данных> to <admin_базы_данных>*».

Примечание. Данные действия можно сделать, установив графическую утилиту **pgAdmin**, предназначенную для более удобного администрирования PostgreSQL, чем командная строка.

После создания кластера серверов ДБ АИБ должен убедиться, что в Консоли ЕЦУ отображаются корректные имена серверов кластера. Если же в Консоли ЕЦУ отображаются некорректные FQDN имена серверов, то необходимо:

1. Вывести проблемный сервер из кластера ДБ.
2. Корректно настроить DNS и проверить настройки серверов кластера.
3. Повторно ввести сервер в кластер ДБ.

Внимание! Создание кластера серверов ДБ возможно только при использовании базы данных PostgreSQL.

Примечание. Возможна установка внешней базы PostgreSQL на один из серверов ЕЦУ, но при этом будет нарушено свойство отказоустойчивости кластера.

Примечание. После разворачивания кластера серверов ЕЦУ Dallas Lock не допускаются изменения настроек сетевых адаптеров, сетевого имени сервера, FQDN имени в записи DNS-сервера и добавление DNS-записей, связанных с серверами ЕЦУ Dallas Lock, т.к. это может повлечь неработоспособность кластера.

Примечание. Если в кластере ЕЦУ Dallas Lock некорректно настроено распознавание FQDN имен серверов ЕЦУ Dallas Lock — перенос и сохранение конфигурации ЕЦУ Dallas Lock может не работать.

Для ввода сервера в состав кластера достаточно, чтобы АИ с лицензией был подключен:

- к одному из серверов, входящих в состав кластера;
  или
- к тому серверу, который вводится в состав кластера.

Ввод в кластер ДБ в процессе установки

Примечание. Если на удаленном сервере ЕЦУ, к которому производится подключение, установлена демоверсия продукта, то добавление узла в кластер серверов ЕЦУ Dallas Lock будет недоступно.

Для добавления узла в кластер серверов ДБ в процессе установки необходимо:

1. Запустить процесс установки ЕЦУ Dallas Lock.
2. На шаге «Выбор типа домена» выбрать пункт «Сервер репликации» (Рис. 40).

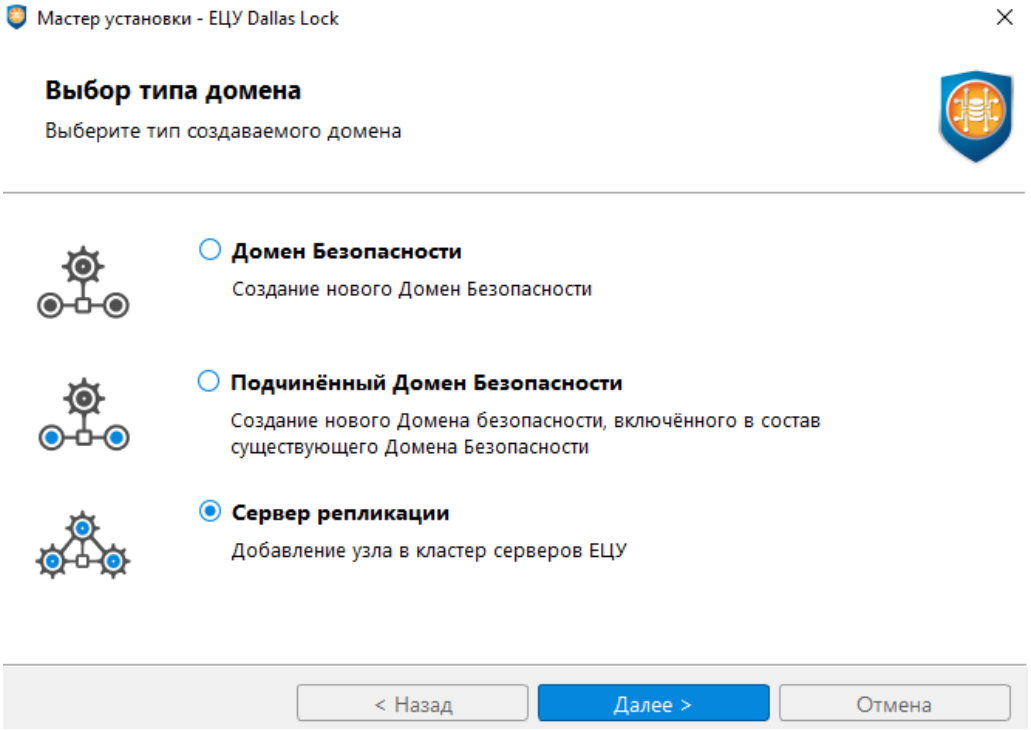

Рис. 40. Выбор типа создаваемого домена

3. Задать параметры главного ДБ (рис. 41):
   - адрес главного ДБ;
   - ключ доступа к ДБ.

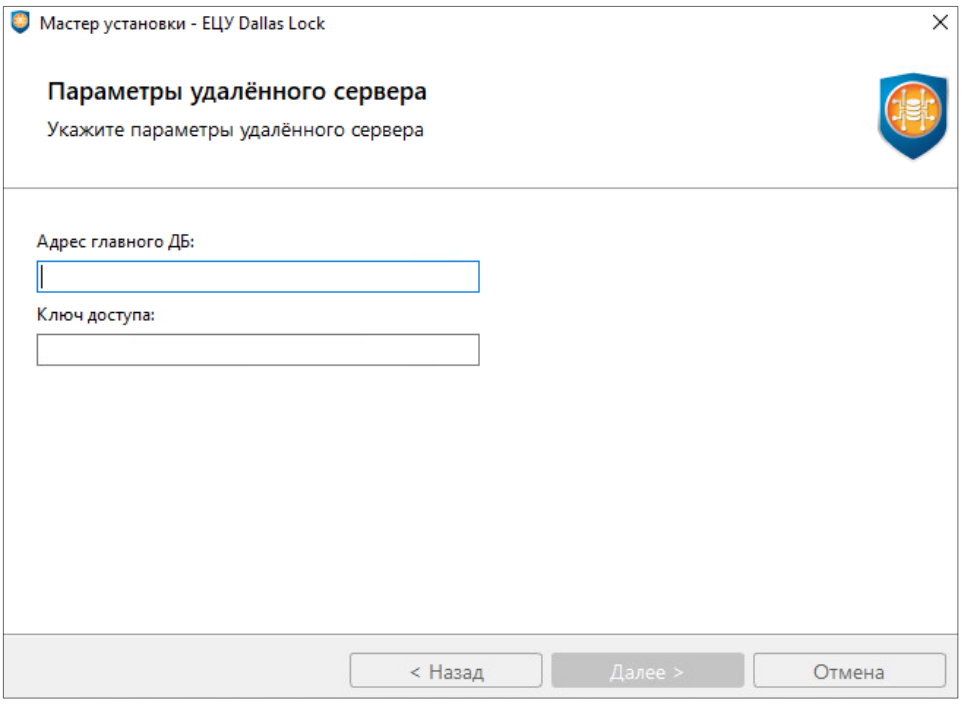

Рис. 41. Параметры удаленного сервера

4. Далее продолжить установку ЕЦУ Dallas Lock.
5. После завершения установки на серверах кластера ЕЦУ Dallas Lock на вкладке «Сводка» → «Информация об объекте» появится имя добавленного узла.

Ввод в кластер ДБ после установки

Внимание! При вводе в кластер ДБ текущего сервера ЕЦУ Dallas Lock будут потеряны ранее добавленные в него модули и настройки, и назначены настройки сервера или кластера серверов ЕЦУ, в ДБ которых происходит ввод.

Для изменения настроек кластера ДБ после установки необходимо открыть главное меню Консоли ЕЦУ → «Параметры кластера ДБ».

В окне «Параметры кластера ДБ», ввести текущий сервер ЕЦУ Dallas Lock в кластер ДБ для репликации (рис. 42).

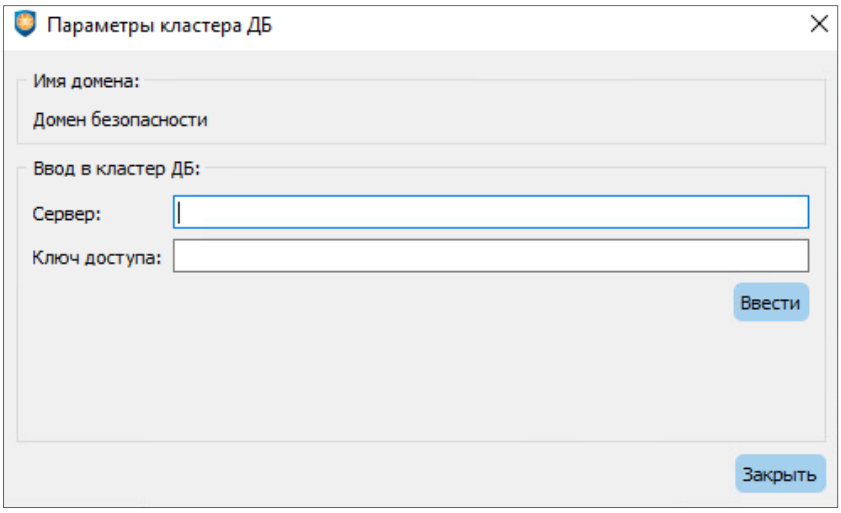

Рис. 42. Параметры кластера ДБ

После заполнения данных главного сервера ДБ нажать кнопку «Ввести». Далее появится информационное сообщение об успешной регистрации сервера (рис. 43).

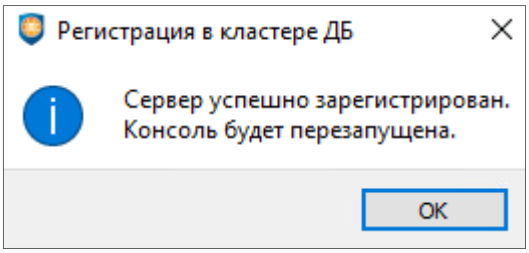

Рис. 43. Сообщение о регистрации в кластере ДБ

Консоль ЕЦУ будет перезапущена. Затем необходимо зарегистрировать экземпляр Консоли ЕЦУ как при первом запуске (см. «Запуск консоли ЕЦУ») и подключиться к серверу.

На уровне ДБ (вкладка «Сводка» → «Информация об объекте») отобразятся имена всех серверов кластера ЕЦУ Dallas Lock, а также будут рассчитаны количественные ограничения лицензии, согласно особенностям назначения квот для домена (см. «Особенности лицензирования кластера ДБ») (рис. 44).

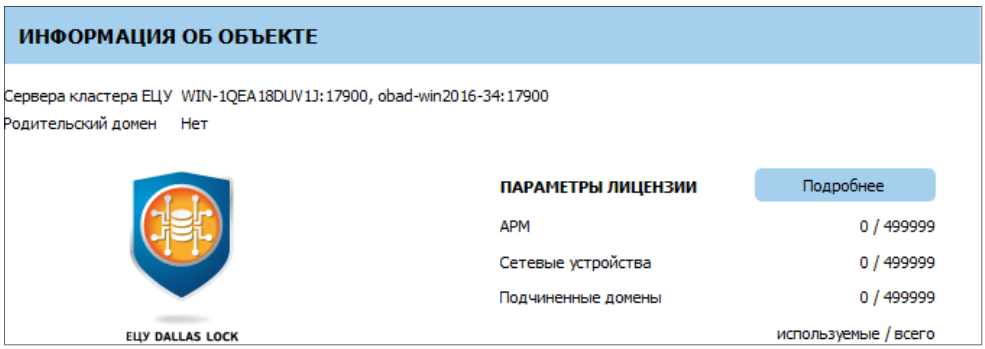

Рис. 44. Информация о кластере серверов

Вывод сервера из кластера ДБ

Для вывода сервера из кластера ДБ необходимо открыть главное меню Консоли ЕЦУ → «Параметры кластера ДБ».

Появится окно «Параметры кластера ДБ», из списка серверов кластера выбрать сервер для вывода и нажать «Вывести» (рис. 45). Появится сообщение об успешном выводе сервера из кластера ЕЦУ Dallas Lock и далее Консоль ЕЦУ перезапустится.

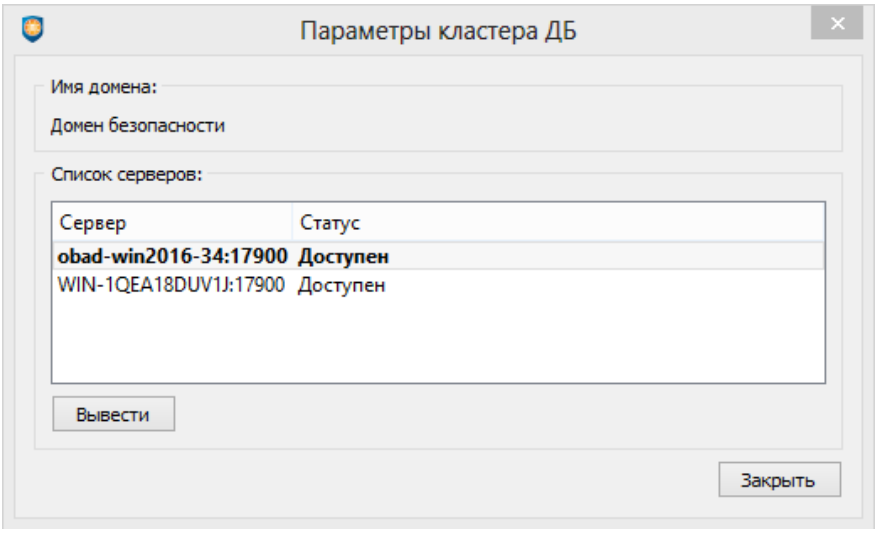

Рис. 45. Список серверов кластера ДБ

При штатном выводе сервера ЕЦУ из кластера осуществляется:

- оповещение серверов ЕЦУ в составе кластера о выводе сервера;
- перераспределение квот между серверами в кластере в соответствии с особенностями назначения квот для домена (см. «Особенности лицензирования кластера ДБ»);
- переход системы хранения журналов выводимого сервера в локальный режим;
- сброс логина и пароля учетной записи admin, а также кода доступа к серверу;
- исчезновение всех объектов из дерева объектов.

Если после вывода сервера из кластера ДБ в результате распределения квот оставшиеся серверы получают квоту на ДБ на меньшее число подчиненных объектов, чем уже зарегистрировано в ДБ, такая квота не применяется. Кластер ДБ функционирует в ограниченном режиме до момента применения лицензии, обеспечивающей достаточную величину квоты для данного ДБ.

4.5.3 Экспорт инцидентов безопасности

Для экспортирования инцидентов безопасности в SIEM-систему необходимо открыть главное меню Консоли ЕЦУ → «Экспорт ИБ».
Появится окно «Экспорт ИБ» (рис. 46).

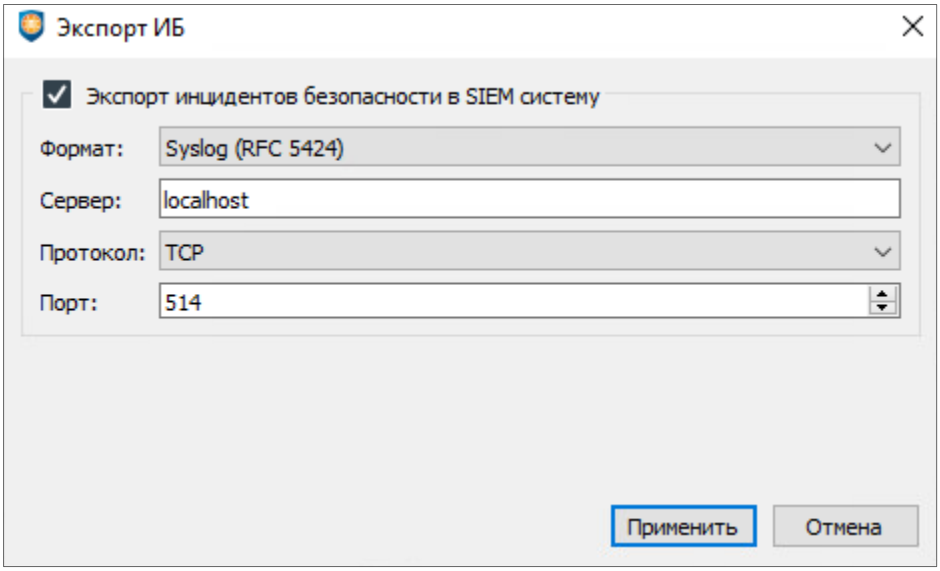

Рис. 46. Экспорт инцидентов безопасности в SIEM

В окне необходимо:

1. Поставить флаг «Экспорт инцидентов безопасности в SIEM-систему».
2. Выбрать формат экспорта.
3. Указать сетевое имя сервера.
4. Выбрать протокол и порт подключения.
5. Нажать кнопку «Применить».

Если процесс прошел успешно, через некоторое время инциденты безопасности будут экспортированы в выбранном формате на SIEM-сервер.

4.5.4 Настройка конфигурационных файлов

В ЕЦУ Dallas Lock существует возможность выбора необходимых типов объектов для работы в данном экземпляре консоли. Для настройки необходимо открыть главное меню Консоли ЕЦУ → «Настройка конфигурационных файлов».
Появится окно «Настройка конфигурационных файлов» (рис. 47).

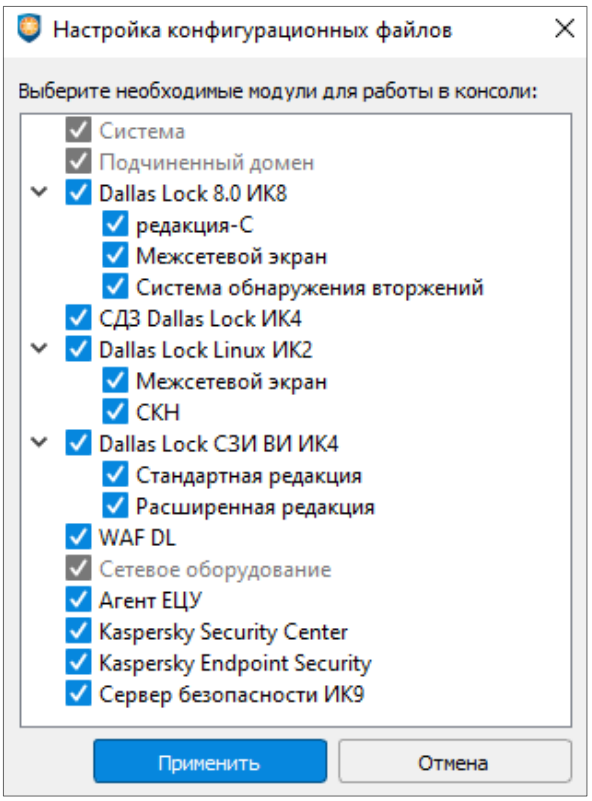

Рис. 47. Настройка конфигурационных файлов

В окне необходимо проставить флаги рядом с объектами, с которыми предполагается работа в данном экземпляре консоли.

4.5.5 Принадлежность к домену Active Directory

Для обеспечения возможности регистрации в Домене безопасности ЕЦУ Dallas Lock учетных записей домена Active Directory должны выполняться следующие условия:

1. ПК с ОС Windows, на котором установлена служба ЕЦУ, должен быть введен домен AD или являться контроллером домена AD.
2. На ПК с ОС Linux, на котором установлена служба ЕЦУ, необходимо указать полностью определенное имя домена.

Для просмотра информации о том, к какому домену AD принадлежит ЕЦУ Dallas Lock, необходимо открыть главное меню Консоли ЕЦУ → «Принадлежность к домену Active Directory».
Появится окно «Принадлежность к домену Active Directory» (рис. 48).

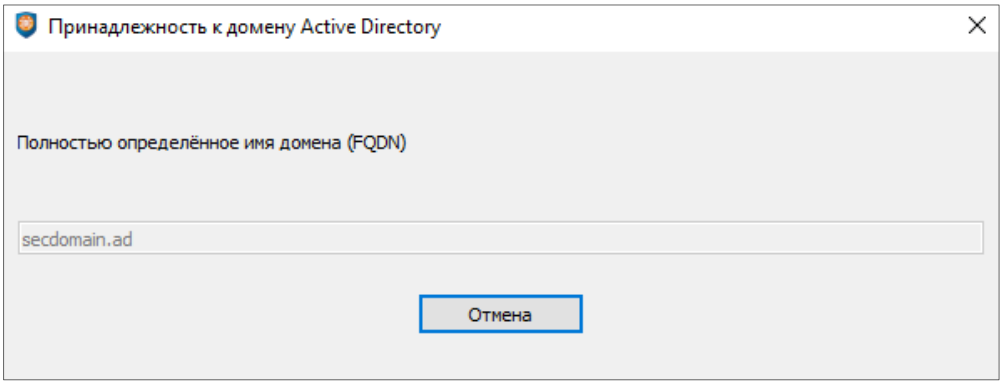

Рис. 48. Принадлежность к домену Active Directory

В окне будет указано полностью определенное имя домена AD (FQDN). Если служба ЕЦУ развернута на ПК с ОС Linux, поле с именем домена можно отредактировать.

4.5.6 Параметры работы

Параметры работы ЕЦУ Dallas Lock настраиваются в главном меню Консоли ЕЦУ → «Параметры…» (рис. 49).

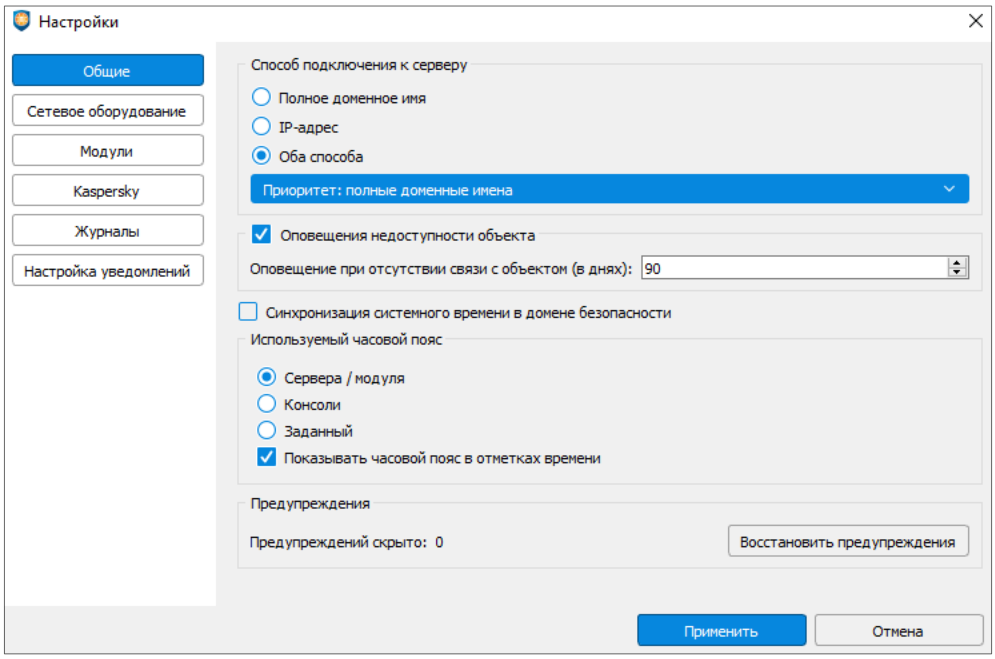

Рис. 49. Общие параметры

Общие параметры работы

На вкладке «Общие» настраиваются параметры, общие для всех объектов ДБ.

В данном окне доступен выбор используемого способа подключения к серверу ЕЦУ Dallas Lock:

- полное доменное имя;
- IP-адрес;
- оба способа с приоритетом подключения по:
  - полным доменным именам;
  - IP-адресам.

В окне производится настройка параметра «Оповещение недоступности объекта» с возможностью отключения/включения данного параметра и установки значения срока в днях, по истечению которого поступает оповещение об отсутствии связи с объектом.

Установка флага для параметра «Синхронизация системного времени в домене безопасности» включает синхронизацию системного времени на всех модулях, входящих в состав ДБ ЕЦУ Dallas Lock.

Параметр «Используемый часовой пояс» позволяет выбрать источник часового пояса с помощью радиокнопки со значениями: «Сервера/модуля», «Консоли» и «Заданный». Также параметр «Используемый часовой пояс» позволяет задать вид отображения времени в журналах Консоли ЕЦУ.

Также есть возможность восстановить скрытые предупреждения, нажав на кнопку «Восстановить предупреждения».

Параметры сетевого оборудования

На вкладке «Сетевое оборудование» задается периодичность проверок сетевого оборудования по протоколу SNMP и SSH (рис. 50).

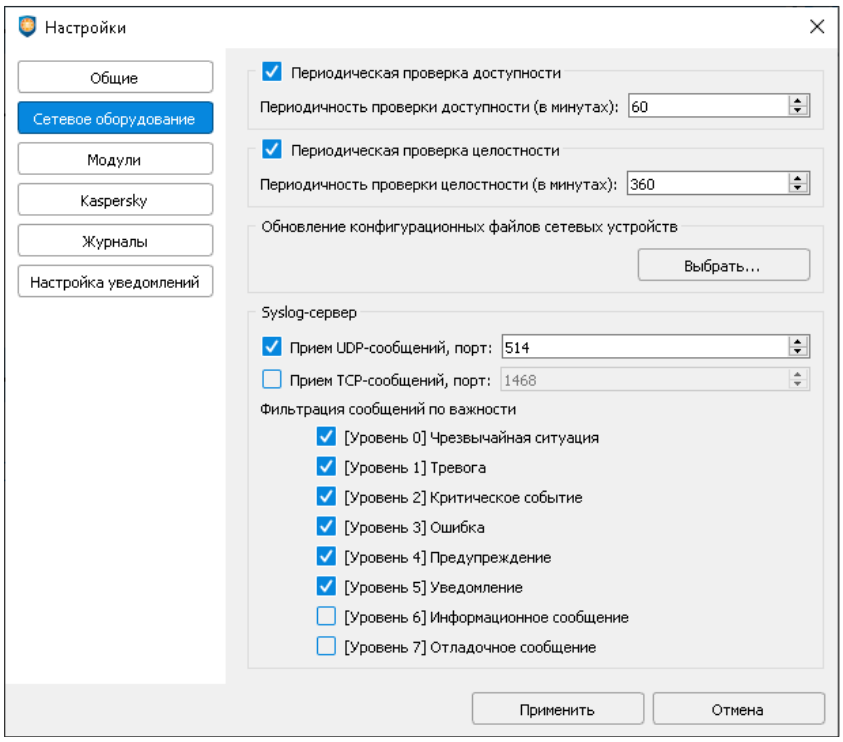

Рис. 50. Параметры SNMP и SSH

Доступны следующие параметры:

- периодичность проверки доступности (в минутах). Данный параметр принимает значения от 10 минут до 31 дня (44 640 минут), значение по умолчанию: 60 минут;
- периодичность проверки целостности (в минутах). Данный параметр принимает значения от 10 минут до 31 дня (44 640 минут), значение по умолчанию: 360 минут.

Пополнить Базу конфигураций ЕЦУ Dallas Lock, т.е добавить не указанные в ЕЦУ Dallas Lock соответствия идентификаторов сетевых устройств *(sysObjectID OID)* и их моделей можно следующими способами:

1)Отредактировать вручную файл *extra-ids.ucNetworkCfg*, который располагается:

- в ОС Windows: *C:\Program Files\UCC\share\snmp\extra-ids.ucNetworkCfg;*
- в ОС Linux: */opt/UCC/share/snmp/extra-ids.ucNetworkCfg.*

2)По запросу в службе технической поддержки (helpdesk@confident.ru) можно получить обновления Базы конфигураций ЕЦУ Dallas Lock. Для применения полученных обновлений, необходимо указать к ним путь в разделе «Обновление конфигурационных файлов сетевых устройств».

Ниже доступны следующие настройки Syslog-сервера:

- включение/выключение с помощью чекбокса приема Syslog-сообщений по UDP-протоколу и назначение соответствующего порта. По умолчанию чекбокс включен, поле «порт» активно, установлен 514 порт;
- включение/выключение с помощью чекбокса приема Syslog-сообщений по TCP-протоколу и назначение соответствующего порта. По умолчанию чекбокс выключен, поле «порт» неактивно, установлен 1468 порт;
- настройка уровней важности сообщений (таблица 1), обработку которых ЕЦУ Dallas Lock должен осуществлять. По умолчанию включены чекбоксы для уровней 0-5.

Таблица 1. Классификация уровней важности событий в Syslog

Значение	Уровень серьезности	Описание
0	Чрезвычайная ситуация (emergencies)	Система не работоспособна
1	Тревога (alerts)	Необходимо срочное вмешательство

2	Критические события (critical)	Критические события о состоянии СУ
3	Сообщения об ошибках (errors)	Условия ошибки
4	Всевозможные предупреждения (warning)	Условия предупреждения
5	Важные уведомления (notifications)	Нормальные, но важные условия (не являются ошибочными состояниями, но требуют особого внимания)
6	Информационные сообщения (informational)	Иные информационные сообщения, не требующие особого внимания
7	Отладочные сообщения (debugging)	Сообщения содержат информацию, используемую только при отладке

Параметры работы модулей

На вкладке «Модули» задается периодичность сбора журналов и синхронизации ЕЦУ Dallas Lock с модулями (рис. 51).

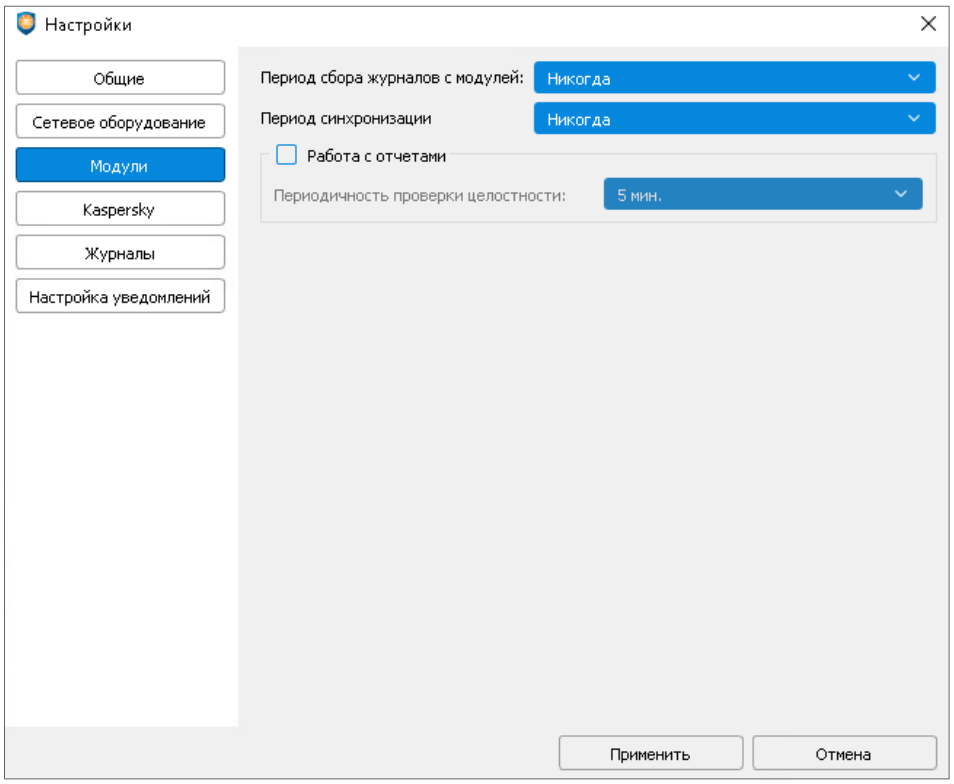

Рис. 51. Параметры модулей

Период сбора журналов с модулей и период синхронизации могут принимать значения от 5 минут до 1 недели и «Никогда». Значение по умолчанию — «Никогда».

Значения данных параметров АИБ должен задавать в зависимости от нагрузки сети, частоты вносимых изменений и количества подключенных модулей.

После установки флага «Работа с отчетами» возможно настроить периодичность проверки целостности отчетов модулей Агент ЕЦУ. Период проверки может принимать значения от 5 минут до 1 недели. По умолчанию функция «Работа с отчетами» — отключена.

Параметры Kaspersky

На вкладке «Kaspersky» (рис. 52) задается периодичность сбора журналов и синхронизации с сервером Kaspersky Security Center (KSC). Период сбора журналов с сервера KSC и период синхронизации могут принимать значения от 5 минут до 1 недели и «Никогда». Значение по умолчанию — «1 ч.».

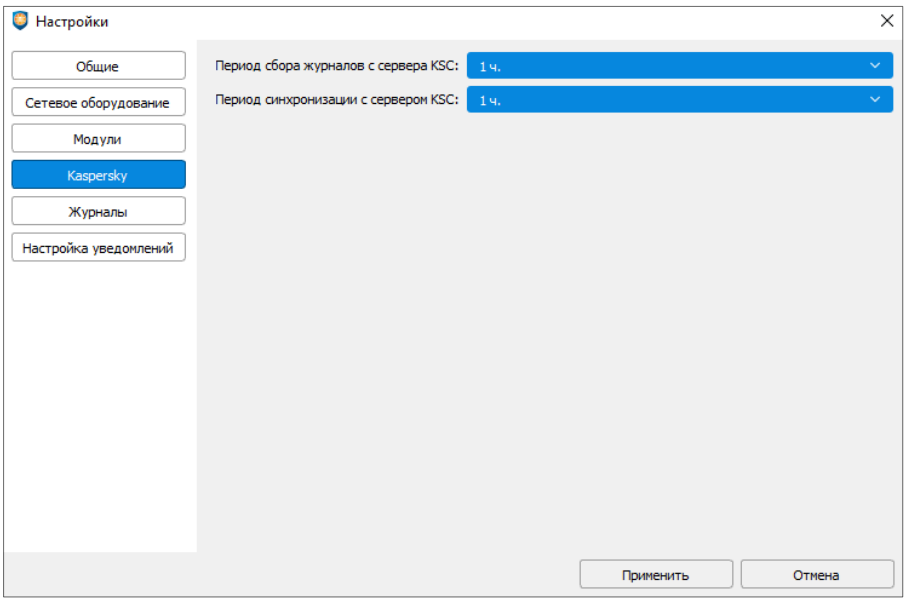

Рис. 52. Параметры Kaspersky

Параметры хранения журналов

На вкладке «Журналы» (рис. 53) отображается информация о текущем способе хранения журналов, выбранном в процессе установки, а также возможность редактирования способа хранения журналов уже на установленном ЕЦУ Dallas Lock.

При выборе «Использовать PostgreSQL» необходимо заполнить поля:

- адрес сервера;
- порт подключения;
- имя базы данных;
- имя пользователя;
- пароль.

При выборе «Использовать внутреннюю системы хранения» заполнять поля не нужно.

По умолчанию выбрано значение «Использовать внутреннюю систему хранения».

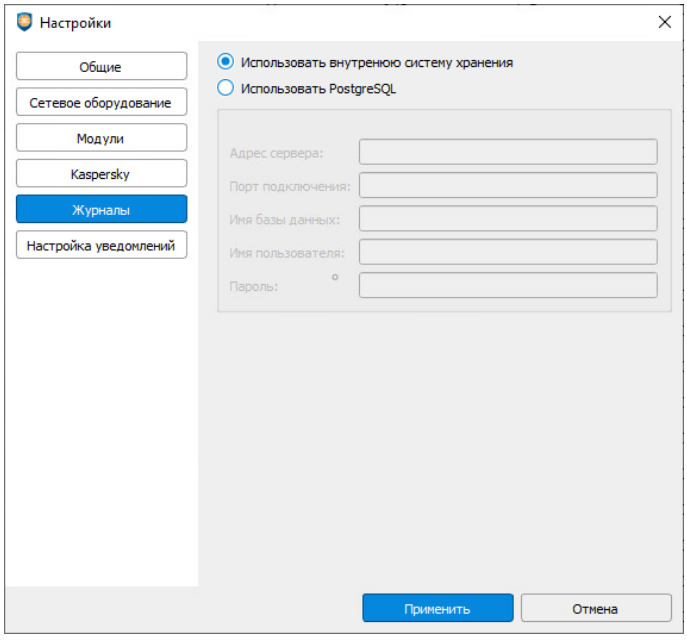

Рис. 53. Параметры хранения журналов

Настройка уведомлений

На вкладке «Настройка уведомлений» (рис. 54) можно определить кому и от кого будет отправлено письмо, также задать тему письма и его текст. Для редактирования вкладки необходимо установить флаг напротив строки «Отправлять уведомления» (по умолчанию флаг не выставлен). Тема и текст письма заданы по умолчанию.

В поле «Ключевые слова» необходимо заполнить поля:

- сервер;
- порт (по умолчанию — 25);
- пользователь;
- пароль.

В строке «Шифрование» выбрать необходимый вариант из предложенных:

- SSL/TLS;
- STARTTLS;
- Нет.

Проверить письмо и точность указанных данных, можно с помощью тестового письма, нажав на кнопку «Отправить тестовое письмо». После всех настроек нажать «Применить».

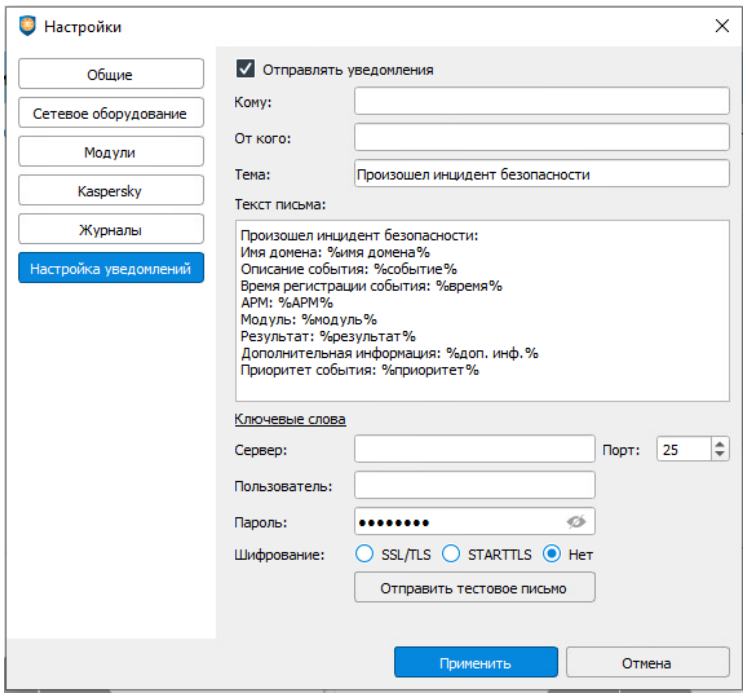

Рис. 54. Настройка уведомлений

5 ДОМЕН БЕЗОПАСНОСТИ ЕЦУ

На уровне ДБ в дереве объектов Консоли ЕЦУ формируется набор вкладок для общей настройки параметров безопасности для всего ДБ и для всех подчиненных объектов данного ДБ. При выборе определенной вкладки появляется возможность просматривать и редактировать параметры безопасности. При выделении вкладок через Ctrl/Shift можно совершить групповые операции обновления или удаления.

5.1 Сводка для ДБ

Для удобства работы возможно узнать общее состояние всего ДБ, данные сведения отображаются на вкладке «Сводка» (рис. 55).

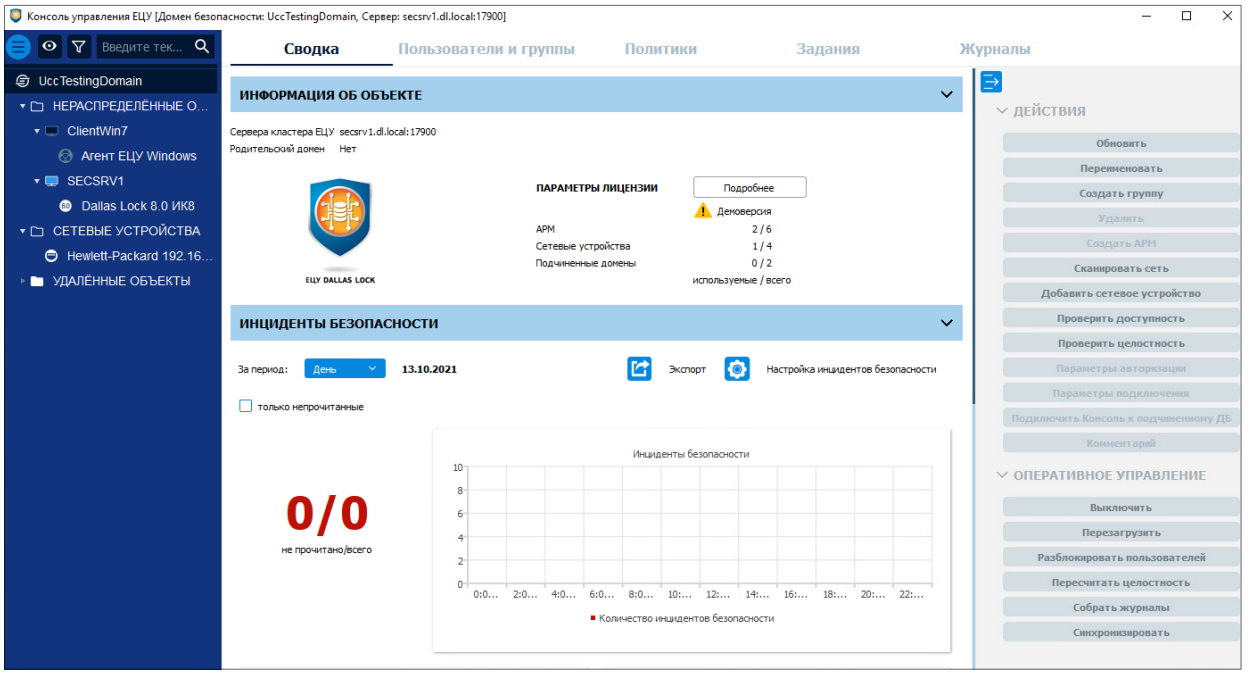

Рис. 55. «Сводка» Домена безопасности ЕЦУ

Доступны следующие действия с ДБ на панели инструментов:

1. Обновить информацию об объекте на вкладке «Сводка»;
2. Переименовать текущий ДБ;
3. Создать новую группу объектов в ДБ;
4. Сканировать сеть для обнаружения модулей и сетевых устройств;
5. Добавить новое сетевое устройство;
6. Проверить доступность сетевых устройств;
7. Проверить целостность сетевых устройств.

Перечисленные выше действия также доступны из контекстного меню узла ДБ в дереве объектов ДБ.

Команды оперативного управления на панели инструментов (набор команд зависит от объектов, входящих в состав ДБ):

1. Выключить;
2. Перезагрузить;
3. Разблокировать пользователей;
4. Пересчитать целостность;
5. Собрать журналы;
6. Синхронизировать;
7. Системный журнал;
8. Включить аварийный режим;
9. Отключить аварийный режим;

10. Удаленное включение;
11. Сбросить блокировки;
12. Обновить.

Примечание. Результат выполнения команд оперативного управления не отражается в Журналах ЕЦУ Dallas Lock. Также не предусмотрены всплывающие и прочие уведомления о результатах выполнения команд оперативного управления.

В рабочей области вкладки «Сводка» расположены следующие разделы:

1. «Информация об объекте» (рис. 56).

В данном разделе выводится информация:

- о серверах, введенных в кластер домена безопасности;
- о наличии родительского домена;
- о состоянии и параметрах лицензии на ЕЦУ Dallas Lock (описание настройки параметров лицензии приведено в разделе «Настройки лицензирования»).

Для обновления информации, представленной в данном разделе, следует нажать расположенную на панели «Действия» кнопку «Обновить» или перейти на любую другую вкладку и вернуться назад.

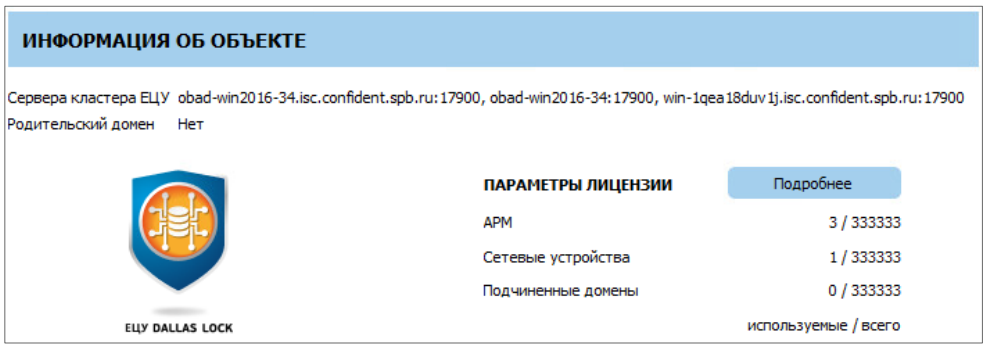

Рис. 56. Раздел «Информация об объекте»

2. «Инциденты безопасности» (рис. 57).

В разделе выводится информация о количестве инцидентов безопасности на всех подчиненных объектах ДБ за выбранный период в формате: не прочитано/всего инцидентов безопасности. При активном флаге «только непрочитанные» на информационной панели будет отображаться информация только о непрочитанных инцидентах безопасности.

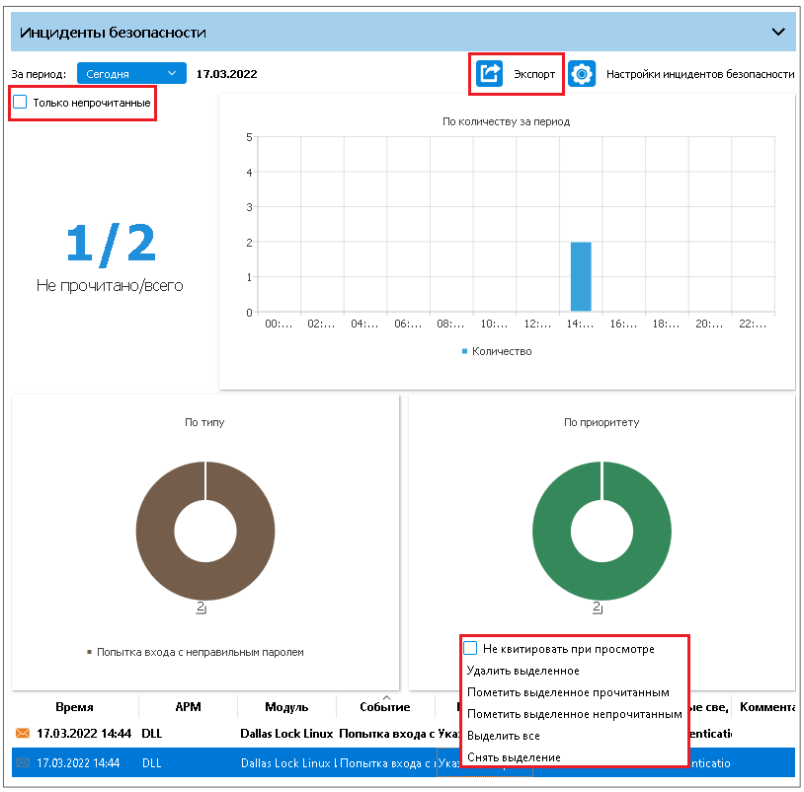

Рис. 57. Раздел «Инциденты безопасности»

Период времени можно изменить в верхней части информационной панели «Инциденты безопасности» с помощью выпадающего списка «За период». Возможны следующие варианты:

- сегодня;
- вчера;
- неделя;
- месяц;
- год;
- за все время;
- выбрать свой — при выборе данного пункта в появившемся окне (рис. 58) возможно задать необходимый отрезок времени.

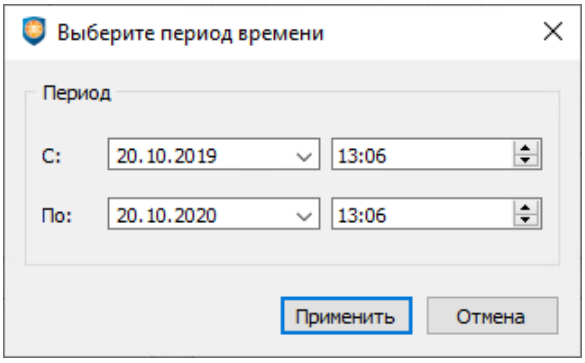

Рис. 58. Выбор периода времени

В центральной части информационной панели «Инциденты безопасности» расположена гистограмма, которая отображает количество инцидентов безопасности всех типов за выбранный период времени с определенным шагом (рис. 57). При нажатии на элемент гистограммы, в таблице отображаются инциденты за выбранный шаг времени.

Под гистограммой расположены круговые диаграммы:

- по типу — отображает количество инцидентов безопасности определенного типа;
- по приоритету — отображает количество инцидентов безопасности по их приоритетам.

Подробнее о настройке отображения информационной панели «Инциденты безопасности» описано в разделе «Настройка инцидентов безопасности».

В нижней части данной информационной панели расположена таблица с сообщениями об инцидентах безопасности. С помощью контекстного меню можно управлять списком инцидентов безопасности (рис. 57):

- не квитировать при просмотре (если чекбокс установлен — просмотренный инцидент не будет автоматически помечен как квитированный);
- удалить выделенное;
- пометить выделенное прочитанным;
- пометить выделенное непрочитанным;
- выделить все;
- снять выделение.

Двойной клик по сообщению с инцидентом откроет окно с данными об этом инциденте (рис. 59), в таблице выбранное сообщение квитируется как прочитанное (при отсутствии чекбокса в контекстном меню «Не квитировать при просмотре»). Нажимая на кнопки «вверх» и «вниз» можно отмечать сообщения как прочитанные, просматривая предыдущие или следующие инциденты.

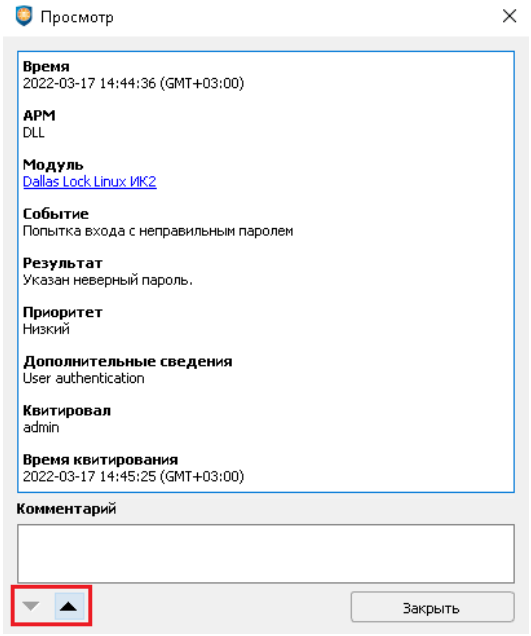

Рис. 59. Список учетных записей ДБ ЕЦУ

Реализована возможность экспорта отчета об инцидентах безопасности в файл по кнопке «Экспорт» (рис. 57). После нажатия «Экспорт», в появившемся окне, нужно указать путь для сохранения отчета (в формате .txt) с данными из таблицы с инцидентами безопасности.

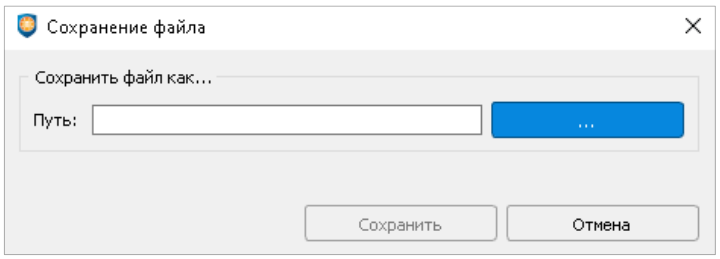

Рис. 60. Экспорт инцидентов безопасности в файл

Примечание. В таблице с сообщениями об инцидентах безопасности время события проставляется в зависимости от модулей, которые данное событие прислали — или время возникновения самого события на модуле, или время получения сообщения о событии на ЕЦУ Dallas Lock.

5.2 Пользователи и группы ДБ

Вкладка «Пользователи и группы» на уровне ДБ позволяет управлять глобальными учетными записями и группами пользователей ДБ ЕЦУ Dallas Lock (рис. 61).

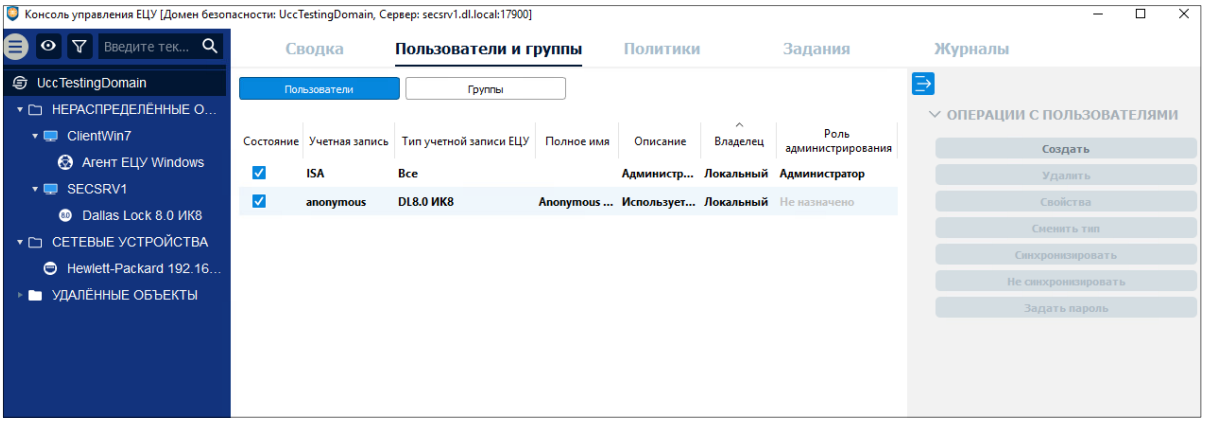

Рис. 61. Список учетных записей ДБ ЕЦУ

5.2.1 Параметры пользователей

Категория «Пользователи» на уровне ДБ содержит список глобальных учетных записей ДБ.

Список учетных записей пользователей на уровне ДБ представляет собой таблицу с полями:

1. «Состояние» — содержит флаг включения/выключения учетной записи пользователя на данном уровне. Поле «Состояние» принимает следующий вид:

☑ — отмеченное флагом поле означает, что данная учетная запись пользователя имеет доступ на уровне ДБ;

☐ — пустое поле означает, что учетная запись отключена для работы на уровне ДБ

Примечание. Значение поля «Состояние» не отражает состояние учетной записи пользователей на вложенных объектах ДБ. Например, учетная запись может быть отключена для работы на уровне ДБ (поле «Состояние» — пустое), но иметь доступ на уровне включенного в него АРМ (стоит флаг в поле «Состояние»).

Если изменить состояние учетной записи на уровне выше в дереве, на вложенных объектах — состояние изменится принудительно. Например, после отключения для работы учетной записи на уровне ДБ, работа учетной записи отключается для всех вложенных групп, АРМ (модулей в составе АРМ), модулей без АРМ и иных объектов.

2. «Учетная запись» — содержит имя учетной записи;
3. «Тип учетной записи ЕЦУ» — содержит информацию о том, для модулей какого типа применяется данная учетная запись. Возможные значения:
   - Все — учетная запись применима для всех модулей (кроме модуля WAF);
   - DL 8.0 — учетная запись применима для модуля СЗИ Dallas Lock 8.0 (см. «МОДУЛЬ СЗИ DALLAS LOCK 8.0-C/K»);
   - DLL — учетная запись применима для модуля СЗИ НСД Dallas Lock Linux (см. «МОДУЛЬ СЗИ НСД DALLAS LOCK LINUX»);
   - DL 8.0 СЗИ ВИ — учетная запись применима для модуля СЗИ ВИ Dallas Lock (см. «МОДУЛЬ СЗИ ВИ DALLAS LOCK»);
   - СДЗ — учетная запись применима для модуля СДЗ Dallas Lock (см. «МОДУЛЬ СДЗ

DALLAS LOCK»).

4. «Полное имя» — содержит полное имя учетной записи;
5. «Описание» — содержит описание учетной записи;
6. «Владелец» — указывает на каком уровне дерева ЕЦУ Dallas Lock была создана учетная запись;

Примечание. Учетные записи не отображаются на вкладке «Пользователи и группы» в категории «Пользователи» на уровне выше, чем уровень, на котором была создана учетная запись. Например, на уровне ДБ нельзя посмотреть учетные записи, созданные на уровне группы объектов.

Примечание. Если учетная запись была создана на уровне ДБ, то:

- на уровне ДБ — поле «Владелец» будет иметь значение «Локальный», и в списке учетная запись будет выделена жирным начертанием;
- на уровне группы (подгруппы) ДБ, АРМ (модулей в составе АРМ), модулей без АРМ и подчиненных доменов — поле «Владелец» будет иметь значение «ДБ *Имя_ДБ*».

Аналогично, если учетная запись была создана на уровне группы объектов, то:

- на уровне группы поле «Владелец» будет иметь значение «Локальный»;
- на уровне модулей этой группы, на которой была создана учетная запись, поле «Владелец» будет иметь значение «Группа *Имя_группы*».

7. «Роль администрирования» (см. «Ролевая модель учетных записей ДБ»).

Для применения изменений списка учетных записей на модулях необходима синхронизация.

Просмотр и настройка параметров пользователей доступны:

- по двойному щелчку левой кнопкой мыши на пользователя в списке;
- при выборе пункта «Свойства» из контекстного меню, вызванного щелчком правой кнопки мыши на пользователе в списке;
- при выделении учетной записи в списке и выборе пункта «Свойства» на панели инструментов «Операции с пользователями» (рис. 61).

Примечание. Настройка параметров пользователей доступна только на уровне владельца учетной записи пользователя.

После выполнения одного из этих действий открывается окно «Редактирование полей пользователя» (рис. 62).

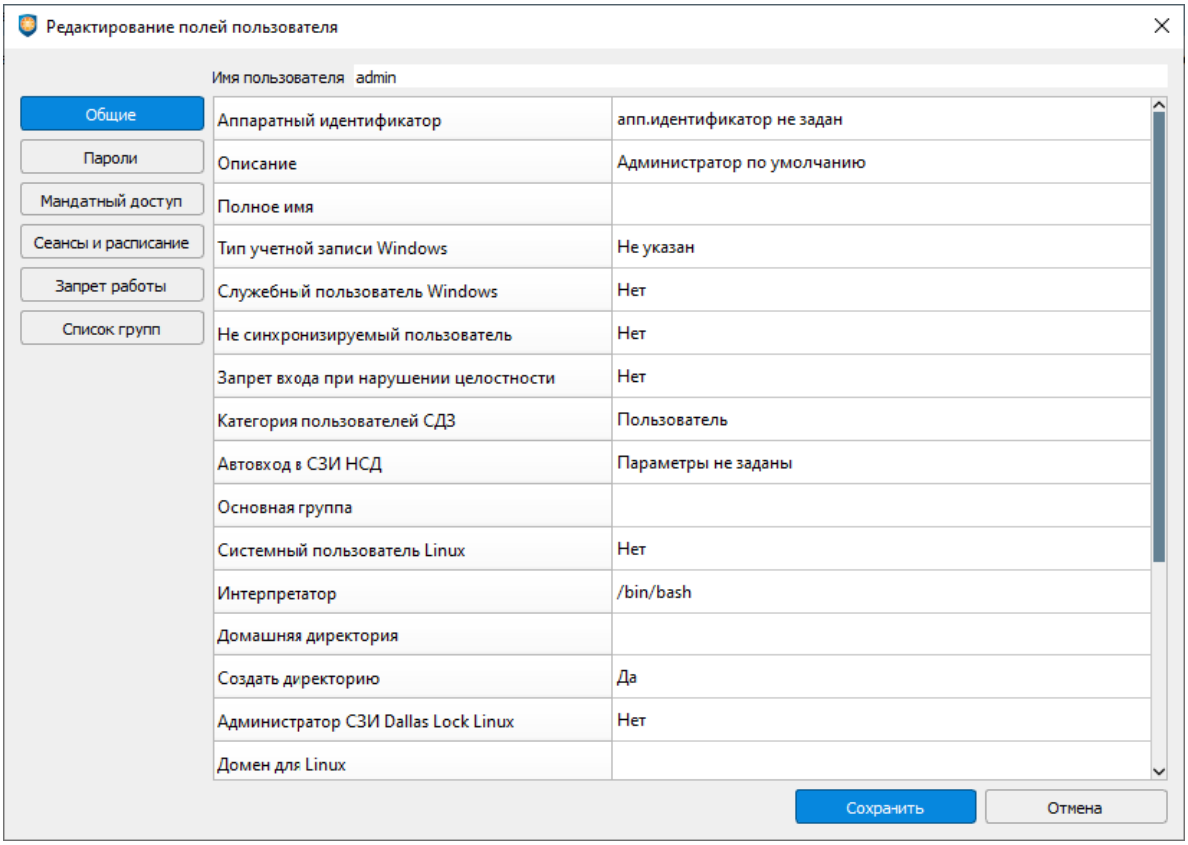

Рис. 62. Редактирование полей пользователя

На вкладке «Общие» предлагается заполнить учетные данные и параметры пользователей (таблица 2).

Таблица 2. Общие параметры пользователей

Заполняемые данные и параметры	Применение
Поле «**Аппаратный идентификатор**» позволяет выбрать аппаратный идентификатор пользователя.	ЕЦУ Dallas Lock; СЗИ Dallas Lock 8.0; СДЗ Dallas Lock; СЗИ НСД Dallas Lock Linux
В поле «**Описание**» можно ввести любой комментарий. Длина комментария не более 95 символов. Вводить комментарий не обязательно	ЕЦУ Dallas Lock; СЗИ Dallas Lock 8.0; СДЗ Dallas Lock СЗИ ВИ Dallas Lock
Заполнить «**Полное имя**». Вводить полное имя не обязательно. По умолчанию поле имеет пустое значение	ЕЦУ Dallas Lock; СЗИ Dallas Lock 8.0; СЗИ ВИ Dallas Lock
Выбрать **«Тип учетной записи Windows».** Для типа «Временный» обязательным условием является настройка расписания работы пользователя. По умолчанию тип учетной записи пользователя будет иметь значение «Не указан»	СЗИ Dallas Lock 8.0; СЗИ ВИ Dallas Lock
Значение «Да» в поле «**Служебный пользователь Windows**» предоставляет данной учетной записи пользователя особый статус. Требуется для корректной работы программ, при установке которых создаются свои учетные записи пользователей и осуществляется автоматический вход при загрузке ОС. Например, такой статус необходим при использовании программ VipNet или VMware. По умолчанию поле имеет значение «Нет»	СЗИ Dallas Lock 8.0; СЗИ ВИ Dallas Lock

Значение «Да» в поле **«Не синхронизируемый пользователь»** устанавливает статус, при котором данная учетная запись пользователя не синхронизируется с ДБ. По умолчанию поле имеет значение «Нет»	СЗИ Dallas Lock 8.0; СЗИ ВИ Dallas Lock
Система защиты обеспечивает проверку целостности программно-аппаратной среды ПК, объектов ФС и реестра. Если для пользователя опция «**Запрет входа при нарушении целостности**» активизирована, то при обнаружении нарушения целостности выдается соответствующее предупреждение и вход в ОС блокируется до тех пор, пока администратор не разблокирует учетную запись. Если же эта опция не включена, то при обнаружении нарушения целостности будет отображено только предупреждение.	СЗИ Dallas Lock 8.0; СДЗ Dallas Lock; СЗИ ВИ Dallas Lock
Назначить «**Категорию пользователя СДЗ**». Значение поля по умолчанию — «Пользователь» **Примечание.** Штатные пользователи, допущенные к работе на защищенном компьютере, не должны иметь категорию «Администраторы» или «Аудиторы».	СДЗ Dallas Lock
Атрибут «**Автовход в СЗИ НСД**» позволяет настроить автовход в СЗИ Dallas Lock 8.0. По умолчанию параметры автовхода не заданы.	СДЗ Dallas Lock
В поле «**Основная группа»** указывается наименование основной группы пользователя. Поле заполняется во время создания учетной записи.	СЗИ НСД Dallas Lock Linux
значение «Да» в поле «**Системный пользователь Linux**» указывает на то, что учетная запись пользователя является системной. По умолчанию поле имеет значение «Нет»	СЗИ НСД Dallas Lock Linux
Поле «**Интерпретатор**» указывает на интерпретатор командной строки. Обязательный атрибут учетной записи пользователя. По умолчанию имеет значение «/bin/bash».	СЗИ НСД Dallas Lock Linux
В поле «**Домашняя директория**» указывается путь к домашней директории пользователя.	СЗИ НСД Dallas Lock Linux
Значение «Да» в поле «**Создать директорию**» указывает на необходимость создания домашней директории пользователя. Если при создании учетной записи пользователя не будет создана домашняя директория, то вход в систему для этой учетной записи будет невозможен. По умолчанию параметр имеет значение «Нет».	СЗИ НСД Dallas Lock Linux
Значение «Да» в поле «**Администратор СЗИ НСД Dallas Lock Linux**» указывает на то, что пользователь является администратором СЗИ НСД Dallas Lock Linux. По умолчанию поле имеет значение «Нет».	СЗИ НСД Dallas Lock Linux
В поле «**Домен для Linux**» указывается имя домена Active Directory. Атрибут обязателен для доменных учетных записей пользователей.	СЗИ НСД Dallas Lock Linux
В поле «**(ВИ) Имя**» указать пользователя. Заполнять поле не обязательно.	СЗИ ВИ Dallas Lock
В поле «**(ВИ) Фамилия**» указать пользователя. Заполнять поле не обязательно.	СЗИ ВИ Dallas Lock

В поле «**(ВИ) E-mail**» указать пользователя. Заполнять поле не обязательно.	СЗИ ВИ Dallas Lock
В поле «**(ВИ) Тип учетной записи (для СЗИ ВИ)**» выбрать пользователей гипервизора. По умолчанию поле имеет значение «Пользователь Windows (Dallas Lock)».	СЗИ ВИ Dallas Lock
В поле **«(ВИ) Роль пользователя консоли СЗИ ВИ»** указать роль пользователя в консоли СЗИ ВИ. По умолчанию поле имеет значение «Нет доступа». **Внимание!** Все пользователи, создаваемые посредством ЕЦУ в Центре Управления СЗИ ВИ по умолчанию выключены. С целью настройки ЦУ СЗИ ВИ (например, распределения пользователей между клиентами СЗИ ВИ) необходимо использовать пользователей, для которых значение поля «Администратор СЗИ ВИ» имеет значение «Да».	СЗИ ВИ Dallas Lock
Поле **«Разрешить локальный вход в ОС с ЦУ СЗИ ВИ»** по умолчанию имеет значение «Нет»	СЗИ ВИ Dallas Lock

На вкладке «Пароли» предлагается заполнить учетные данные и параметры пользователей, относящиеся к настройкам паролей (таблица 3).

Таблица 3. Параметры паролей пользователей

Заполняемые данные и параметры	Применение
Значение «Да» в поле «**При следующем входе требовать смену пароля**» означает, что единовременно будет направлен запрос на смену пароля при входе пользователя в систему. По умолчанию поле имеет значение «Нет».	СЗИ Dallas Lock 8.0; СДЗ Dallas Lock; СЗИ ВИ Dallas Lock
Поле «**Запрет изменения пароля**». По умолчанию поле имеет значение «Нет».	СЗИ Dallas Lock 8.0; СДЗ Dallas Lock; СЗИ ВИ Dallas Lock
Значение «Да» в поле «**Пароль без ограничения срока действия**» отменяет действие политики входа «Максимальный срок действия паролей», распространяемой на всех пользователей. По умолчанию поле имеет значение «Нет».	СЗИ Dallas Lock 8.0; СДЗ Dallas Lock; СЗИ ВИ Dallas Lock
Поле «**Минимальный срок действия пароля (в днях)**» указывает на минимальный срок действия пароля в днях. Обязательное поле. Принимает значения от «1» до «180»[7]. Установка значения «Не используется» обозначает, что для данной учетной записи пользователя ограничений на период ее неиспользования накладываться не будет. По умолчанию имеет значение «Не используется».	СЗИ НСД Dallas Lock Linux
Поле «**Максимальный срок действия пароля (в днях)**» указывает на максимальный срок действия пароля в днях. Обязательное поле. Принимает значения от «1» до «180»[7].	СЗИ НСД Dallas Lock Linux

[7]**Внимание!** Если нарушено соотношение максимального и минимального сроков действия пароля (минимальный срок больше максимального), то при синхронизации списка пользователей с модулями СЗИ НСД Dallas Lock Linux возникает ошибка, создание/изменение параметров таких учетных записей не осуществляется.

Установка значения «Не используется» обозначает, что для данной учетной записи пользователя ограничений на период ее неиспользования накладываться не будет. По умолчанию имеет значение «Не используется».	
Поле «**Предупреждение о смене пароля (в днях)**» указывает на значение (в днях) после которого пользователю будут выдаваться уведомления о необходимости смены пароля, с указанием количества дней до истечения срока действия пароля. Обязательное поле. Принимает значения от «1» до «180». Установка значения «Не используется» обозначает, что для данной учетной записи пользователя ограничений на период ее неиспользования накладываться не будет. По умолчанию имеет значение «Не используется».	СЗИ НСД Dallas Lock Linux
Поле «**Дата последней смены пароля**». По умолчанию поле имеет значение «Не определено».	СЗИ НСД Dallas Lock Linux

На вкладке «Мандатный доступ» предлагается заполнить учетные данные и параметры, относящие к работе пользователя с уровнями доступа и мандатными метками в Домене безопасности (таблица 4).

Таблица 4. Мандатный доступ пользователей

Заполняемые данные и параметры	Применение
Необходимо выбрать «**Мандатный уровень»** (только для Dallas Lock 8.0 редакции «С»), под которым пользователь сможет работать.	СЗИ Dallas Lock 8.0
Необходимо указать «**Мандатные метки»** (только для Dallas Lock 8.0 редакции «С»), с которыми пользователь сможет работать.	СЗИ Dallas Lock 8.0

На вкладке «Сеансы и расписание» предлагается заполнить учетные данные и параметры, относящиеся к ограничениям работы пользователя по времени (таблица 5).

Таблица 5. Сеансы и расписание пользователей

Заполняемые данные и параметры	Применение
Определить «**Число разрешенных сеансов**». При установленном значении для каждой учетной записи будет проверяться количество одновременных интерактивных и сетевых сессий (входов) на модуле.	СЗИ Dallas Lock 8.0; СЗИ НСД Dallas Lock Linux; СЗИ ВИ Dallas Lock
Необходимо задать «**Расписание работы**» пользователя, выбрать период и время. Вне указанного периода пользователь не сможет зайти на модуль. По окончании времени работы ПК пользователя будет заблокирован при условии включения политики «Принудительное завершение работы по расписанию» («Политики» → «Права пользователей»). **Примечание.** «Расписание работы» пользователя может быть определено с дискретностью 30 минут.	СЗИ Dallas Lock 8.0; СДЗ Dallas Lock; СЗИ НСД Dallas Lock Linux
Указать допустимый «**Период неиспользования (в днях)**». Если период, в который под учетной записью не производился вход в систему, превышает выбранный допустимый период — учетная запись блокируется. Обязательное поле. Принимает значения от «1» до «180». Установка значения «Не используется» обозначает, что для	СЗИ НСД Dallas Lock Linux

данной учетной записи пользователя ограничений на период ее неиспользования накладываться не будет. По умолчанию имеет значение «Не используется».	
Задать дату «**Истечение срока действия учетной записи**». По умолчанию поле имеет значение «Без ограничений». При снятом флаге «Без ограничений» становится активным поле для выбора даты. В поле указывается дата, когда данная учетная запись будет заблокирована системой. В этом случае поле обязательно для заполнения. При активном флаге поле для установки даты неактивно, время действия учетной записи не ограничено.	СЗИ НСД Dallas Lock Linux

На вкладке «Запрет работы» предлагается заполнить учетные данные и параметры, относящиеся к ограничению работы пользователя при наступлении определенных событий в системе или установки запрета администратором (таблица 6).

Таблица 6. Запрет работы пользователей

Заполняемые данные и параметры	Применение
Значение «Да» в поле «**Учетная запись отключена**» дает возможность отключить учетную запись любого пользователя, после чего пользователь не сможет войти на АРМ до тех пор, пока администратор ЕЦУ не деактивирует эту опцию. По умолчанию поле имеет значение «Нет».	СЗИ Dallas Lock 8.0; СДЗ Dallas Lock; СЗИ ВИ Dallas Lock
При значении «Да» поля «**Запретить работу при событиях вскрытия корпуса**» вход в систему блокируется при срабатывании ДВК. На экране приглашения в систему отображается соответствующее сообщение. По умолчанию поле имеет значение «Нет». **Примечание.** Данный атрибут не применим для вариантов исполнения изделия ПФНА.501410.003-02 и ПФНА.501410.003-04 (платы СДЗ Dallas Lock формата PCIe «КТ-521» и M.2 «КТ-550»).	СДЗ Dallas Lock
Значение «Да» в поле «**Блокировать загрузку нештатной ОС**» устанавливает запрет на загрузку ОС с носителя, отличающегося от указанного в поле «Загрузочное устройство» вкладки «Параметры» оболочки администратора СДЗ Dallas Lock. По умолчанию поле имеет значение «Нет».	СДЗ Dallas Lock
При значении «Да» поля «**Запретить работу при сломанных или ненастроенных часах**» вход в систему блокируется при неисправности часов. На экране приглашения в систему отображается соответствующее сообщение. По умолчанию поле имеет значение «Нет». **Примечание.** Данный атрибут не применим для вариантов исполнения изделия ПФНА.501410.003-02 и ПФНА.501410.003-04 (платы СДЗ Dallas Lock формата PCIe «КТ-521» и M.2 «КТ-550»).	СДЗ Dallas Lock
При значении «Да» поля «**Запретить работу при неисправности ДСЧ**» вход в систему блокируется при неисправности датчика случайных чисел платы СЗД Dallas Lock. На экране приглашения в систему отображается соответствующее сообщение. По умолчанию поле имеет значение «Нет».	СДЗ Dallas Lock

На вкладке «Список групп» с помощью кнопки «Добавить…» администратор имеет возможность включить пользователя в определенную группу. В основной рабочей области отображены названия групп, в которые включен пользователь (рис. 63). При выборе группы из основной рабочей области ее возможно удалить из списка с помощью кнопки «Удалить».

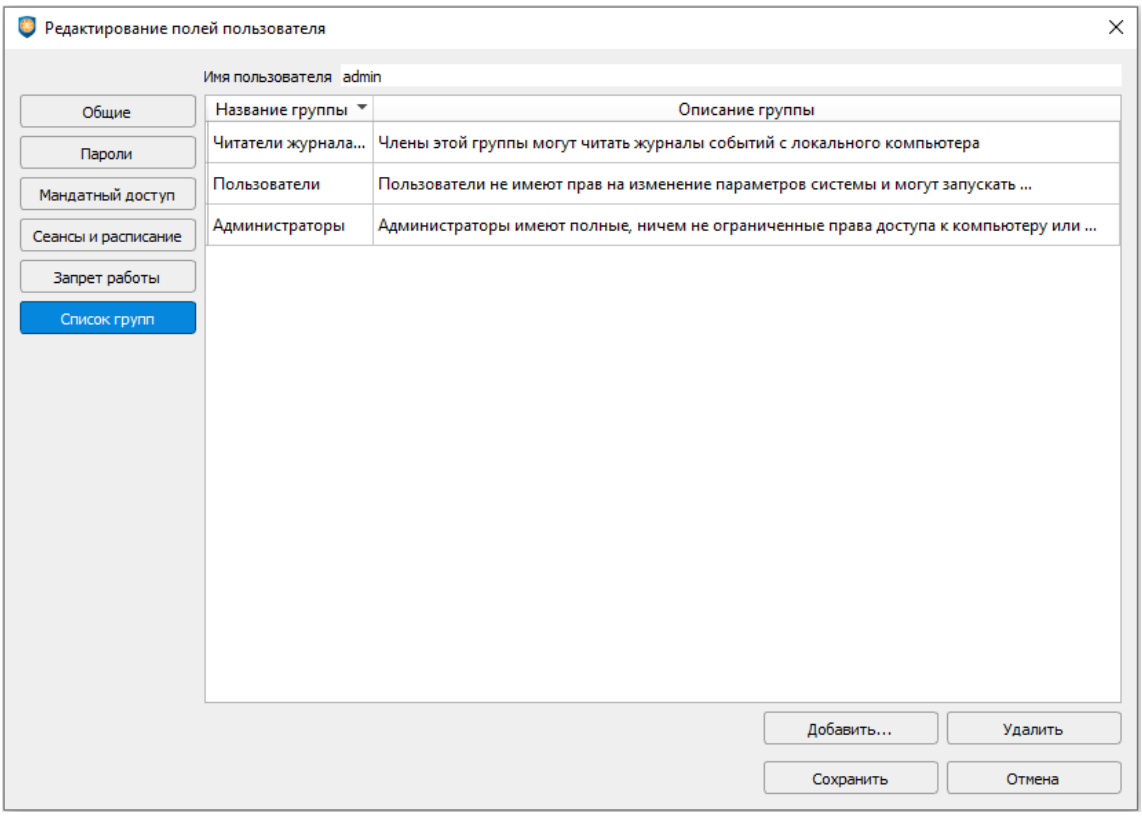

Рис. 63. Список групп пользователя

Примечание. Вкладка «Список групп» недоступна для учетной записи **anonymous**.

5.2.2 Параметры групп пользователей

Категория «Группы» на уровне ДБ содержит список глобальных учетных записей ДБ.

Рабочая область категории «Группы» представляет собой таблицу с полями:

1. «Состояние» — содержит флаг включения/выключения группы пользователей на данном уровне. Поле «Состояние» принимает следующий вид:

☑ — отмеченное флагом поле означает, что данная группа пользователей имеет доступ на уровне ДБ;

☐ — пустое поле означает, что данная группа пользователей не имеет доступа на уровне ДБ.

Примечание. Значение поля «Состояние» не отражает состояние группы пользователей на вложенных в группу объектах. Например, учетная запись может быть отключена для работы на уровне группы (поле «Состояние» — пустое), но иметь доступ на уровне включенного в нее АРМ (стоит флаг в поле «Состояние»).

Если изменить состояние учетной записи на уровне выше в дереве — на вложенных объектах состояние изменится принудительно. Например, после отключения для работы группы пользователей на уровне группы, работа группы пользователей отключается для всех вложенных подгрупп, АРМ (модулей в составе АРМ) и модулей без АРМ.

2. «Название группы» — содержит имя группы пользователей.
3. «Тип» — содержит информацию, о том для модулей какого типа применяется данная группа пользователей.
4. «Описание группы» — содержит описание группы пользователей.
5. «Владелец» — указывает на каком уровне дерева ЕЦУ Dallas Lock была создана группа пользователей.

Примечание. Группы пользователей не отображаются в категории «Группы» на вкладке «Пользователи и группы» на уровне выше, чем уровень, на котором была создана группа пользователей. Например, на уровне ДБ нельзя посмотреть группы пользователей, созданные на уровне группы ДБ.

Примечание. Если группа пользователей была создана на уровне ДБ, то:

- на уровне ДБ — поле «Владелец» будет иметь значение «Локальный», и в списке группа пользователей будет выделена жирным начертанием;
- на уровне группы (подгруппы) ДБ, АРМ (модулей в составе АРМ), модулей без АРМ и подчиненных доменов — поле «Владелец» будет иметь значение: *«ДБ *Имя_ДБ*»*.

Аналогично, если группа пользователей была создана на уровне группы объектов ДБ, то:

- на уровне группы ДБ поле «Владелец» будет иметь значение *«Локальный»;*
- на уровне модулей этой группы, на которой была создана группа пользователей, поле «Владелец» будет иметь значение *«Группа *Имя_группы*».*

Для применения изменений списка групп пользователей, на модулях необходима синхронизация.

В категории «Группы» на вкладке «Пользователи и группы» доступно только:

- создание и удаление групп (удаление невозможно для групп по умолчанию);
- редактирование описания групп (невозможно для групп по умолчанию);
- изменение типа группы.

Просмотр и настройка параметров групп доступны:

- по двойному щелчку левой кнопкой мыши по группе в списке;
- при выборе пункта «Свойства» из контекстного меню, вызванного щелчком правой кнопки мыши на группе в списке;
- при выделении группы в списке и выбору пункта «Свойства» на панели инструментов «Операции с группами».

После выполнения одного из этих действий открывается окно «Редактирование полей группы» (рис. 64).

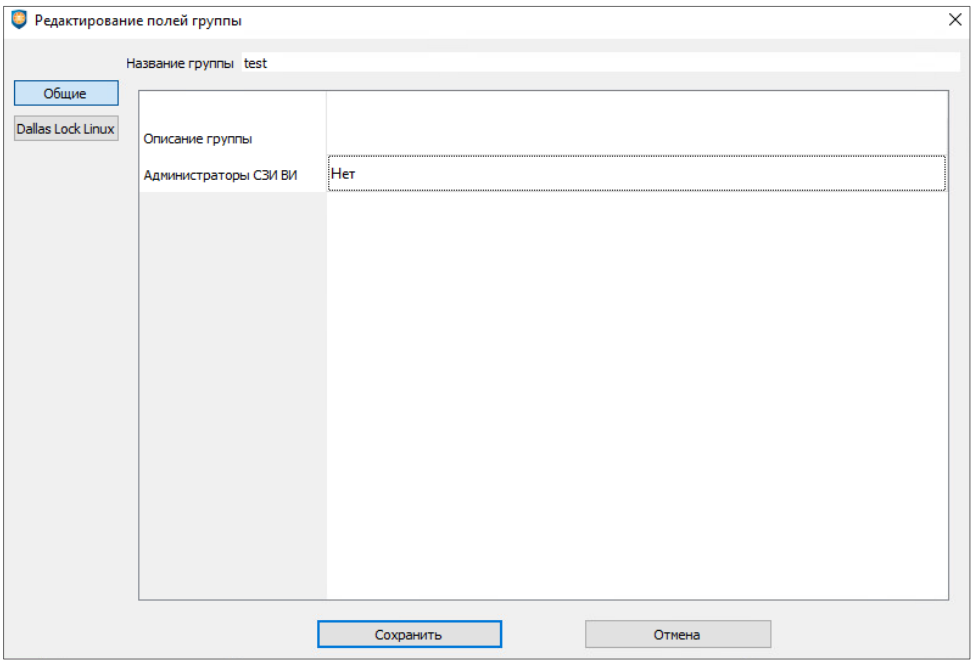

Рис. 64. Редактирование полей групп

На вкладке «Общие» предлагается оставить комментарий в поле «Описание группы», назначить пользователей, входящих в группу, на роль «Администратор ВИ» в ЦУ СЗИ ВИ в поле «(ВИ) Администраторы СЗИ ВИ» и выбрать пользователей гипервизора в поле «(ВИ) Тип учетной записи (для СЗИ ВИ)».

На вкладке «Dallas Lock Linux» предлагается выбрать значение атрибута «Системная группа». Атрибут принимает значения «Да» и «Нет». По умолчанию значение атрибута «Нет».

Примечание. Вкладка «Dallas Lock Linux» доступна только для групп пользователей, применяющихся на модуле СЗИ НСД Dallas Lock Linux (поле «Тип» может принимать значения «DLL» или «Все»).

Назначить все необходимые политики безопасности для группы можно, редактируя политики безопасности различных категорий.

Примечание. Включение и исключение пользователей из групп осуществляется в параметрах пользователей на вкладке «Список групп».

5.2.3 Создание пользователей ДБ

Список учетных записей ДБ на вкладке «Пользователи и группы» → «Пользователи» формируется из учетных записей по умолчанию и зарегистрированных через Консоль ЕЦУ.

По умолчанию в ЕЦУ Dallas Lock всегда присутствуют следующие глобальные учетные записи:

- **anonymous** — учетная запись используется для сетевых входов с незащищенных компьютеров;
- **администратор по умолчанию** — учетная запись, регистрируемая в процессе установки ЕЦУ Dallas Lock.

В ЕЦУ Dallas Lock возможна регистрация пользователей следующих видов:

1. Глобальные пользователи, созданные средствами Консоли ЕЦУ.
2. Доменные пользователи, созданные средствами службы AD (если ДБ находится в ЛВС под управлением контроллера домена).

Число зарегистрированных пользователей на каждом АРМ ограничивается только размером свободного дискового пространства.

Для создания глобальных пользователей с помощью Консоли ЕЦУ необходимо:

1. Открыть вкладку «Пользователи и группы» в Консоли ЕЦУ.
2. Выбрать категорию «Пользователи».
3. На панели инструментов в операциях с пользователями нажать «Создать» или выбрать соответствующий пункт из контекстного меню.
4. На экране появится окно создания пользователя (рис. 65).

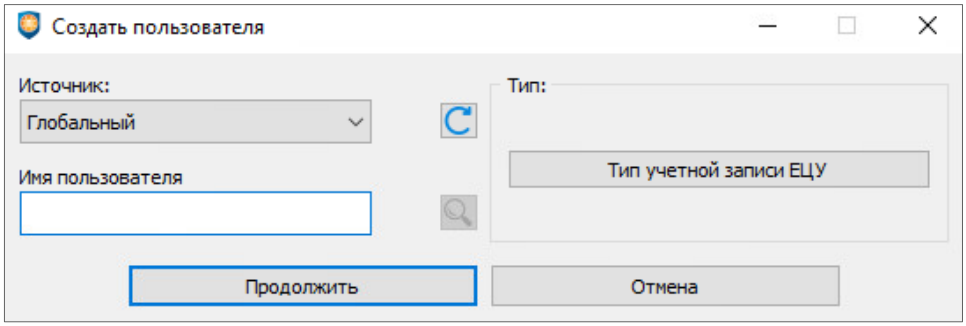

Рис. 65. Создание пользователя

5. В поле источник выбрать «Глобальный».
6. В поле «Имя пользователя» ввести логин (имя) регистрируемого пользователя. При вводе имени в системе существуют следующие правила:
   - максимальная длина имени — 20 символов;
   - имя может содержать латинские символы, символы кириллицы, цифры и специальные символы (кроме запрещенных ОС: " / \ [ ] : | < > + = ; , ? @ *);
   - разрешается использовать различные регистры клавиатуры, при этом регистр не учитывается (User и user являются одинаковыми именами).

Примечание. При наличии в Домене безопасности ПК, работающих под ОС Linux, не рекомендуется использовать кириллические символы в именах пользователей и групп в связи с отсутствием гарантии обеспечения корректной работы.

Примечание. Имя учетной записи считается уникальным в рамках одного Домена безопасности.

Примечание. После создания нового пользователя изменить его имя посредством Консоли ЕЦУ невозможно.

7. Выбрать «Тип учетной записи» в зависимости от того, для модулей какого типа применяется данная учетная запись пользователя.

   Изменить тип учетной записи можно, используя кнопку «Сменить тип» на панели инструментов «Операции с пользователями» или выбрав данное действие из контекстного меню.
8. После нажатия «Продолжить» появится окно для редактирования параметров учетной записи пользователя (см. «Параметры пользователей»).

   Изменить параметры учетной записи можно, используя кнопку «Свойства» на панели инструментов «Операции с пользователями» или выбрав данное действие из контекстного меню.
9. Завершающей операцией по созданию учетной записи пользователя является назначение пароля (см. «Назначение пароля»). Назначение пароля предлагается после заполнения всех необходимых параметров в окне создания учетной записи и нажатия кнопки «Сохранить».

Учетная запись будет создана на модуле после синхронизации с ЕЦУ Dallas Lock.

5.2.4 Назначение аппаратного идентификатора

Перед назначением аппаратного идентификатора рекомендуется устанавливать драйверы, поставляемые в комплекте с идентификатором, или скачать их с сайта производителя. Также рекомендуется форматировать АИ перед его назначением пользователю, как при новом назначении, так и при изменении способа записи в память АИ для того же пользователя.

Примечание. Работа аппаратных идентификаторов через подключение типа shared к КУ ЕЦУ в виртуальных машинах VMWare Workstation не гарантируется. Необходимо использовать обычное подключение или КУ ЕЦУ запускать с локальных АРМ.

Для назначения аппаратного идентификатора пользователю необходимо:

1. Открыть окно «Редактирование полей пользователя».
2. Выбрать вкладку «Общие».
3. Дважды щелкнуть левой кнопкой мыши по параметру «Аппаратный идентификатор».
4. Откроется окно «Назначение аппаратного идентификатора» (рис. 66).

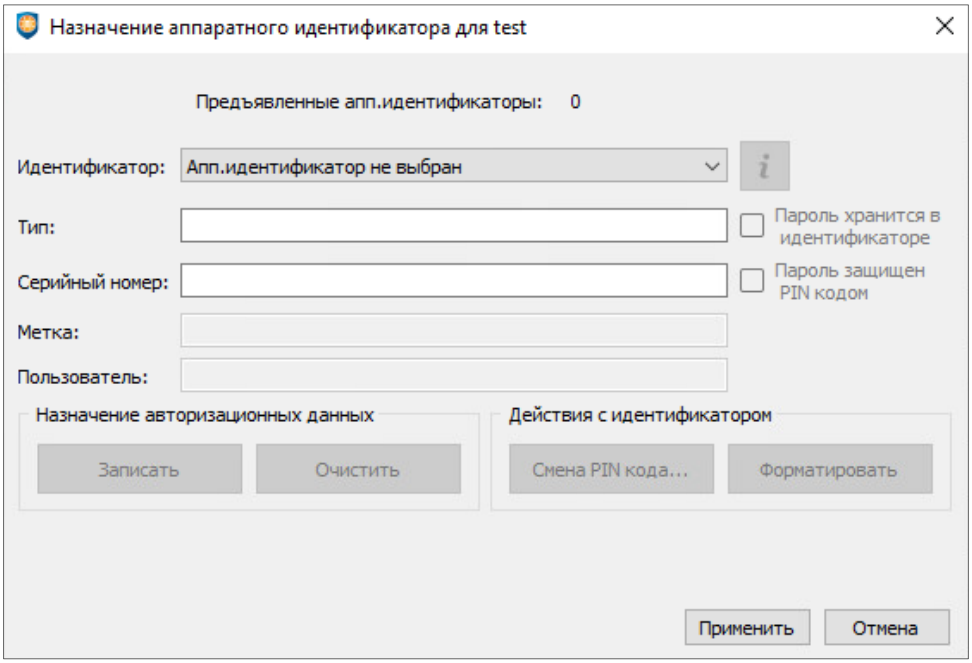

Рис. 66. Окно назначения аппаратного идентификатора

5. Предъявить аппаратный идентификатор, вставив его в соответствующий USB-порт или прикоснувшись к считывателю (в зависимости от типа идентификатора).
6. В строке состояния «Предъявленные апп.идентификаторы» будет указанно количество предъявленных в данный момент идентификаторов, а в списке выпадающего меню «Идентификатор» появятся их наименования.
7. Выбрать необходимый идентификатор из списка.
8. Далее в полях с параметрами АИ появятся: тип, серийный номер, и для некоторых видов идентификаторов станут доступны дополнительные функции (рис. 67). Кнопка позволяет открыть окно с информацией о параметрах выбранного идентификатора.

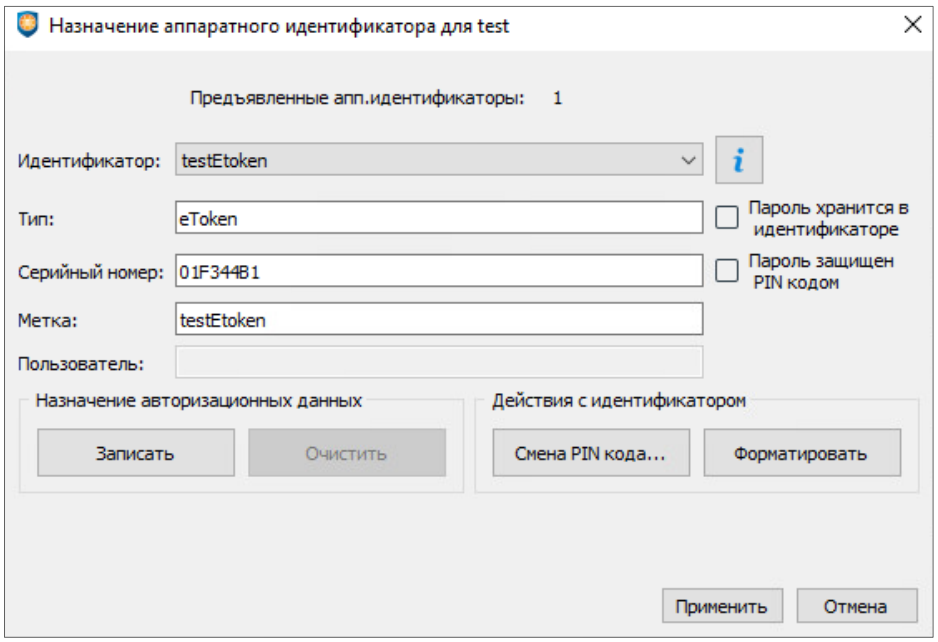

Рис. 67. Параметры назначенного идентификатора

9. Для назначения пользователю выбранного аппаратного идентификатора необходимо нажать «Применить» и далее «Сохранить».

После назначения АИ учетной записи (для входа в ОС на модулях или для подключения к серверу ЕЦУ Dallas Lock), помимо ввода авторизационной информации, потребуется предъявить назначенный аппаратный идентификатор.

Примечание. При изменении параметров доступа АИ и синхронизации через ЕЦУ на СЗИ НСД Dallas Lock Linux выполняется сброс «типа доступа» АИ до значения ЕЦУ: «UCC» для графической оболочки и «SET FROM UCC» для консольной.

При последующей авторизации пользователя в Linux, в СЗИ НСД Dallas Lock Linux присваивается соответствующий тип доступа, что и на ЕЦУ.

Назначение авторизационных данных

Записать в память аппаратного идентификатора авторизационные данные (логин и пароль) учетной записи пользователя, которому он назначается, можно тремя способами:

1. Записать в память идентификатора *логин и пароль* пользователя и хранение данных *защитить PIN-кодом*.

Для этого необходимо выполнить следующее:

- выбрать в выпадающем списке необходимый идентификатор;
- отметить флагом поле **«Пароль хранится в идентификаторе»**. Поле **«Пароль защищен PIN-кодом»** выделится автоматически. Далее нажать кнопку «Записать» (рис. 68);

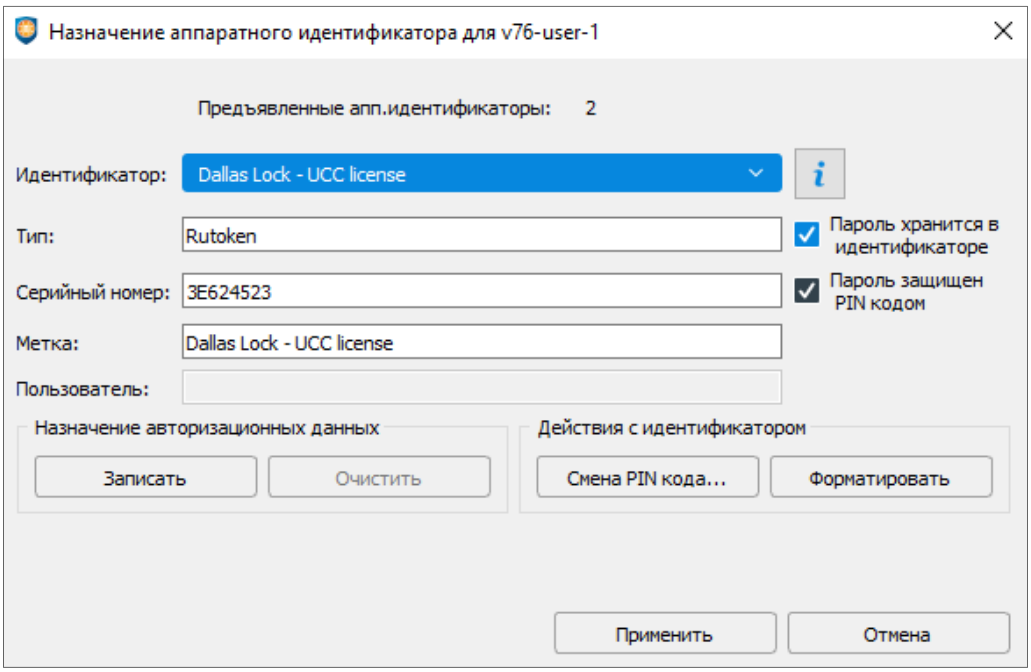

Рис. 68. Запись авторизационной информации в идентификатор

- в появившемся окне ввести: PIN-код идентификатора и пароль пользователя с подтверждением (рис. 69), нажать «OK»;

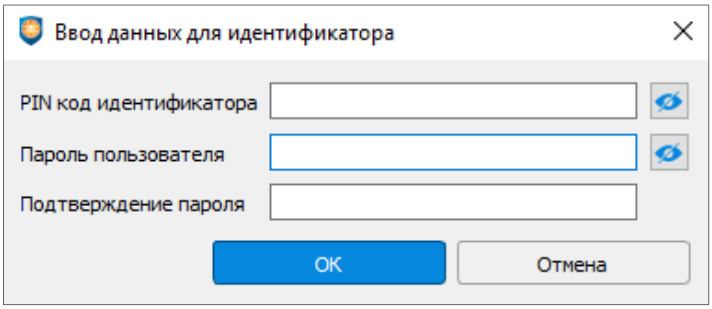

Рис. 69. Ввод дополнительной информации

- в окне параметров учетной записи системы защиты нажать «Применить» и «OK».

После этого в память данного идентификатора будет прописан логин и пароль учетной записи пользователя, причем пароль будет защищен PIN-кодом самого идентификатора.

Теперь для входа в ОС, после предъявления идентификатора, пользователю необходимо заполнить только поле ввода PIN-кода (логин и пароль считаются автоматически, для считывания пароля потребуется ввод PIN-кода).

2. Записать в память идентификатора *логин и пароль* учетной записи.

Для этого необходимо выполнить следующее:

- снять флаг для поля «Пароль защищен PIN-кодом»;
- записать авторизационные данные (кнопка «Записать»).

В этом случае пароль учетной записи в идентификаторе — незащищен, и система выдаст предупреждение.

Таким образом, для входа в ОС пользователю станет достаточным только предъявление идентификатора (логин и пароль считаются автоматически).

3. Записать в память идентификатора *только логин* учетной записи пользователя.

Для этого не требуется выделение полей хранения паролей. Достаточно нажать «Записать». Система потребует ввести дополнительно только PIN-код пользователя данного

идентификатора.

При входе в ОС после предъявления идентификатора учетная запись будет однозначно идентифицирована с логином данного конкретного пользователя, остальные авторизационные поля пользователю необходимо будет ввести самостоятельно.

Для того, чтобы *удалить авторизационную информацию из памяти идентификатора*, нужно воспользоваться одним из следующих способов:

- нажать «Очистить» в поле назначения авторизационных данных;
- отформатировать идентификатор методом, описанным в пункте «Действия с идентификатором». В этом случае помимо удаления системой защиты авторизационных данных из памяти идентификатора администратору безопасности необходимо изменить PIN-коды идентификатора.

Авторизация с записанными данными возможна при входе в ОС после включения компьютера, а также при разблокировке компьютера и терминальном подключении.

Действия с идентификатором

Для работы с некоторыми аппаратными идентификаторами необходимы *их авторизационные PIN-коды:* PIN-код администратора и PIN-код пользователя, которые уже установлены в памяти самих идентификаторов по умолчанию (так называемые «заводские настройки»). Информацию о них можно получить из документации, поставляемой вместе с аппаратными идентификаторами и драйверами.

Внимание! Для обеспечения требуемого уровня безопасности PIN-коды по умолчанию для аппаратных идентификаторов следует изменить.

Изменить пароль аппаратного идентификатора можно с помощью утилиты для идентификатора (скачать с сайта производителя), либо используя окно параметров назначенного пользователю идентификатора (рис. 67). Для этого в поле «Действия с идентификатором» необходимо выбрать кнопку «Смена PIN-кода» или кнопку «Форматировать».

По нажатию кнопки «Смена PIN-кода» откроется окно, в котором необходимо ввести значения PIN-кода пользователя: старое (текущее) значение, новое значение и повтор нового значения. Дополнительные кнопки рядом с полями ввода позволят изменить скрытые символы на явные, повтор ввода PIN-кода в этом случае не потребуется (рис. 70).

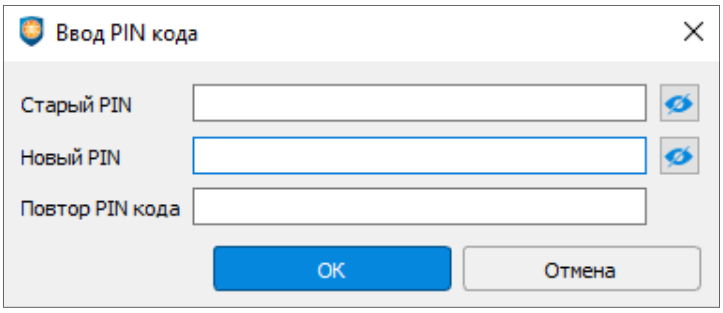

Рис. 70. Окно смены PIN-кода

Для форматирования аппаратного идентификатора нажать «Форматировать» откроется окно (рис. 71), в котором необходимо заполнить следующие поля:

- *Текущий PIN-код администратора* данного аппаратного идентификатора, необходимый для легального форматирования идентификатора.

Ввести новые данные:

- *Метка* — любое наименование.
- *Новый PIN-код* администратора и повтор.
- *Новый PIN-код* пользователя и повтор.

Если два данных PIN-кода совпадают, то флаг в поле «PIN-код администратора и пользователя совпадают» позволит ввести PIN-код только в одно поле.

Внимание! Параметры символов PIN-кода для идентификатора (наличие цифр, букв и другие) определяются настройкой параметров в утилите соответствующего идентификатора. Прежде чем изменять PIN-коды идентификатора, следует настроить данные параметры в утилите (по умолчанию *выключены).*

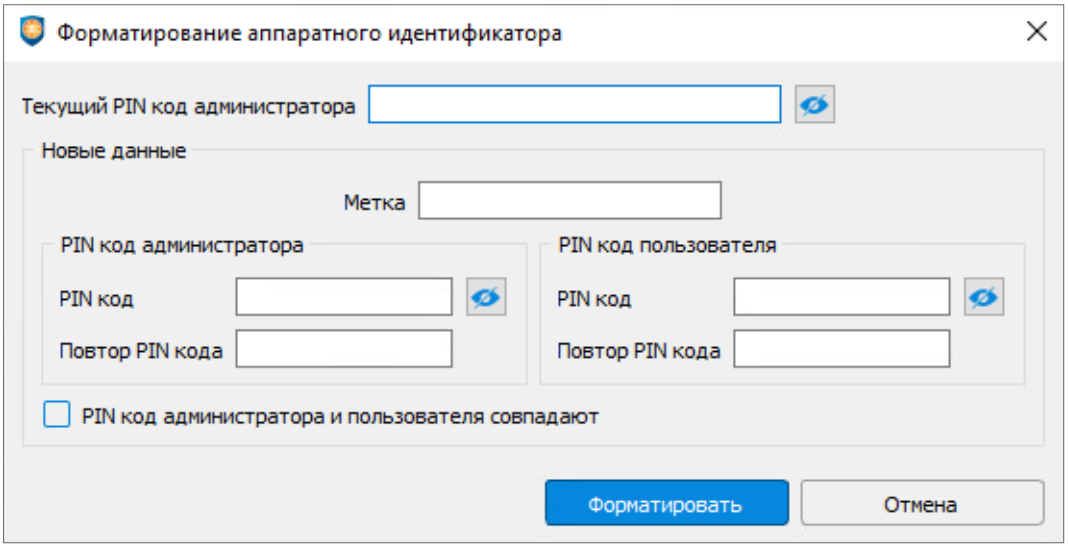

Рис. 71. Окно форматирования идентификатора

Примечание. Для аппаратных идентификаторов Рутокен:

1) Форматировать идентификатор нужно в утилите производителя («Панель управления Рутокен»).
2) Если на Рутокен ранее были записаны какие-либо данные для аппаратной аутентификации, перед тем как записать на АИ аутентификационную информацию в КУ ЕЦУ, необходимо произвести форматирование данного АИ в утилите производителя.

Снятие аппаратной идентификации

Для того, чтобы снять назначение аппаратного идентификатора для учетной записи отдельного пользователя, необходимо в окне параметров учетной записи в поле «Идентификатор» (рис. 67) выбрать значение «Аппаратный идентификатор не назначен», нажать «Применить» и «ОК».

Сам идентификатор для последующего применения рекомендуется очистить от авторизационных данных, если они были назначены (см. «Назначение авторизационных данных»), или отформатировать.

5.2.5 Удаление пользователей ДБ

Внимание! Следует внимательно относиться к удалению пользователей в ДБ. Если на каком-либо из уровней Домена безопасности не останется ни одного пользователя с ролью «Администратор» (см. «Ролевая модель учетных записей ДБ»), доступ к настройкам на этом уровне будет ограничен до момента появления пользователя с достаточным набором привилегий.

Для удаления пользователя из Домена безопасности вне зависимости от того, какими средствами он создан или зарегистрирован в самом ДБ, необходимо выделить его имя в списке на уровне «Владельца», нажать кнопку «Удалить» или выбрать соответствующее действие из контекстного меню. Учетная запись будет удалена с модулей после синхронизации с ЕЦУ Dallas Lock.

5.2.6 Назначение пароля

Для назначения пароля пользователю необходимо выделить его имя в списке и нажать кнопку «Задать пароль». Появится окно, где требуется ввести новый пароль и подтвердить его (рис. 72).

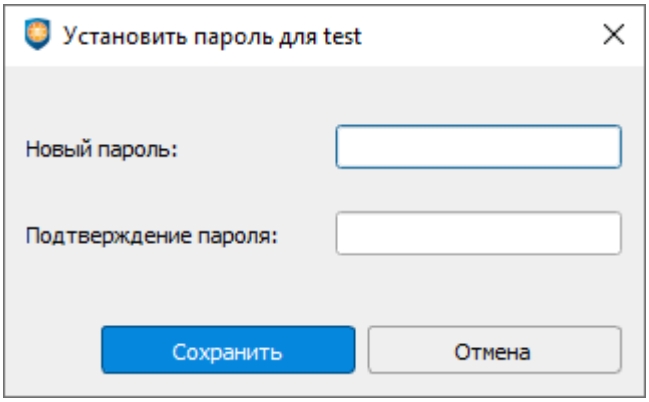

Рис. 72. Форма ввода пароля

При вводе пароля необходимо руководствоваться следующими правилами:

- максимальная длина пароля составляет 31 символ;
- пароль может содержать латинские символы, символы кириллицы, цифры и специальные символы;
- сложность пароля (наличие определенных символов, длина, срок действия и прочие) регулируется специальными политиками, которые устанавливаются администратором (см. «Настройка парольных политик»).

После ввода нового пароля возникнет дополнительная кнопка . Иконка изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто.

При задании пароля глобальной учетной записи ДБ необходимо, чтобы пароль соответствовал парольным политикам безопасности ОС Windows на модулях. Если требование не будет соблюдено, то возникнет ошибка «Операция заблокирована ОС Windows» в процессе синхронизации учетных записей. Из-за данной ошибки может наблюдаться следующее:

- проблема создания учетной записи с недостаточно сложным паролем;
- проблема синхронизации пароля учетной записи, если пользователь был создан ранее.

Во избежание ошибки синхронизации учетных записей, рекомендуется отключить парольные политики ОС Windows. Данная функциональная возможность реализована в СЗИ Dallas Lock 8.0 независимо от механизмов ОС.

5.2.7 Регистрация доменных пользователей в ДБ

Очень часто компьютеры с установленной системой защиты объединены в локальную сеть, физическую и логическую структуру которой объединяет служба каталогов Microsoft Active Directory. Это позволяет централизованно администрировать все ресурсы, включая пользователей, файлы, периферийные устройства, доступ к службам, сетевым ресурсам, веб-узлам, базам данных и прочие. Группа компьютеров, совместно использующих общую базу данных каталога, образует домен.

Таким образом, с учетными записями пользователей, созданными в домене, можно проводить операции на рабочих станциях, зарегистрированных в этом домене, и в том числе регистрировать в ЕЦУ Dallas Lock.

Примечание. Для безошибочной работы регистрации доменных учетных записей в ЕЦУ Dallas Lock, установленном в ОС семейства Linux, необходимо на DNS-серверах, к которым обращается АРМ с ЕЦУ Dallas Lock, корректно настроить обратную зону (то есть должна присутствовать обратная зона, содержащая PTR-записи всех контроллеров AD).

Для проверки данного требования АИБ нужно на АРМ с ЕЦУ Dallas Lock выполнить следующие команды:

- «*nslookup <имя_домена>*» — убедиться, что выводится IP-адрес;
- «*nslookup <полученный ip-адрес>*» — убедиться, что выводится корректное FQDN-имя контроллера AD.

Примечание. При регистрации в ЕЦУ Dallas Lock доменных учетных записей Active Directory необходимо, чтобы время сервера ЕЦУ Dallas Lock было синхронизировано с временем контроллера домена Active Directory.

Для регистрации в Домене безопасности ЕЦУ Dallas Lock доменных пользователей в качестве глобальных, необходимо выполнить следующее:

1. Убедиться, что Домен безопасности ЕЦУ Dallas Lock принадлежит домену Active Directory (см. «Принадлежность к домену Active Directory»).
2. Получить список доменных пользователей. Для этого при создании пользователя в выпадающем списке поля «Источник» необходимо выбрать имя домена и нажать кнопку поиска (рис. 73).

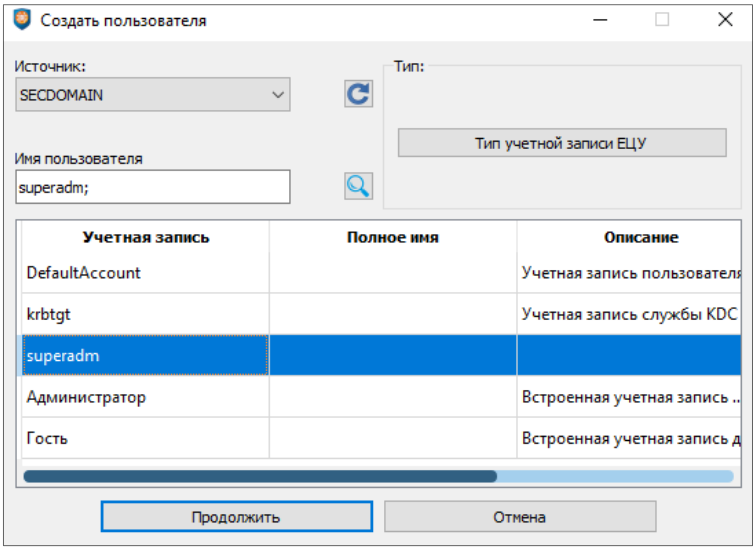

Рис. 73. Заполнение учетной записи пользователя

Примечание. При регистрации доменной учетной записи необходимо нажать на кнопку «Обновить» для ввода авторизационных данных AD, далее выбрать в поле «Источник» имя домена AD и произвести поиск учетных записей выбранного домена.

Для получения списка учетных записей домена необходимо дополнительно ввести авторизационные данные администратора домена в появившемся окне (рис. 74).

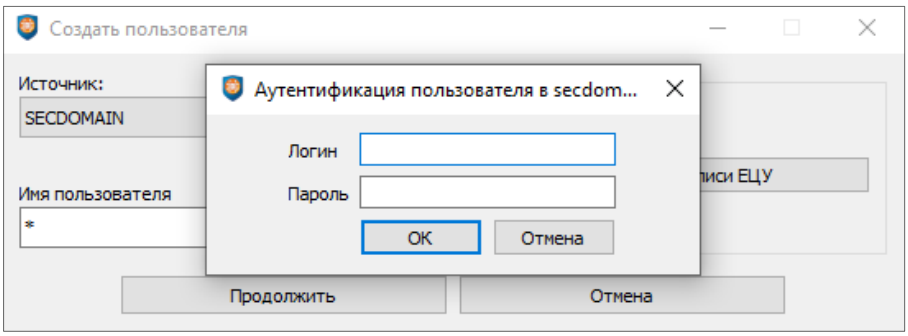

Рис. 74. Авторизационные данные администратора домена AD

3. Выбрать учетную запись пользователя и нажать «Продолжить». Можно выделить несколько учетных записей, имеющихся в ОС, и зарегистрировать их одновременно.

В ДБ автоматически сформируется учетная запись пользователя с тем же именем домена, логином и паролем. Учетная запись пользователя в списке учетных записей будет иметь вид: «имя домена/имя пользователя».

Имеющихся доменных пользователей можно зарегистрировать в ЕЦУ Dallas Lock, но их нельзя создать средствами Консоли ЕЦУ. Если нужен новый доменный пользователь, его придется создать средствами администрирования на контроллере домена и только после этого зарегистрировать в ЕЦУ Dallas Lock.

Список доменных пользователей и групп кэшируется Консолью ЕЦУ в своей памяти. Поэтому, если новый пользователь создан на контроллере домена, он может появиться в списке Консоли ЕЦУ не сразу. Необходимо обновить список с помощью кнопки «Обновить» .

Примечание. Процесс получения списка доменных пользователей может быть достаточно длительным. Во время этого процесса возможно появление диалогового окна с просьбой ввести идентификационную информацию администратора.

С зарегистрированными в ЕЦУ Dallas Lock доменными пользователями можно проводить любые операции по реализации политик безопасности, однако нельзя менять пароль средствами ЕЦУ Dallas Lock. При попытке изменить пароль будет выведено предупреждение.

Примечание. Аппаратный идентификатор может быть назначен только для отдельно взятой доменной учетной записи зарегистрированной в ДБ без маски.

Также средствами ЕЦУ Dallas Lock невозможно изменить список групп, в которые входит доменный пользователь.

5.2.8 Регистрация доменных пользователей по маске в ДБ

В системе ЕЦУ Dallas Lock реализован механизм регистрации доменных учетных записей пользователей системы с использованием масок по символу «*». В этом контексте символ «*» имеет значение «все». Учетная запись «Имя_домена*» означает всех пользователей данного домена.

По такой маске возможна регистрация только доменных учетных записей, для локальных это невозможно, и каждая запись должна быть создана отдельно.

Механизм регистрации доменных учетных записей системы с использованием масок позволяет привести систему входа к строгому виду.

Для разрешения входа в систему всех доменных пользователей (в том числе пользователей доверенных доменов) в ЕЦУ Dallas Lock должна быть зарегистрирована учетная запись «**».

Для этого необходимо при создании нового пользователя указать источник «*» и нажать кнопку «Продолжить».

Примечание. Учетная запись «**» создается на модуле СЗИ Dallas Lock 8.0 на ПК, являющимся членом домена Windows, при установке с конфигурацией по умолчанию.

Каждая учетная запись может быть в состоянии «вход разрешен» и «вход запрещен». Чтобы запретить вход под соответствующей учетной записью необходимо, чтобы в свойствах учетной записи на вкладке «Запрет работы», для параметра «Учетная запись отключена» было выбрано значение «Да» (рис. 75).

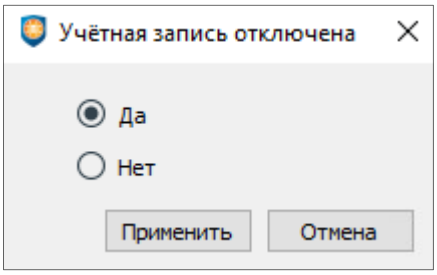

Рис. 75. Учетная запись отключена

Если для существующей учетной записи вида «**» запретить вход в систему и одновременно разрешить вход для учетных записей типа «ZCB*», то в систему защиты пользователи доменов входить не смогут, но смогут входить только пользователи домена ZCB. Другой пример: если запретить вход в систему для записи «ZCB*» и разрешить для «ZCB\admin1», «ZCB\admin2», то это будет означать, что из домена ZCB на защищенный системой компьютер смогут входить только пользователи admin1 и admin2.

Таким образом, систему проверки пользователей можно легко привести к «строгой» системе, достаточно отключить учетную запись «**» и, далее, в явном виде регистрировать учетные записи необходимых доменных пользователей.

Примечание. Если в ЕЦУ зарегистрирована доменная учетная запись «**» или «Имя_домена*», то назначать параметры пользователей можно как для учетной записи «**» (или «Имя_домена*»), так и для каждой индивидуальной учетной записи домена, выбрав ее из списка.

5.2.9 Создание групп пользователей ДБ

Группы предназначены для объединения пользователей, у которых права безопасности могут быть схожими. Такое объединение может упростить работу администратора при выполнении настроек Домена безопасности.

Группы безопасности упрощают управление доступом к ресурсам. Можно добавлять пользователей к группам безопасности, а затем предоставлять этим группам права доступа, и удалять их оттуда в соответствии с потребностями этих пользователей.

Для просмотра и редактирования списка групп системы безопасности в Консоли ЕЦУ необходимо выбрать вкладку «Пользователи и группы» → «Группы». В окне Консоли ЕЦУ автоматически появляется ряд предварительно сконфигурированных групп в локальной ОС, в которые можно включать глобальных пользователей (рис. 76).

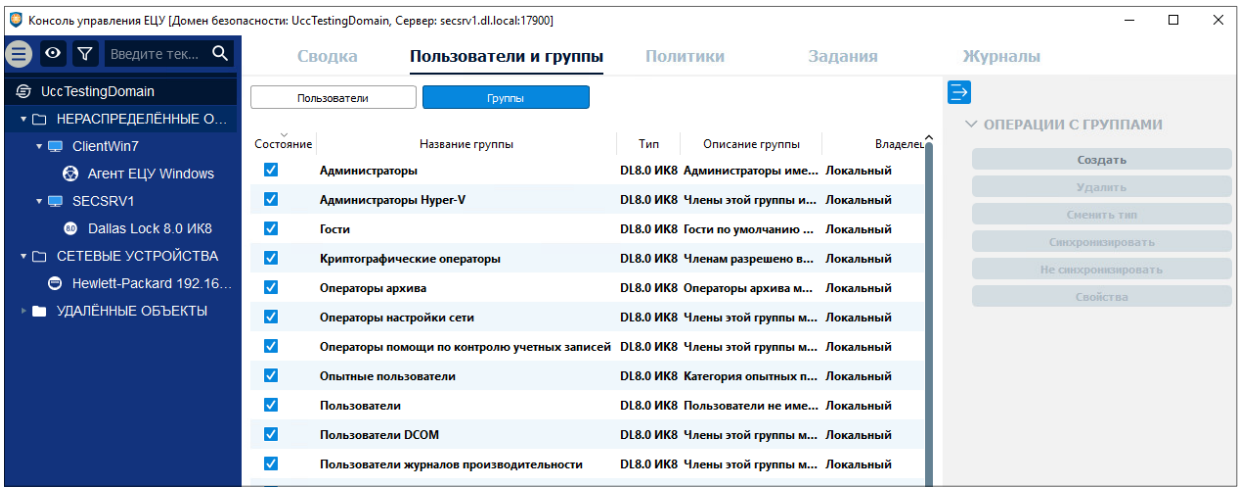

Рис. 76. Группы пользователей

Вновь созданные с помощью ЕЦУ Dallas Lock глобальные группы автоматически создадутся и в подчиненных модулях после синхронизации. Удаленные глобальные группы пропадут из списков групп на модулях после синхронизации.

Примечание. В данные глобальные группы, сформированные в ЕЦУ Dallas Lock, можно добавлять только глобальных и модульных пользователей. Доменные пользователи добавляются в группы на контроллере домена. Также при настройке политик безопасности при добавлении групп появляется возможность выбора глобальных и модульных групп.

Для создания глобальных групп с помощью Консоли ЕЦУ необходимо:

1. Открыть вкладку «Пользователи и группы» в Консоли ЕЦУ.
2. Выбрать категорию «Группы».
3. На панели инструментов в операциях с группами нажать кнопку «Создать» или выбрать соответствующую из контекстного меню, нажав правую кнопку мыши.
4. На экране появится окно создания группы (рис. 77).

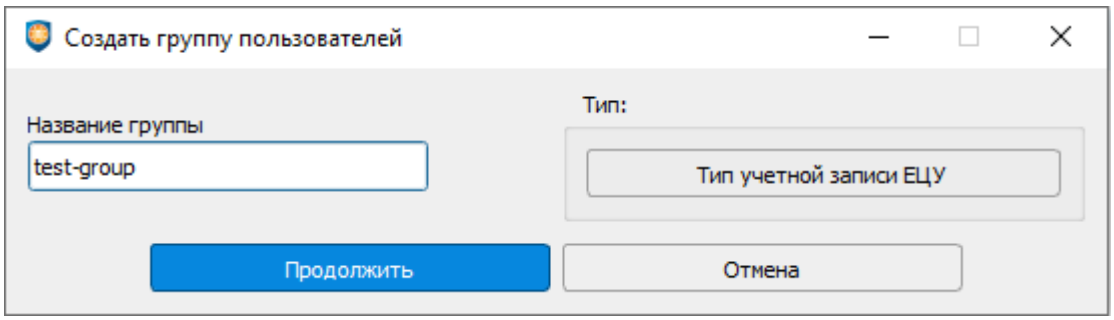

Рис. 77. Создание глобальной группы

5. В поле «Название группы» необходимо ввести название регистрируемой группы.

Примечание. При наличии в Домене безопасности ПК, работающих под ОС Linux, не рекомендуется использовать кириллические символы в именах пользователей и групп в связи с отсутствием гарантии обеспечения корректной работы.

Примечание. Название глобальной группы считается уникальным в рамках одного Домена безопасности.

6. Выбрать «Тип учетной записи ЕЦУ» в зависимости от того, для модулей какого типа применяется

данная группа пользователей.

Изменить тип учетной записи можно, используя кнопку «Сменить тип» на панели инструментов «Операции с группами» или выбрав данное действие из контекстного меню.

7. После нажатия «Продолжить» появится окно для редактирования параметров группы пользователей (см. «Параметры групп пользователей»).

Изменить параметры группы можно, используя кнопку «Свойства» на панели инструментов «Операции с группами» или выбрав данное действие из контекстного меню.

5.2.10 Удаление групп пользователей ДБ

Для удаления глобальной группы из Домена безопасности необходимо выделить ее название в списке на уровне «Владельца», нажать кнопку «Удалить» или выбрать соответствующее действие из контекстного меню. Группа пользователей будет удалена с модулей после синхронизации с ЕЦУ Dallas Lock.

5.3 Ролевая модель учетных записей ДБ

Настройки по правам администрирования в ДБ осуществляются в рабочей области для вкладки «Пользователи и группы» в категории «Пользователи» в поле «Роль администрирования» (рис. 78).

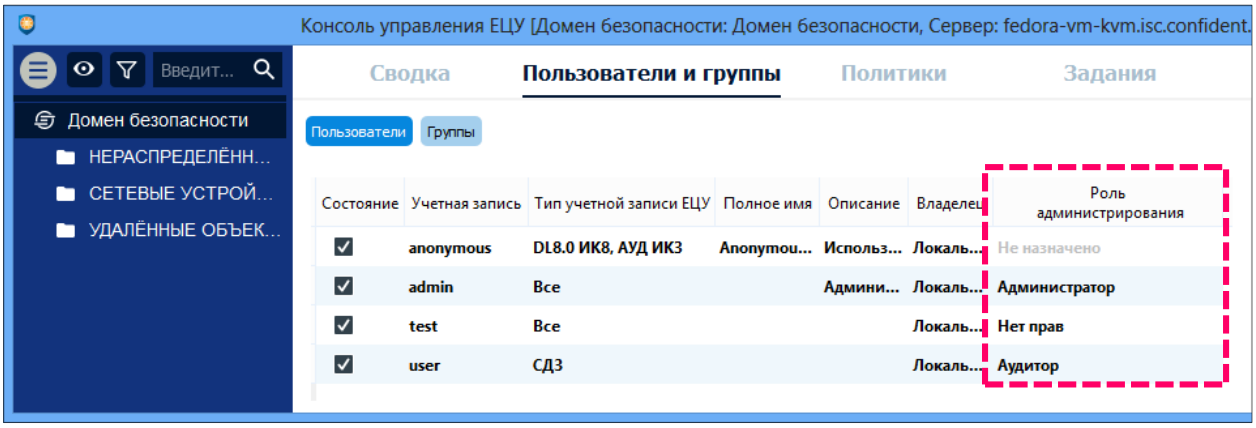

Рис. 78. Роль администрирования

Роль представляет собой совокупность привилегий — полномочий по выполнению действий в части администрирования ДБ.

На основе групп привилегий в ЕЦУ Dallas Lock сформированы следующие роли администрирования:

- «Администратор» — максимальные привилегии на управление ДБ или его частью, в зависимости от уровня назначения роли;
- «Аудитор» — в зависимости от уровня назначения роли, Аудитор может иметь определенный набор привилегий на просмотр информации о ДБ или его части:
  - состояние защищенности;
  - просмотр списка пользователей, их параметров и назначенных ролей;
  - просмотр значений политик безопасности;
  - чтение журналов.
- «Нет прав» — пользователи без прав на администрирование и аудит ДБ;
- «Не назначено».

По умолчанию новым пользователям назначается роль «Не назначено».

У назначения на роль есть параметр «Владелец» — уровень на котором была назначена данная роль. Если на уровне «Владельца» учетной записи пользователя определена роль «Не назначено», то по умолчанию такой пользователь не будет обладать привилегиями на администрирование ДБ на данном уровне, при этом, если на подчиненных узлах:

- роль не переопределена (значение «Не назначено»), то пользователь будет наследовать роль с более высокого уровня дерева ДБ;
- роль пользователя переопределена (значение отличное от «Не назначено»),

то пользователь будет иметь на этом подчиненном уровне и уровнях ниже этого привилегии в соответствии с назначенной ролью.

Внимание! Следует внимательно относиться к созданию и удалению назначений ролей пользователей на администрирование ДБ. Если на каком-либо из уровней Домена безопасности не останется ни одного пользователя с ролью «Администратор», доступ к настройкам на этом уровне будет органичен до момента появления пользователя с достаточным набором привилегий.

5.4 Политики ДБ

После установки системы управления, необходимо произвести ее настройку. Под настройкой системы понимается установка значений политик Домена безопасности, удовлетворяющих политикам безопасности организации.

Вкладка «Политики» позволяет редактировать параметры безопасности на уровне всего ДБ, после синхронизации на всех подчиненных объектах в ДБ применяются установленные настройки (рис. 79).

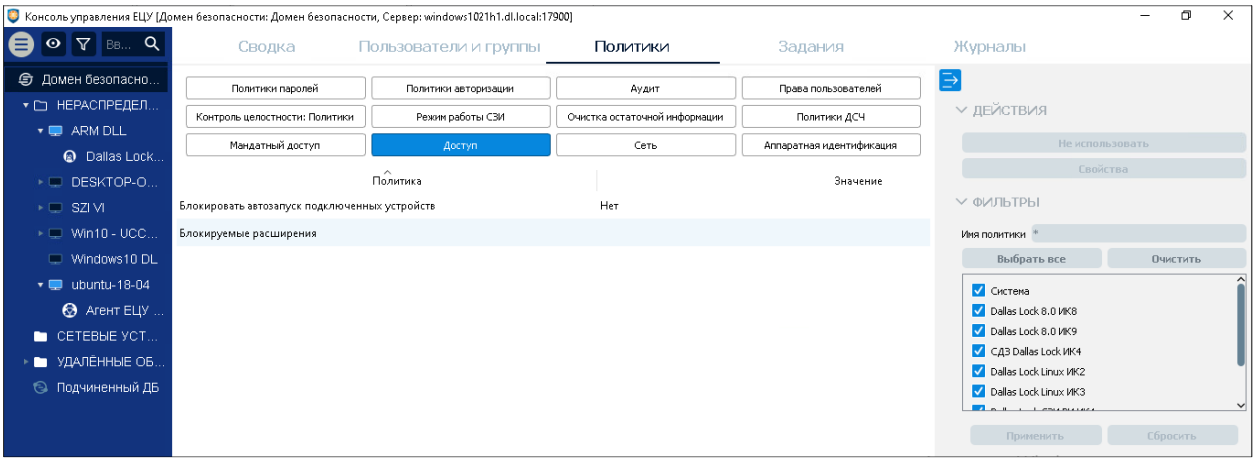

Рис. 79. Вкладка Политики ДБ

Открыть редактор политики можно следующими способами:

- дважды щелкнуть левой кнопкой мыши по изменяемой политике;
- вызвать контекстное меню изменяемой политики и выбрать «Свойства»;
- нажать кнопку «Свойства» на панели «Действия».

5.4.1 Настройка парольных политик

Настройки, касающиеся значений парольных политик, регулируются в категории «Политики паролей» на вкладке «Политики».

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке политик паролей.

Примечание. Следует учесть, что в ОС Windows есть свои, независимые политики сложности пароля. И в некоторых случаях пароль может удовлетворять политикам Dallas Lock, но не удовлетворять политикам Windows. В данном случае такой пароль установить не удастся.

Таблица 7. Парольные политики

Максимальный срок действия пароля
Политика устанавливает максимальный срок действия пароля пользователей. По истечении срока действия пользователю автоматически будет предложено сменить пароль. Не распространяется на учетные записи пользователей с установленным атрибутом «Бессрочный пароль».

Политика принимает значения от 1 дня до 25 недель (180 дней) и «Не используется» — максимальный срок действия пароля не установлен. По умолчанию политика имеет значение «6 нед. 0 дн.».

Политика применяется на:

- службу ЕЦУ;
- модулях:
  - СЗИ Dallas Lock 8.0-K/C;
  - СДЗ Dallas Lock;
  - СЗИ ВИ Dallas Lock;
  - СЗИ НСД Dallas Lock Linux.

Минимальный срок действия пароля

Данной политикой устанавливается минимальный срок действия пароля для всех пользователей. До истечения установленного срока СЗИ не позволит пользователю сменить свой пароль.

Политика принимает значения от 1 дня до 30 дней и «Не используется». При выборе значения «Не используется» минимальный срок действия пароля не ограничен.

По умолчанию политика имеет значение «10 дн.».

Заданный параметр не является приоритетным. Он действует только если для пользователя не указано никаких иных значений срока действия пароля.

Минимальный срок действия пароля для каждого конкретного пользователя определяется по следующей схеме:

- Если администратор установил для конкретного пользователя принудительную смену пароля при следующем входе на компьютер, то в процессе очередной загрузки компьютера под этим пользователем система защиты обязательно потребует сменить пароль (наивысший приоритет).
- Если отсутствует требование смены пароля при следующем входе, то СЗИ не позволит сменить пароль если не истек установленный минимальный срок действия пароля. При этом на экране отобразится сообщение «Пароль не может быть изменен».
- Флаг в поле «Пароль без ограничения срока действия», установленный в настройках учетной записи в категории «Пароли», не даст возможности сменить пароль до окончания установленного минимального срока действия пароля.

Примечание. Если нарушено соотношение максимального и минимального сроков действия пароля (минимальный срок действия пароля больше максимального), то СЗИ проигнорирует значение минимального срока действия пароля.

Политика применяется на:

- службу ЕЦУ;
- модулях:
  - СЗИ Dallas Lock 8.0-K/C;
  - СДЗ Dallas Lock;
  - СЗИ ВИ Dallas Lock;
  - СЗИ НСД Dallas Lock Linux.

Минимальная длина пароля

Данной политикой устанавливается ограничение на минимальную длину пароля. При регистрации нового пользователя и при изменении старого пароля система контролирует длину вводимого пароля. Если число символов в пароле меньше установленного значения, то на экране появится предупреждение «Ввод пароля: введен слишком короткий пароль».

Политика принимает значения от 1 до 14 символов и «Не используется». По умолчанию политика имеет значение «Не используется». При выборе значения «Не используется» устанавливаемый пароль может иметь пустое значение.

Действие политики распространяется на значения паролей, PIN-кодов и ключей.

Следует иметь в виду, что если в процессе работы изменено значение длины пароля (например, увеличено), то у зарегистрированных пользователей она остается прежней до первой смены значения.

Политика применяется на:
- службу ЕЦУ;
- модулях:
  - СЗИ Dallas Lock 8.0-K/C;
  - СДЗ Dallas Lock;
  - СЗИ НСД Dallas Lock Linux;
  - СЗИ ВИ Dallas Lock.

Напоминать о смене пароля за

С помощью данного параметра система защиты позволит напоминать пользователю о том, что через определенное количество дней необходимо сменить пароль.

Политика принимает значения от 1 до 15 дней и «Не используется». По умолчанию политика имеет значение «3 дн.». Если выбрано значение «Не используется», то напоминаний о необходимости смены пароля не будет.

Напоминание о предстоящей смене пароля будет появляться на экране при загрузке СЗИ данным пользователем, начиная с того момента, когда до смены пароля (фактически до истечения максимального времени действия пароля) осталось количество дней, равное установленному значению для этой политики.

Примечание. Параметры, устанавливающие срок действия пароля, действуют независимо от аналогичных параметров ОС Windows. В Windows действуют свои политики безопасности, которые также могут потребовать смены пароля независимо от СЗИ Dallas Lock 8.0.

В СЗИ Dallas Lock 8.0 и ОС Windows совпадают следующие парольные политики:
- максимальный срок действия пароля;
- минимальная длина пароля;
- минимальный срок действия пароля;
- пароль должен отвечать требованиям сложности.

Чтобы не возникало конфликта парольных политик ОС Windows и СЗИ Dallas Lock 8.0, нужно сделать данные политики идентичными в ОС и СЗИ, либо отключить политики в ОС.

Политика применяется на:
- службу ЕЦУ;
- модулях:
  - СЗИ Dallas Lock 8.0-K/C;
  - СДЗ Dallas Lock;
  - СЗИ ВИ Dallas Lock;
  - СЗИ НСД Dallas Lock Linux.

Необходимо изменение пароля не меньше, чем в

Данной политикой задается количество символов, на которое, как минимум, должен отличаться новый пароль от старого при его смене.

Политика принимает значения от 1 до 10 символов и «Не используется». По умолчанию политика имеет значение «Не используется».

Примечание. Если данная политика включена для ОС Windows (значение, отличное от «Не используется»), то при смене пароля через комбинацию клавиш «Ctrl + Alt + Del», новый пароль должен отличаться от старого не менее, чем на указанное количество символов. Сверка старого и нового пароля осуществляется посимвольно.

При смене пароля через оболочку администратора СЗИ Dallas Lock 8.0 данный параметр не учитывается.

Пример. У пользователя имеется пароль «password1», если в выше описанной опции количество символов указано 2, то при смене пароля «password1» на «password**2**» выведется сообщение «Пароль должен сильнее отличаться от предыдущего». Правильной будет смена пароля с «password1» на «**P**assword**2**».

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-K/C;
- СДЗ Dallas Lock;
- СЗИ ВИ Dallas Lock.

Необходимо наличие спецсимволов

Если данная политика включена (значение «Да»), то при создании пароля в нем должны присутствовать специальные символы из следующего списка: "`", "~", "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "_", "-", "+", "{", "}", "[", "]", "\", "|", ":", ";", """, "'", "<", ">", ",", ".", "?", "/".

По умолчанию политика имеет значение «Нет».

Действие политики распространяется на значения паролей, PIN-кодов и ключей.

Пример. У пользователя имеется пароль «password1», если выше описанная опция активирована, то при смене пароля на «password**2**» выведется сообщение «В пароле должны содержаться спецсимволы». Правильной будет смена пароля с «password1» на «password#».

Политика применяется на:

- службу ЕЦУ;
- модулях:
  - СЗИ Dallas Lock 8.0-K/C;
  - СДЗ Dallas Lock;
  - СЗИ НСД Dallas Lock Linux;
  - СЗИ ВИ Dallas Lock.

Необходимо наличие строчных и прописных букв

Если данная политика включена (значение «Да»), то при создании пароля в нем должны присутствовать строчные и прописные буквы.

По умолчанию политика имеет значение «Нет».

Действие политики распространяется на значения паролей, PIN-кодов и ключей.

Пример. У пользователя имеется пароль «password1», если выше описанная опция активирована, то при смене пароля на «pacsword1» выведется сообщение «В пароле должны содержаться и строчные, и прописные буквы». Правильной будет смена пароля с «password1» на «pa**C**sword1».

Политика применяется на:

- службу ЕЦУ;
- модулях:
  - СЗИ Dallas Lock 8.0-K/C;
  - СДЗ Dallas Lock;
  - СЗИ НСД Dallas Lock Linux;
  - СЗИ ВИ Dallas Lock.

Необходимо наличие цифр

Если данная политика включена (значение «Да»), то при создании пароля в нем должны присутствовать цифры.

По умолчанию политика имеет значение «Нет».

Действие политики распространяется на значения паролей, PIN-кодов и ключей.

Пример. У пользователя имеется пароль «password», если описанная выше опция активирована, то при попытке смены пароля на «password**d**» выведется сообщение «В пароле должны содержаться цифры». Правильной будет смена пароля с «password» на «password**12**».

Политика применяется на:

- службу ЕЦУ;
- модулях:
  - СЗИ Dallas Lock 8.0-K/C;
  - СДЗ Dallas Lock;
  - СЗИ НСД Dallas Lock Linux;
  - СЗИ ВИ Dallas Lock.

Необходимо отсутствие цифры в первом и последнем символах

Данной политикой устанавливается ограничение на использование цифр в первом и последнем символах пароля.

Если данная политика включена (значение «Да»), то при создании пароля в нем не должно содержаться цифр в первом и последнем символах.

По умолчанию политика имеет значение «Нет».

Действие политики распространяется на значения паролей, PIN-кодов и ключей.

Пример. У пользователя имеется пароль «password», если описанная выше опция активирована, то при попытке смены пароля на «password**1**», «**1**password» или «**1**password**1**» выведется сообщение «Необходимо отсутствие цифры в первом и последнем символах». Правильной будет смена пароля с «password» на «password**d**».

Политика применяется на:

- службу ЕЦУ;
- модулях:
  - СЗИ Dallas Lock 8.0-K/C;
  - СДЗ Dallas Lock;
  - СЗИ ВИ Dallas Lock.

(ВИ) vSphere: Минимальная длина пароля

Данной политикой устанавливается ограничение на минимальную длину пароля для гипервизоров vSphere.

Политика принимает значения от 1 до 30 символов. По умолчанию значение: 1 символ.

При регистрации новой учетной записи и при изменении старого пароля в ЦУ СЗИ ВИ Dallas Lock контролируется длина вводимого пароля. Если число символов в пароле меньше установленного значения, то на экране появится предупреждение «Ввод пароля: введен слишком короткий пароль».

Следует иметь в виду, что если в процессе работы изменить значение длины пароля (например, увеличить), то у зарегистрированных учетных записей она останется прежней до первой смены пароля.

Политика применяется на модулях СЗИ ВИ Dallas Lock.

(ВИ) Гипервизоры: Минимальное количество классов символов

Данная политика определяет количество классов символов (буквы в верхнем и нижнем регистре, цифры и специальные символы), которые должны присутствовать в пароле, для учетной записи Сервера виртуализации в ЦУ СЗИ ВИ Dallas Lock.

Политика принимает значения от 1 до 4 и «Не используется». Значение «1» означает, что пароль может содержать любые символы, например, только цифры. По умолчанию значение политики: 1 символ.

Политика применяется на модулях СЗИ ВИ Dallas Lock.

(ВИ) Сервер виртуализации: Количество предыдущих паролей, которые пользователь не может использовать

Данной политикой устанавливается количество предыдущих паролей каждого пользователя, которые не могут быть выбраны ими при смене пароля, для учетной записи Сервера виртуализации в ЦУ СЗИ ВИ Dallas Lock.

Политика принимает значения от 1 до 10. Например, значение «5» запрещает использовать пять предыдущих паролей для выбранного пользователя. По умолчанию значение политики: «1».

Политика применяется на модулях СЗИ ВИ Dallas Lock.

(ВИ) Сервер виртуализации: Максимальная длина пароля

Данной политикой устанавливается ограничение на максимальную длину пароля для учетной записи Сервера виртуализации в ЦУ СЗИ ВИ Dallas Lock.

Политика принимает значения от 1 до 14 символов и «Не используется». По умолчанию значение данной политики: «Не используется».

Политика применяется на модулях СЗИ ВИ Dallas Lock.

(ВИ) Сервер виртуализации: Максимальное допустимое количество одинаковых символов, стоящих рядом
Данной политикой устанавливается максимально допустимое количество одинаковых символов, которые могут присутствовать при задании пароля, для учетной записи Сервера виртуализации в ЦУ СЗИ ВИ Dallas Lock. Политика принимает значения от 1 до 5 символов и «Не используется». По умолчанию значение данной политики: «Не используется». Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Сервер виртуализации: Минимальное количество прописных букв
Данной политикой устанавливается минимальное количество прописных (больших) букв, которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации в ЦУ СЗИ ВИ Dallas Lock. Политика принимает значения от 1 до 9 символов и «Не используется». По умолчанию значение данной политики: «Не используется». Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Сервер виртуализации: Минимальное количество символов алфавита
Данной политикой устанавливается минимальное количество символов алфавита, которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации в ЦУ СЗИ ВИ Dallas Lock. Политика принимает значения от 1 до 15 символов и «Не используется». По умолчанию значение данной политики: «Не используется». Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Сервер виртуализации: Минимальное количество специальных символов
Данной политикой устанавливается минимальное количество специальных символов ("`", "~", "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "_", "-", "+", "{", "}", "[", "]", "\", "|", ":", ";", """, "'", "<", ">", ",", ".", "?", "/"), которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации в ЦУ СЗИ ВИ Dallas Lock. Политика принимает значения от 1 до 9 символов и «Не используется». По умолчанию значение данной политики: «Не используется». Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Сервер виртуализации: Минимальное количество строчных букв
Данной политикой устанавливается минимальное количество строчных (маленьких) букв, которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации в ЦУ СЗИ ВИ Dallas Lock. Политика принимает значения от 1 до 9 символов и «Не используется». По умолчанию значение данной политики: «Не используется». Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Сервер виртуализации: Минимальное количество числовых символов
Данной политикой устанавливается минимальное количество числовых символов, которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации в ЦУ СЗИ ВИ Dallas Lock. Политика принимает значения от 1 до 9 символов и «Не используется». По умолчанию значение данной политики: «Не используется». Политика применяется на модулях СЗИ ВИ Dallas Lock.

5.4.2 Настройка политик авторизации

На вкладке «Политики» в категории «Политики авторизации» настраиваются параметры, касающиеся входа в систему.

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке политик авторизации.

Таблица 8. Политики авторизации

Автоматический выбор аппаратного идентификатора при авторизации
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Включение данной политики позволит автоматически выбрать подключенный аппаратный идентификатор при авторизации. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Автоматическое блокирование неактивных учетных записей
Политика принимает значения от 1 до 90 дней и «Не используется». По умолчанию значение данной политики: «Не используется». Данная политика позволяет настроить и выполнить автоматическую блокировку неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования. При активации данной политики на ЕЦУ выполняется блокировка неактивной учетной записи пользователей на отдельном модуле СЗИ Dallas Lock 8.0-K/C. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Блокировать компьютер в случае ввода неправильных паролей
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет настроить блокирование компьютера в случае ввода пользователем неправильных паролей. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Блокировать компьютер при отключении аппаратного идентификатора
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». При включении данной политики всем пользователям, которым назначен аппаратный идентификатор, работа на данном ПК при отключении идентификатора будет заблокирована. Политика не распространяется на идентификаторы, предъявляемые по касанию. Политика применяется на модулях: •СЗИ Dallas Lock 8.0-K/C; •СЗИ ВИ Dallas Lock.
Блокировать подключение незарегистрированных накопителей USB-Flash
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет блокировать незарегистрированные USB-Flash накопители. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Блокировать файл-диски при отключении аппаратного идентификатора
Возможное значение политики: «Да/Нет». По умолчанию значение политики: «Нет». Если при создании файл-диска помимо пароля используется аппаратный идентификатор, то при отключении идентификатора от ПК, файл-диск также будет отключен. Стоит учитывать, что при изменении настроек аппаратного идентификатора необходимо начать новый сеанс работы пользователя для выполнения корректной блокировки. Политика не распространяется на идентификаторы, предъявляемые по касанию. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Ввести в домен Active Directory
Политика позволяет ввести наименование домена, для которого настроено взаимодействие с модулями СЗИ НСД Dallas Lock Linux. По умолчанию значение данной политики: «Не используется».

Политика применяется на модулях СЗИ НСД Dallas Lock Linux.

Время бездействия, после которого будет заблокирован сеанс доступа

Данная политика определяет время бездействия пользователя, по прошествии которого сеанс доступа данного пользователя будет заблокирован.

Возможно установить время бездействия от 1 минуты до 5 часов. По умолчанию значение данного параметра: «Не используется».

Примечание. Если данная политика используется для ОС Linux (значение, отличное от «Не используется»), следует учитывать, что блокировка графической сессии также доступна к изменению с помощью стандартных утилит настройки ОС. Такое изменение не отобразится в оболочке администрирования СЗИ НСД Dallas Lock Linux и ЕЦУ Dallas Lock.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СЗИ НСД Dallas Lock Linux.

Время блокировки учетной записи в случае ввода неправильных паролей

Данная политика позволяет установить, сколько времени учетная запись будет заблокирована после того, как пользователь ввел неверный пароль больше допустимого числа раз. В этот временной интервал пользователь не сможет загрузить компьютер и ОС, даже при верном вводе пароля.

По истечении указанного времени учетная запись автоматически разблокируется, и пользователь снова получит возможность ввести пароль. Сбросить автоматическую блокировку досрочно может только администратор безопасности или пользователь, обладающий правом редактирования учетных записей.

Возможное значение параметра: от 1 минуты до 5 часов и «Не используется». Если выбрано значение «Не используется», то разблокировать учетную запись может только администратор безопасности. По умолчанию значение данной политики: «Не используется».

Политика применяется на:

- службу ЕЦУ;
- модулях:
  - СЗИ Dallas Lock 8.0-К/С;
  - СДЗ Dallas Lock;
  - СЗИ ВИ Dallas Lock.

Время ожидания авторизации пользователя

Политика принимает значения от 1 до 10 минут и «Не используется» — время ожидания ввода авторизационных данных не ограничено. По умолчанию значение данной политики: 2 минуты.

Значение данной политики определяет время, отводимое на ввод пользователем авторизационных данных (от начала набора данных до нажатия кнопки «ОК»). Если пользователь не успел завершить ввод авторизационных данных, то введенные данные очищаются.

Политика применяется на модулях СДЗ Dallas Lock.

Запретить использование парольного интерфейса входа

Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет».

При использовании смарт-карт для авторизации в ОС возможно отключить интерфейс входа по имени пользователя и паролю, включением данной политики (значение «Да»).

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СЗИ ВИ Dallas Lock.

Запретить повторное использование имени пользователя в течение

Политика принимает значения от 1 года до 2 лет и «Не используется». По умолчанию значение данного параметра: «Не используется».

Включение данной политики устанавливает запрет на повторное использование имени пользователя при регистрации новой учетной записи.

Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.

Запретить смену пользователя без перезагрузки

Возможное значение политики: «Вкл./Выкл.». По умолчанию значение — «Выкл.».

Данная политика позволяет предотвратить теоретическую возможность извлечения какой-либо информации из оперативной памяти ПК, оставшуюся там после завершения сеанса работы другого пользователя.

При включении данной политики (значение «Вкл.»), активируется запрет на осуществление смены пользователя без перезагрузки компьютера. При включенном значении политики при выборе пункта «Завершение работы» в окне «Завершение работы Windows», компьютер автоматически уйдет в перезагрузку.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СЗИ ВИ Dallas Lock.

Исключения для контроля приложений, печати и изолированных процессов

Данная политика позволяет настроить список файлов, для которых не производится контроль приложений, печати и изолированных процессов.

Список содержит имена и названия исключений, перечисленные через «;». Имена могут не содержать пути, либо включать в себя последнюю часть пути или полный путь (этот вариант наиболее безопасен). Формат значения параметра: «имя (путь), исключение;».

Список исключений:

- all – для всех компонентов;
- ips – для СОВ;
- print – для печати;
- clipboard – для изолированных процессов.

Если в любом элементе списка в качестве имени указано «*» — настройка будет активной для всех исключений.

По умолчанию значение — Не используется.

Использовать авторизационную информацию от СДЗ Dallas Lock

Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет».

При включении данной политики (значение «Да») автоматически используется авторизационная информация от СДЗ Dallas Lock. Политика применяется только при установленной аппаратной плате. Для работы политики необходимо в ОС установить драйвер для СДЗ.

Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.

Использовать аппаратный идентификатор по умолчанию

Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет».

Значение «Да» данной политики включает использование аппаратного идентификатора по умолчанию.

Политика применяется на модулях СДЗ Dallas Lock.

Количество попыток неверного ввода пароля

Значение, установленное для этой политики, регламентирует, сколько раз пользователь имеет право ошибаться при вводе пароля.

Если число ошибок больше допустимого, учетная запись будет заблокирована, и пользователь не сможет загрузить компьютер и ОС.

Возможное значение параметра: от 1 до 10 и «Не используется» — пользователь может вводить неверный пароль неограниченное число раз. По умолчанию значение данной политики: «8».

Политика применяется на:

- службу ЕЦУ;

- модулях:
  - СЗИ Dallas Lock 8.0-К/С;
  - СЗИ НСД Dallas Lock Linux;
  - СДЗ Dallas Lock;
  - СЗИ ВИ Dallas Lock.

Максимальное количество сессий

Данная политика устанавливает максимальное количество активных сессий на данном ПК. Возможные значения от 1 до 20 сессий и «Не используется» — означает, что параметр будет отключен. По умолчанию установлено значение «3».

Политика применяется на модулях СЗИ НСД Dallas Lock Linux.

Отображать имя последнего вошедшего пользователя

Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Да».

В значении «Да» в окне авторизации поле «Пользователь» заполняется именем учетной записи пользователя, осуществившего последний успешный вход. При значении «Нет» поле остается пустым.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СДЗ Dallas Lock;
- СЗИ ВИ Dallas Lock.

Отображать информацию о последнем успешном входе

Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет».

При включении данной политики для модуля СЗИ Dallas Lock 8.0 и СЗИ ВИ Dallas Lock (значение «Да») после загрузки ОС в области уведомлений Windows на панели задач будет появляться сообщение с информацией о дате последнего входа пользователя на данный компьютер, типе входа: сетевой, локальный, терминальный, неуспешных попытках входа и состоянии параметров учетной записи пользователя.

При включении данной политики для модуля СДЗ Dallas Lock (значение «Да») при очередном входе пользователя во время выполнения процедуры контроля целостности объектов отображается дата и время последнего успешного входа данного пользователя.

При значении «Нет» — информация не отображается.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СДЗ Dallas Lock;
- СЗИ ВИ Dallas Lock.

Разрешить авторизацию всем пользователям домена

Возможное значение политики: «Да/Нет». По умолчанию значение политики — «Нет».

При установлении значения «Да» учетные записи, зарегистрированные на контроллере домена Active Directory, для работы с которым настроено СЗИ НСД Dallas Lock Linux, пока не зарегистрированные в СЗИ НСД Dallas Lock Linux, будут регистрироваться в нем по мере прохождения процесса авторизации в СЗИ НСД Dallas Lock Linux.

Политика применяется на модулях СЗИ НСД Dallas Lock Linux.

Разрешить использование смарт-карт

Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет».

Включение данной политики разрешает использование микропроцессорных смарт-карт для авторизации в ОС Windows при работе ПК в корпоративном домене. Смарт-карты применяются вместе с личными идентификационными номерами (PIN-кодами).

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СЗИ ВИ Dallas Lock.

Считывать авторизационную информацию с аппаратного ключа
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Да». В значении «Да» во время авторизации информация автоматически считывается с аппаратного идентификатора. В значении «Нет» этого не происходит. Данная политика доступна только в базовом режиме работы модуля СДЗ Dallas Lock.
Текст сообщения при входе
В окне редактирования данной политики имеется возможность проставить флаг «Выводить сообщение при входе», ввести заголовок и текст предупреждения, которое будет отображаться пользователю до входа в ОС. Смысл данного текста должен предупреждать о реализации мер по обеспечению безопасности информации, и о необходимости соблюдения установленных правил обработки информации. Нажатие «ОК» пользователем будут означать подтверждение ознакомления. По умолчанию данная политика не используется. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
(ВИ) KVM: Блокировать протокол SSH
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Значение «Да» данной политики блокирует удаленный доступ к Серверу виртуализации по протоколу SSH. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) vCSA: Блокировать протокол SSH
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Политика контролирует удаленный доступ в vCSA по протоколу SSH. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) vCSA: Разрешить вход на Web-клиент vCSA Management Interface
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет настроить разрешение входа на Web-клиент VCSA Management Interface. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) vCSA: Разрешить локальный вход с консоли
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет настроить разрешение локального входа с консоли. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) vSphere: Запрет на работу через Web-клиент
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет заблокировать возможность подключения к Серверу виртуализации или гипервизору ESXi через Web-клиент VMware vSphere. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) KVM: Блокировать доступ к Cockpit Web Interface
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Да». Данная политика позволяет настроить разрешения входа на Web-клиент Cockpit Web Interface. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Гипервизоры: Блокировать протокол SSH

Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет».

Если разрешено использование ESXi Shell, то его можно запустить непосредственно на гипервизоре ESXi через DCUI или удаленно по SSH. Данная политика блокирует такую возможность.

Политика применяется на модулях СЗИ ВИ Dallas Lock.

(ВИ) Гипервизоры: Включить отправку системного журнала по SSL

Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет».

Данная политика позволяет включать шифрование информации, передаваемой по протоколу syslog.

Примечание. Данная политика работает только с добавленным корневым сертификатом СЗИ ВИ в доверенные корневые сертификаты VMware PSC.

Политика применяется на модулях СЗИ ВИ Dallas Lock.

(ВИ) Гипервизоры: Время, в течение которого допускается выполнить одну попытку ввода пароля

Политика принимает значения от 1 до 29 минут. По умолчанию значение: 1 минута.

Данная политика позволяет установить количество времени, в течение которого допускается выполнить одну попытку ввода пароля на модуле СЗИ ВИ Dallas Lock. Если произошла неудачная попытка ввода пароля, то выполнить новую попытку ввода пароля возможно будет только через указанный период времени.

Политика применяется на модулях СЗИ ВИ Dallas Lock.

(ВИ) Гипервизоры: Запретить возможность авторизации (Lockdown Mode)

Данная политика позволяет настроить запрет возможности авторизации. Возможно установить запрет при удаленном подключении, при прямом и удаленном подключении.

По умолчанию значение данной политики: «Не запрещать».

Политика применяется на модулях СЗИ ВИ Dallas Lock.

(ВИ) Гипервизоры: Количество попыток ввода нового пароля, удовлетворяющего текущим парольным политикам

Значение, установленное для этой политики, регламентирует, сколько раз пользователь имеет право ошибаться при вводе нового пароля.

Политика принимает значения от 1 до 10. По умолчанию значение данной политики: «1».

Политика применяется на модулях СЗИ ВИ Dallas Lock.

(ВИ) Гипервизоры: Период неиспользования

Политика принимает значения от 1 до 180 дней и «Не используется». По умолчанию значение данной политики: «Не используется».

Данной политикой устанавливается период времени, через который будут отключены неиспользуемые учетные записи гипервизора на модуле СЗИ ВИ Dallas Lock. Сбросить автоматическую блокировку досрочно на модуле может только администратор безопасности или пользователь, обладающий правом редактирования учетных записей.

Политика применяется на модулях СЗИ ВИ Dallas Lock.

(ВИ) Общее: Включить синхронизацию времени Linux клиентов

Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет».

Данная политика позволяет отключить синхронизацию времени между модулем СЗИ ВИ Dallas Lock и гипервизорами, работающими на ОС семейства Linux.

Политика применяется на модулях СЗИ ВИ Dallas Lock.

(ВИ) Общее: Включить синхронизацию времени по NTP
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет использовать NTP-сервера из заданного списка для синхронизации времени между сервером УД и агентами СЗИ ВИ. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Сервер виртуализации: Время, в течение которого подсчитываются ошибки ввода пароля
Политика принимает значения от 1 минуты до 4 часов 59 минут. По умолчанию значение данной политики: 1 минута. Данная политика позволяет установить количество времени, в течение которого подсчитываются ошибки ввода пароля на модуле СЗИ ВИ Dallas Lock. Если за данный период времени количество неудачных попыток входа достигнет максимального количества ошибок ввода пароля, учетная запись будет заблокирована на время, заданное в политике «Время блокировки учетной записи в случае ввода неправильных паролей». В случае, если за установленное время количество неудачных попыток входа не достигло заданного максимального количества ошибок ввода пароля — счетчик неудачных попыток обнуляется. Политика применяется на модулях СЗИ ВИ Dallas Lock.

5.4.3 Настройка политик аудита

На вкладке «Политики» в категории «Аудит» настраиваются параметры, касающиеся ведения журналов, в которых осуществляется регистрация событий, связанных с безопасностью.

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке политик аудита.

Таблица 9. Политики аудита

Аудит USB-накопителей
Возможное значение политики: «Не используется», «Зарегистрированные USB-накопители», «Незарегистрированные USB-накопители», «Все USB-накопители». По умолчанию значение данной политики: «Незарегистрированные USB-накопители». Данная политика позволяет вести регистрацию событий, связанных с подключаемыми USB-устройствами. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Аудит системных пользователей
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.». Включение данной политики позволяет вести учет действий системных пользователей модуля (SYSTEM, LOCAL SERVICE, NETWORK SERVICE и пр.) в журнале ресурсов (при условии, что журнал ресурсов включен). В большинстве случаев, аудит этих пользователей не требуется. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Аудит событий зачистки
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Включение данной политики позволяет регистрировать на модуле события зачистки остаточной информации в следующих случаях: • при включенных параметрах зачистки остаточной информации в СЗИ модуля; • при зачистке остаточной информации на модуле по запросу пользователя; • при зачистке накопителя на модуле. Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-K/C;
- СЗИ ВИ Dallas Lock.

Аудит устройств

Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.».

Включение данной политики позволяет регистрировать события по доступу к подключаемым на модуле устройствам в Журнале ресурсов (при условии, что журнал ресурсов включен). Сами события настраиваются непосредственно в консоли администрирования СЗИ модуля в окне редактирования параметров дескриптора устройства (класса устройств).

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-K/C;
- СЗИ ВИ Dallas Lock.

Вести журнал входов

Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.».

Включение журнала позволяет протоколировать в нем события, связанные с входом, выходом, разблокировкой пользователей на ПК, включая как локальные, так и сетевые, в том числе терминальные входы и выходы на модуле.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-K/C;
- СЗИ ВИ Dallas Lock;
- СЗИ НСД Dallas Lock Linux.

Вести системный журнал

Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.».

Включение данной политики (значение «Вкл.») позволяет протоколировать на модуле в журнале события системного журнала операционной системы (SysLog).

Политика применяется на модулях СЗИ НСД Dallas Lock Linux.

Выгрузка журналов

Настройка данной политики в дополнительном окне позволяет:

- экспортировать журналы СЗИ Dallas Lock 8.0 в журнал событий Windows;
- экспортировать журналы СЗИ Dallas Lock 8.0 в SIEM систему с возможностью выбора из выпадающих списков формата выгрузки (Syslog, CEF или LEEF) и кодировки выгрузки (UTF-8 или CP1251).

Для обоих типов экспорта возможно задать список экспортируемых журналов и определить период выгрузки журналов в диапазоне от 10 сек. до 24 часов.

По умолчанию политика имеет значение «Выкл.»

Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.

Журнал МЭ

Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.».

Политика позволяет управлять ведением журнала пакетов МЭ на клиентах СБ ВИ «Dallas Lock» (включение/отключение журнала).

Политика применяется на модулях СЗИ ВИ Dallas Lock.

Журнал доступа к устройствам

Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.».

Включение данной политики (значение «Вкл.») позволяет активировать фиксацию событий, связанных с настройками правил разграничения доступа, и обращения к подключаемым устройствам в журнале доступа к устройствам на модуле.

Политика применяется на модулях СЗИ НСД Dallas Lock Linux.

Журнал запуска/завершения процессов

Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.».

Включение журнала позволяет протоколировать в нем события запусков/завершения процессов в ОС на модуле.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СЗИ ВИ Dallas Lock.

Журнал печати

Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.».

Включение журнала позволяет протоколировать в нем события печати на локальных и сетевых печатающих устройствах (принтерах, МФУ, плоттерах и пр.) на модуле.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СЗИ НСД Dallas Lock Linux.

Журнал ресурсов

Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.».

Включение журнала позволяет протоколировать в нем события по доступу к ресурсам ФС, программно-аппаратной среды и к устройствам (при включенном параметре «Аудит устройств» см. ниже). А также события очистки остаточной информации (при включении «Аудит: событий зачистки»). Возможен аудит действий пользователей как с локальными ресурсами, так и с сетевыми. Сюда же заносятся события непосредственно по управлению доступом к ресурсам (в случае, когда на объект назначается любой дескриптор доступа, аудита, контроля целостности).

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СЗИ НСД Dallas Lock Linux;
- СЗИ ВИ Dallas Lock.

Журнал управления политиками безопасности

Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.».

Включение политики (значение «Вкл.») позволяет протоколировать события изменения политик безопасности в журнале.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СЗИ НСД Dallas Lock Linux;
- СЗИ ВИ Dallas Lock.

Журнал управления пользователями и группами

Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.».

Журнал содержит события, связанные с настройками, созданием и удалением учетных записей пользователей, групп учетных записей. Включение политики (значение «Вкл.») позволяет протоколировать в журнале данные события.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СЗИ НСД Dallas Lock Linux;
- СЗИ ВИ Dallas Lock.

Заносить в журнал исходящие попытки входа на удаленные компьютеры

Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет».

Включение данной политики (значение «Да») позволяет регистрировать на модуле события исходящей попытки входа пользователя на удаленный компьютер через ЛВС в журнале входов (при условии, что журнал входов включен).

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;

- СЗИ ВИ Dallas Lock.

Заносить в журнал ошибки Windows

Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.».

Включение данной политики позволяет вести учет ошибок доступа ОС Windows в журнале ресурсов (при условии, что журнал ресурсов включен). Так как СЗИ Dallas Lock 8.0 не подменяет механизмы контроля доступа к ресурсам ОС, а добавляет свои, то любое действие над ФС вначале попадает для проверки в драйвер защиты СЗИ, и, если этот драйвер разрешает данное действие, оно передается дальше ОС Windows. ОС может отказать уже по своим причинам — эти отказы и протоколируются. В большинстве случаев аудит этих ошибок не требуется.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СЗИ ВИ Dallas Lock.

Заносить в журнал события запуска и остановки ОС

Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Да».

Включение данной политики (значение «Да») позволяет регистрировать на модуле события, связанные с запуском/завершением работы ОС, события запуска/остановки ядра защиты СЗИ Dallas Lock, в журнале управления политиками (при условии, что данный журнал включен).

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СЗИ ВИ Dallas Lock.

Заносить в журнал события запуска и остановки модулей администрирования DL

Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Да».

Включение данной политики (значение «Да») позволяет регистрировать события, связанные с запуском/завершением работы модулей администрирования СЗИ Dallas Lock в журнале управления политиками (при условии, что данный журнал включен).

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СЗИ ВИ Dallas Lock.

Использовать часы платы СДЗ Dallas Lock

Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет».

Включение данной политики (значение «Да») позволяет использовать время из часов СДЗ Dallas Lock. Политика применяется только при установленной на АРМ аппаратной плате. Для работы политики необходимо в ОС модуля установить драйвер для СДЗ.

Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.

Максимальное количество записей в журнале

Настройка данной политики позволяет установить максимальное количество записей в определенном журнале модуля.

Политика может принимать значение «Не используется» или «100–20000».

По умолчанию в данной политике для каждого журнала задано значение 20000 записей.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СЗИ ВИ Dallas Lock.

Объём журналов в Мб (100-10000)

Политика устанавливает ограничения объема журналов в диапазоне от 100/Мб до 10000/Мб для архивации.

По умолчанию политике установлено значение «100/Мб».

Политика применяется на модулях СЗИ НСД Dallas Lock Linux.

Периодическая архивация журнала

Границы возможного временного интервала архивации варьируются от 1 часа до 1 года. По умолчанию политике задано значение «Не используется».

Включение данной политики позволяет управлять периодами автоматической архивации журналов. После настройки данной политики все журналы по расписанию архивируются, все записи из них сохраняются в файл в системной папке на АРМ с установленным СЗИ Dallas Lock 8.0 «C:\DLLOCK80\Logs», записи журналов очищаются, и они начинают вестись заново.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-K/C;
- СЗИ ВИ Dallas Lock.

Создавать теневые копии распечатываемых документов

Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет».

Данная политика позволяет включить (значение «Да») сохранение копий распечатываемых документов в отдельную папку на модуле по пути «C:\DLLOCK80\Logs\PrintCopy». В данной папке при каждой печати будут создаваться подпапки с файлами, названия которых состоят из времени печати и имени печатающего устройства.

Политика применяется на модулях СЗИ Dallas Lock 8.0.

Срок хранения журналов в месяцах

Данная политика позволяет управлять сроком хранения журналов на модулях. По истечению заданного в политике срока, формируется архив, и журналы начинают заполняться новыми данными.

Политика принимает значения от 3 до 6 месяцев. По умолчанию для данной политики установлено значение 3 месяца.

Политика применяется на модулях СЗИ НСД Dallas Lock Linux.

Фиксировать в журнале неправильные пароли

Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет».

При значении «Да» неверный пароль, введенный пользователем, отображается в журнале в столбце «Неверный пароль». При значении «Нет» — не отображается.

Внимание! При значении политики «Да» возникает риск использования информации, содержащейся в столбце «Неверный пароль», для скрытой компрометации паролей пользователей. Ошибки пользователей при вводе пароля неминуемо приведут к раскрытию части пароля, что может значительно облегчить для злоумышленника задачу его подбора.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-K/C;
- СДЗ Dallas Lock;
- СЗИ ВИ Dallas Lock.

(Агент ЕЦУ Linux) Журнал аутентификации

Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Вкл.».

Включение журнала (значение «Вкл.») позволяет протоколировать на модуле в журнале события аутентификации.

Политика применяется на модулях Агент ЕЦУ Linux.

(Агент ЕЦУ Linux) Журнал печати

Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.».

Включение журнала позволяет протоколировать в нем события печати на локальных и сетевых печатающих устройствах (принтерах, МФУ, плоттерах и пр.) на модуле.

Политика применяется на модулях Агент ЕЦУ Linux.

(Агент ЕЦУ Linux) Журнал пользовательских сообщений
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Вкл.». Включение журнала (значение «Вкл.») позволяет протоколировать на модуле в журнале события пользовательских сообщений. Политика применяется на модулях Агент ЕЦУ Linux.
(Агент ЕЦУ Linux) Системный журнал
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Вкл.». Включение данной политики (значение «Вкл.») позволяет протоколировать на модуле в журнале события системного журнала операционной системы (SysLog). Политика применяется на модулях Агент ЕЦУ Linux.
(Агент ЕЦУ Linux) Собирать только указанные уровни сообщений
Возможное значение политики: «Не используется» / «[*код события*]». Список правил отбора пишется в одну строку, элементы списка разделяются запятыми, значение по умолчанию: «Не используется». Включение данной политики позволяет фиксировать только те события, коды которых указаны в списке событий. Политика применяется на модулях Агент ЕЦУ Linux.
(Агент ЕЦУ Windows) Журнал безопасности
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Включение политики (значение «Вкл.») позволяет протоколировать события изменения политик безопасности в журнале. Политика применяется на модулях Агент ЕЦУ Windows.
(Агент ЕЦУ Windows) Журнал приложений
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Вкл.». В данном журнале фиксируются события об активности приложений, их целостности и набора загружаемых ими компонентов. Политика применяется на модулях Агент ЕЦУ Windows.
(Агент ЕЦУ Windows) Журнал установок
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.». В данном журнале фиксируются события, связанные с инсталляцией обновлений Windows, дополнительных приложений. Политика применяется на модулях Агент ЕЦУ Windows.
(Агент ЕЦУ Windows) Системный журнал
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Вкл.». Включение данной политики (значение «Вкл.») позволяет протоколировать на модуле в журнале события системного журнала операционной системы (SysLog). Политика применяется на модулях Агент ЕЦУ Windows.
(Агент ЕЦУ Windows) Собирать только указанные события
Возможное значение политики: «Не используется» / «[*код события*]». Значение по умолчанию: «[*код события*]». Включение данной политики позволяет фиксировать только те события, коды которых указаны в списке событий. Политика применяется на модулях Агент ЕЦУ Windows.
(ВИ) VMM: Блокировать SC VMM
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет заблокировать возможность подключиться к серверу VMM. Политика применяется на модулях СЗИ ВИ Dallas Lock.

(ВИ) Журнал агента гипервизора
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить регистрацию событий, происходящих на гипервизоре Hyper-V. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Заблокировать выгрузку журналов syslog в SQL
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Значение «Да» данной политики позволяет блокировать выгрузку журналов syslog в SQL для предотвращения передачи служебных данных. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Общее: ESXi Shell
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить на гипервизоре vSphere регистрацию событий и записей всех введенных команд в ESXi Shell. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Общее: USB-устройства
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию событий, связанных с подключаемыми USB-устройствами к гипервизору vSphere. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Общее: Агент ESXi
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию сведений о действиях агента, который управляет и конфигурирует гипервизор vSphere виртуальные машины, а также включить регистрацию событий аутентификации на гипервизоре vSphere. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Общее: Аутентификация
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию событий, связанных с аутентификацией на гипервизоре. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Общее: Виртуальные машины
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию событий, связанных с виртуальными машинами и гипервизорами. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Общее: Зачистка ФС
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию событий, связанных с зачисткой файловой системы гипервизора vSphere. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Общее: Системные события
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет».

Данная политика позволяет включить (значение «Да») на гипервизоре vSphere регистрацию общих сообщений журнала (Syslog), которые могут быть использованы для устранения неполадок. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Уведомления: Журнал событий ВИ Hyper-V (операции VMM)
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию событий, связанных с управлением хостами, кластерами и облачным сервисом виртуальной инфраструктуры Hyper-V. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Уведомления: События управления ВМ
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию событий, связанных с управлением ВМ гипервизора Hyper-V. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Уведомления: События управления конфигурацией ВМ
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию событий, связанных с управлением конфигурацией ВМ. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Уведомления: События управления конфигурацией гипервизора
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию событий, связанных с управлением конфигурацией ВМ виртуальной инфраструктуры Hyper-V. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Уведомления: События управления сетью
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить регистрацию событий, связанных с управлением сетью виртуальной инфраструктуры Hyper-V. Политика применяется на модулях СЗИ ВИ Dallas Lock.
(ВИ) Уведомления: События управления состоянием ВМ
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию событий, связанных с управлением состояния ВМ виртуальной инфраструктуры Hyper-V. Политика применяется на модулях СЗИ ВИ Dallas Lock.

5.4.4 Настройка политик прав пользователей

На вкладке «Политики» в категории «Права пользователей» настраиваются параметры, касающиеся полномочий пользователей на администрирование системы защиты, а также управляющие разрешением и запретом интерактивного и удаленного входов в ОС.

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке политик прав пользователей.

Для того, чтобы некоторый пользователь N имел возможность предоставлять другим пользователям полномочия на администрирование системы защиты, необходимо соблюдение двух условий:

1. Пользователь N должен быть наделен полномочием на изменение параметров безопасности.
2. Пользователь N должен сам обладать тем полномочием, которое хочет предоставить другим пользователям.

В системе защиты реализован механизм контроля за распространением полномочий. Осуществление этого контроля позволяет пользователю предоставлять другим пользователям только те полномочия, которыми он наделен сам. Например, если пользователь не наделен полномочием на управление аудитом, то и никакому другому пользователю он не сумеет предоставить это полномочие.

При попытке предоставить другому пользователю полномочие, которым данный пользователь сам не обладает, система защиты выведет предупреждение. Пользователь не сможет назначить сам себе дополнительное полномочие, повысить уровень доступа, включить себя в группу, обладающую расширенными по сравнению с данным пользователем правами.

Внимание! Назначать политики и права следует очень внимательно. Если при предоставлении любого полномочия выбрать группу «Все», то данным полномочием будут обладать все пользователи, в том числе и тот пользователь, который установил данный параметр. Так, например, если администратор при запрете локального (интерактивного) входа в ОС выберет группу «Все», то сам он также не сможет больше осуществить вход в ОС. Исключение будет составлять только учетная запись суперадминистратора на модулях СЗИ Dallas Lock 8.0-К/С.

Также следует учесть, что пользователь, обладающий полномочием на редактирование параметров безопасности, может лишить любых пользователей любых полномочий, даже тех, которыми он сам не обладает. Если пользователь сам себя лишил какого-либо полномочия, то восстановить это полномочие он не сможет.

Внимание! Правило разрешения и запрета действий субъектов следующее:

Условие	Результат
Нет никаких запретов и разрешений	Действие запрещено
Есть запись о разрешении и нет записи о запрете	Действие разрешено
Есть запись о запрете	Действие запрещено, несмотря на наличие или отсутствие записи о разрешении

В списке субъектов, для которых устанавливается запрет или разрешение, определяется иерархия в порядке возрастания: группа «Все» → индивидуальная группа → учетная запись (доменная учетная запись «по маске») → пользователь.

Таким образом, чтобы субъекту (например, пользователю) действие было разрешено, то он не должен входить в состав субъекта (например, группы), для которого это действие имеет явный запрет.

Пример:

Требуется настроить запрет входа в ОС для локальных пользователей (в доменной архитектуре).

Для запрета входа локальных пользователей необходимо изменить параметр «Интерактивный вход: разрешен» убрать учетную запись «Все» и добавить учетную запись «**». Если есть необходимость разрешения входа для пользователей определенного домена, то предварительно нужно создать учетную запись в виде «Имя_домена*».

Таблица 10. Политики прав пользователей

Аудит: Просмотр журналов
С помощью данной политики можно дать право определенным пользователям или группам на просмотр только журналов в оболочке администратора СЗИ. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Аудит: Просмотр теневых копий распечатываемых документов
С помощью данной политики можно дать право определенным пользователям или группам на просмотр теневых копий распечатываемых документов (копии создаются при условии, что включен параметр аудита «Создавать теневые копии распечатываемых документов»).

Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Аудит: Просмотр теневых копий файлов
С помощью данной политики можно дать право определенным пользователям или группам на просмотр теневых копий файлов. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Аудит: Управление
С помощью данной политики можно дать право определенным пользователям или группам на управление аудитом (назначение и редактирование назначенных параметров). Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Деактивация системы защиты
В значение данной политики прописывается имя учетной записи пользователя, имеющего право на управление деактивацией системы защиты (смена лицензии, удаление СЗИ, включение/выключение «мягкого» режима, «режима обучения» и «неактивного режима»). Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Изменение системного времени и часового пояса
С помощью данной политики можно запретить пользователям устройств, входящих в состав ДБ, изменять установленные дату и время. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Интерактивный вход: Запрещен
С помощью данной политики возможно запретить возможность интерактивного входа определенным пользователям и группам в ОС. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Интерактивный вход: Разрешен
С помощью данной политики возможно разрешить возможность интерактивного входа определенным пользователям и группам в ОС. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Параметры безопасности: Просмотр
С помощью данной политики можно дать право определенным пользователям или группам на просмотр установленных параметров аудита (в том числе журналов) и доступа. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Параметры безопасности: Управление
С помощью данной политики можно дать определенным пользователям или группам полномочия на управление параметрами безопасности. Если пользователю (группе пользователей) разрешено изменение параметров безопасности, то он может делегировать все свои полномочия другим пользователям с учетом действия контроля за распространением полномочий (см. выше). Если пользователю предоставлено право на управление параметрами безопасности, то право на просмотр установленных настроек предоставляется автоматически. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.

Печать запрещена
С помощью данной политики можно гибко настроить список учетных записей, которым запрещена печать с данного компьютера. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Печать разрешена
С помощью данной политики можно гибко настроить список учетных записей, которым разрешена печать с данного компьютера. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Принудительное завершение работы по расписанию
Данная политика позволяет настроить список учетных записей и групп, для которых согласно настройке «Расписание работы» по окончанию времени работы ПК пользователя будет заблокирован. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Ресурсы: Управление дискреционным доступом
С помощью данной политики можно назначить учетные записи пользователей для управления дискреционным доступом. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Ресурсы: Управление контролем целостности
С помощью данной политики можно назначить учетные записи пользователей для управления контролем целостности. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Ресурсы: Управление мандатным доступом
С помощью данной политики можно назначить учетные записи пользователей для управления мандатным доступом. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Удаленный вход: Запрещен
С помощью данной политики возможно запретить возможность удаленного входа определенным пользователям и группам в ОС. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Удаленный вход: Разрешен
С помощью данной политики возможно разрешить возможность удаленного входа определенным пользователям и группам в ОС. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Учетные записи: Принудительная двухфакторная аутентификация
Если в значении данной политики стоит определенная учетная запись или группа, то при регистрации новой учетной записи (в составе данной группы или индивидуально) или редактировании в СЗИ присвоение идентификатора будет обязательным, иначе будет выведено предупреждение об ошибке. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.

Учетные записи: Управление
Если в значении данной политики стоит учетная запись или группа, то она обладает полномочиями по созданию, удалению и изменению учетных записей пользователей в системе защиты. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.

5.4.5 Настройка политик контроля целостности

На вкладке «Политики» в категории «Контроль целостности: Политики» настраиваются параметры проверки целостности отдельно для:

- объектов ФС;
- объектов программно-аппаратной среды;
- реестра.

По умолчанию проверка целостности установлена только при загрузке модуля.

В остальных случаях, для корректной работы политик, необходимо настроить каждый параметр политик контроля целостности в соответствии с требованиями политики безопасности организации:

- установить режим проверки (при загрузке, периодичный контроль или контроль по расписанию);
- указать алгоритм расчета контрольной суммы (CRC32 или Хэш MD5).

Примечание. Если для проверки объектов программно-аппаратной среды не выбран алгоритм расчета контрольной суммы, то проверка целостности для данного типа объектов выполнятся не будет.
Автоматический выбор алгоритма расчета контрольной суммы по умолчанию не предусмотрен.

Таблица 11. Политики контроля целостности

Генерация событий аудита аппаратной целостности
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Включение данной политики (значение «Да») позволяет отслеживать события нарушения аппаратной целостности. Политика применяется на модулях СЗИ НСД Dallas Lock Linux.
Изменение файлов с назначенным контролем целостности
Данная политика позволяет управлять возможностью изменения файлов с назначенным контролем целостности. Политика может принимать одно из значений: • «Разрешить» — при нарушении целостности СЗИ не блокирует доступ к объекту, для которого назначен контроль целостности; • «Запретить» — при нарушении целостности СЗИ блокирует доступ к объекту, для которого назначен контроль целостности; • «Проверять цифровую подпись исполняемых файлов» — осуществляется проверка электронной подписи для исполняемых файлов (список расширений файлов можно дополнить). По умолчанию значение данной политики: «Разрешить». Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Контроль ФС по расписанию
Данная политика позволяет включить контроль целостности файловой системы по расписанию и настроить расписание контроля. По умолчанию данная политика не используется. Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-K/C;
- СЗИ ВИ Dallas Lock.

Контроль прогр. апп. среды по расписанию

Данная политика позволяет включить контроль целостности программно-аппаратной среды по расписанию и настроить расписание контроля.

По умолчанию данная политика не используется.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-K/C;
- СЗИ ВИ Dallas Lock.

Контроль реестра по расписанию

Данная политика позволяет включить контроль целостности реестра Windows по расписанию и настроить расписание контроля.

По умолчанию данная политика не используется.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-K/C;
- СЗИ ВИ Dallas Lock.

Контроль целостности прогр. апп. среды: BIOS

Данная политика позволяет включить контроль изменений параметров BIOS.

По умолчанию данная политика выключена.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-K/C;
- СЗИ ВИ Dallas Lock.

Контроль целостности прогр. апп. среды: USB-устройства

Данная политика позволяет включить контроль изменений в USB-контроллере, подключения и отключения USB-портов.

По умолчанию данная политика выключена.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-K/C;
- СЗИ ВИ Dallas Lock.

Контроль целостности прогр. апп. среды: Диски

Данная политика позволяет включить контроль изменений контроллеров гибких дисков, дисководов и дисковых устройств.

По умолчанию данная политика выключена.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-K/C;
- СЗИ ВИ Dallas Lock.

Контроль целостности прогр. апп. среды: Драйверы

Данная политика управляет контролем целостности установки и удаления драйверов.

По умолчанию данная политика выключена.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-K/C;
- СЗИ ВИ Dallas Lock.

Контроль целостности прогр. апп. среды: Кодеки
Данная политика управляет контролем установки или удаления кодеков на ПК. По умолчанию данная политика выключена. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Контроль целостности прогр. апп. среды: Операционная система
Данная политика управляет контролем изменений свойств ОС данного ПК: изменений имени, IP-адреса и пр. По умолчанию данная политика выключена. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Контроль целостности прогр. апп. среды: Папки общего доступа
Данная политика управляет контролем создания или удаления папок общего доступа на данном ПК. По умолчанию данная политика выключена. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Контроль целостности прогр. апп. среды: Принтеры
Данная политика управляет контролем списка всех установленных на ПК принтеров, факсов, МФУ и др. печатающих устройств. По умолчанию данная политика выключена. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Контроль целостности прогр. апп. среды: Программы
Данная политика управляет контролем установки или удаления программ на данном ПК. По умолчанию данная политика выключена. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Контроль целостности прогр. апп. среды: Разделы диска
Данная политика управляет контролем изменений разделов жесткого диска, форматирований диска, подключений новых дисков. По умолчанию данная политика выключена. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Контроль целостности прогр. апп. среды: Сеть
Данная политика управляет контролем сетевых подключений и сетевых карт. По умолчанию данная политика выключена. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.

Контроль целостности прогр. апп. среды: Система
Данная политика позволяет включить контроль портов, мониторов, шин, звуковых устройств и других системных устройств. По умолчанию данная политика выключена. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Контроль целостности прогр. апп. среды: Список пользователей
Данная политика управляет контролем списка пользователей, созданных в локальной ОС. По умолчанию данная политика выключена. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Контроль целостности прогр. апп. среды: Устройства ввода
Данная политика управляет контролем подключенных устройств ввода на данном ПК: клавиатуры, мыши. По умолчанию данная политика выключена. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Периодический контроль ФС
Политика принимает значения от 1 минуты до 5 часов и «Не используется». По умолчанию значение данной политики: «Не используется». Данная политика позволяет включить периодический контроль файловой системы и настроить периодичность проверки. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Периодический контроль прогр. апп. среды
Политика принимает значения от 1 минуты до 5 часов и «Не используется». По умолчанию значение данной политики: «Не используется». Данная политика позволяет включить периодический контроль программно-аппаратной среды и настроить периодичность проверки. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Периодический контроль реестра
Политика принимает значения от 1 минуты до 5 часов и «Не используется». По умолчанию значение данной политики: «Не используется». Данная политика позволяет включить периодический контроль реестра Windows и настроить периодичность проверки. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Проверять целостность ФС при загрузке ОС
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.».

Данная политика позволяет управлять включением/отключением автоматической проверки целостности файловой системы при загрузке ОС.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СЗИ ВИ Dallas Lock.

Проверять целостность прогр. апп. среды при загрузке ОС

Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.».

Данная политика позволяет управлять включением/отключением автоматической проверки программно-аппаратной целостности при загрузке ОС.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СЗИ НСД Dallas Lock Linux;
- СЗИ ВИ Dallas Lock.

Проверять целостность реестра при загрузке ОС

Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.».

Данная политика позволяет управлять включением/отключением автоматической проверки целостности реестра Windows при загрузке ОС.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С;
- СЗИ ВИ Dallas Lock.

Изменение файлов с назначенным контролем целостности

Возможное значение политики «Разрешить»/«Запретить». Значение по умолчанию: «Запретить».

Данная политика позволяет контролировать возможность пользователя изменять файлы с назначенным контролем целостности. При значении «Разрешить» при нарушении целостности СЗИ не блокирует доступ к объекту, для которого назначен контроль целостности. При значении «Запретить» при нарушении целостности СЗИ блокирует доступ к объекту, для которого назначен контроль целостности.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С.

Проверка цифровой подписи исполняемых файлов

Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.».

Данная политика позволяет определять необходимость проверки цифровой подписи исполняемых файлов. При значении «Вкл.» необходимо указать расширения исполняемых файлов для проверки цифровой подписи.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С.

Блокируемые расширения файлов

Политика позволяет управлять списком расширений, работа с которыми будет блокирована. Значение по умолчанию: «Не используется».

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-К/С.

5.4.6 Настройка политик режима работы СЗИ

На вкладке «Политики» в категории «Режим работы СЗИ» настраиваются параметры неактивного режима СЗИ для модуля СЗИ Dallas Lock 8.0 и СЗИ ВИ Dallas Lock.

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке политик режима работы СЗИ.

Таблица 12. Политики режима работы СЗИ

Межсетевой экран
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Вкл.». Данная политика позволяет управлять включением/выключением модуля «Межсетевой экран» СЗИ Dallas Lock 8.0. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Неактивный режим СЗИ Dallas Lock
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.». Данная политика позволяет управлять включением/выключением «Неактивного режима СЗИ» в СЗИ Dallas Lock 8.0. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Неактивный режим СЗИ ВИ Dallas Lock
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.». Данная политика позволяет управлять включением/выключением «Неактивного режима СЗИ» в СЗИ ВИ Dallas Lock. Политика применяется на модулях СЗИ ВИ Dallas Lock.
Система обнаружения вторжений
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Вкл.». Данная политика позволяет управлять включением/выключением модуля «Система обнаружения вторжений» СЗИ Dallas Lock 8.0. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.

5.4.7 Настройка политик очистки остаточной информации

Большинство ОС при удалении файла не удаляют содержимое файла, а удаляют лишь запись о файле из директории ФС. Так сделано для ускорения работы системы.

Реальное содержимое файла остается на запоминающем устройстве, и его можно просмотреть до тех пор, пока ОС заново не использует это пространство для хранения новых данных. Остаточная информация может привести к непреднамеренному распространению конфиденциальной и секретной информации.

На вкладке «Политики» в категории «Очистка остаточной информации» настраиваются параметры очистки остаточной информации, которые предназначены для обеспечения гарантий по предотвращению восстановления удаленных на модулях данных.

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке политик очистки остаточной информации.

Таблица 13. Политики очистки остаточной информации

Затирающая последовательность
Данной политикой определяется метод затирания остаточной информации путем установки числовых байтовых значений (от 0 до F) для каждого из четырех циклов затирания. Если эти значения не установлены или установлены не для каждого цикла, то по умолчанию для затирающей последовательности циклов используется последовательность, установленная в СЗИ Dallas Lock 8.0. Установленный метод затирания используется при всех установленных видах очистки остаточной информации: по команде администратора, в автоматическом режиме, и при зачистке накопителя. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.

Количество циклов затирания
Политика «Количество циклов затирания» позволяет выбрать от одного до четырех циклов затирания информации на модуле. Значение по умолчанию: «1». Установленное количество циклов затирания используется при всех установленных видах очистки остаточной информации: по команде администратора, в автоматическом режиме, и при зачистке накопителя. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Очищать освобождаемое дисковое пространство
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Включение данной политики (значение «Да») позволяет автоматически затирать всю остаточную информацию при освобождении областей на дисках, то есть при удалении файлов или при уменьшении размеров файлов на модуле. Затирание производится записью маскирующей последовательности (политика «Затирающая последовательность») поверх освобождаемого пространства заданным количеством циклов затирания (политика «Количество циклов затирания»). Включение данного параметра может заметно снизить скорость выполнения файловых операций, особенно при количестве циклов затирания больше единицы. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Очищать только конфиденциальные данные
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Включение данной политики (значение «Да») позволяет осуществлять автоматическую зачистку освобождаемого дискового пространства только при удалении/перемещении/уменьшении размера объектов ФС при работе под мандатной меткой или уровнем доступа больше нуля на модуле. Данная политика функционирует при условии включенной политики «Очищать освобождаемое дисковое пространство». Политика применяется на модулях СЗИ Dallas Lock 8.0-С.
Очищать файл подкачки виртуальной памяти
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Включение данной политики (значение «Да») позволяет автоматически затирать всю остаточную информацию в файле подкачки Windows на модуле. Затирание производится записью маскирующей последовательности поверх файла подкачки. Очистка производится при завершении работы (закрытии файла подкачки) и, если очистка была прервана, при старте системы (открытии файла подкачки). Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Проверять зачистку остаточной информации
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Если данная политика включена, то после проведения очистки объектов ФС на модуле, дополнительно выполняется проверка того, что очистка действительно осуществлена. В том случае, если проверка выявила, что очистка не осуществлена или завершена с ошибкой, то в журнал ресурсов модуля заносится соответствующее событие. Проверка осуществляется при очистке остаточной информации, выполняемой по команде администратора, в автоматическом режиме, и при зачистке накопителя целиком (функция «Зачистка диска»). Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.

5.4.8 Настройка политик ДСЧ

На вкладке «Политики» в категории «Политики ДСЧ» настраиваются параметры работы датчика случайный чисел для модулей СДЗ Dallas Lock.

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке политик ДСЧ.

Таблица 14. Политики ДСЧ

Разрешить генерацию пароля
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Да». В значении «Да» пользователю дается возможность генерации паролей. В значении «Нет» у пользователя нет возможности воспользоваться генерацией пароля. Политика применяется на модулях СДЗ Dallas Lock.
Тестировать ДСЧ при входе
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Да». В значении «Да» осуществляется тестирование ДСЧ при входе. При значении «Нет» тестирование ДСЧ при входе отключено Политика применяется на модулях СДЗ Dallas Lock.
Число попыток самотестирования ДСЧ
Возможное значение параметра: от 1 до 3. Значение по умолчанию: «1». Установленное значение данной политики регламентирует число попыток самотестирования ДСЧ. Политика применяется на модулях СДЗ Dallas Lock.

5.4.9 Настройка политик мандатного доступа

Согласно мандатному принципу управления доступом, каждому объекту можно присвоить уровень доступа и мандатную метку. Для учетной записи пользователя также назначается уровень доступа и мандатная метка, которые определяют объекты, к которым может быть доступ. Мандатный принцип управления доступом делится на две категории:

1. **Иерархическая категория** — осуществляется сравнение уровней доступа объекта и пользователя. В модуле СЗИ Dallas Lock 8.0-C уровни доступа имеют номера от 0 до 7. Чем больше номер, тем выше уровень доступа. Если не указан уровень доступа, то считается, что объект имеет уровень доступа 0 («Открытые данные»). Если уровень доступа присвоить родительскому объекту (папке, диску), то все объекты, находящиеся внутри, будут иметь тот же уровень доступа, за исключением тех случаев, когда им явно присвоен другой уровень доступа.

   Для удобства работы, уровням доступа можно присваивать имена. По умолчанию первым пяти уровням доступа (от 0 до 4) присвоены наименования:
   - 0 (Открытые данные);
   - 1 (Конфиденциальные данные);
   - 2 (Персональные данные);
   - 3 (Секретные данные);
   - 4 (Совершенно секретно).

   Согласно данному присвоению уровней доступа, пользователь, имеющий допуск уровня «Конфиденциальные данные», не может получить доступ к объекту с уровнем доступа «Секретные данные». В то же время, пользователь с допуском уровня «Секретные данные» имеет право доступа к объекту с уровнем «Конфиденциальные данные».

2. **Неиерархическая категория** — осуществляется сравнение мандатных меток объекта и пользователя. В случае совпадения мандатных меток объекта и пользователя, пользователь получает доступ к объекту. В случае несовпадения мандатных меток объекта и пользователя — доступ блокируется. Например, пользователь, имеющий мандатную метку «Метка 1», не может получить доступ к объектам с мандатными метками «Метка 2», «Метка 3» и т. д. Данный пользователь может получить доступ только к объектам с мандатной меткой «Метка 1». По умолчанию на модуле СЗИ Dallas Lock 8.0-C мандатные метки отсутствуют.

На вкладке «Политики» в категории «Мандатный доступ» настраиваются параметры работы с уровнями доступа и мандатными метками в Домене безопасности.

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке политик мандатного доступа.

Таблица 15. Политики мандатного доступа

Вход: выбор мандатной метки при входе в ОС
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.». Включение данной политики разрешает использование мандатных меток для авторизации в ОС Windows. Политика применяется на модулях СЗИ Dallas Lock 8.0-C.
Вход: запрет одновременной работы пользователей с различными уровнями или метками мандатного доступа
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.». При включении запрета одновременной работы пользователей с различными уровнями или метками мандатного доступа на данном ПК будет возможна одновременная работа нескольких интерактивных пользователей, зашедших только под одним уровнем доступа или мандатной метки. Причем данный уровень будет определяться по уровню или метке первого пользователя, зашедшего на данный компьютер.   **Примечание**. Если при включении запрета, есть уже запущенные сессии с различными уровнями доступа или мандатными метками, рекомендуется выполнить перезагрузку компьютера. Если не следовать данной рекомендации, может получиться, что суперадминистратор при блокировании своей запущенной сессии не сможет ее разблокировать в виду вступления в действия имеющегося ограничения. Политика применяется на модулях СЗИ Dallas Lock 8.0-C.
Мандатные метки
Данная политика предназначена для редактирования списка мандатных меток для организации неиерархического принципа управления мандатным доступом в ДБ. В редакторе политики можно создавать новые мандатные метки и удалять существующие. Политика применяется на модулях СЗИ Dallas Lock 8.0-C.
Уровни доступа
Данная политика предназначена для редактирования списка уровней доступа для организации иерархического принципа управления мандатным доступом в ДБ. В редакторе политики можно присвоить/отредактировать имя, соотносимое с определенным уровнем доступа. Всего доступно 8 уровней доступа (от «0» до «7»). Политика применяется на модулях СЗИ Dallas Lock 8.0-C.

5.4.10 Настройка политик доступа

На вкладке «Политики» в категории «Доступ» настраиваются параметры блокировки работы с файлами определенных расширений и блокировки автозапуска подключенных устройств.

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке политик доступа.

Таблица 16. Политики доступа

Блокировать автозапуск подключенных устройств
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». При включении данной политики автоматически блокируется возможность запуска без команды пользователя (автозапуска) устройства при подключении. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Блокируемые расширения
Данная политика используется для работы со списком запрещенных расширений файлов (последовательности символов, добавляемых к имени файла и предназначенных для идентификации формата файла). По умолчанию данная политика не используется. Список блокируемых расширений файлов пишется в одну строку, элементы списка разделяются точкой с запятой. Функция «Блокируемые расширения» будет распространяться на всех пользователей кроме суперадминистратора. При попытке пользователя открыть файл с заблокированным расширением, появится соответствующее предупреждение. **Внимание!** Следует учесть, что добавление в список блокируемых расширений, таких как exe, dll, sys, может привести к неработоспособности ОС (исключение составит работа под учетной записью суперадминистратора). Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Время ожидания подключения по VNC(секунд)
Политика позволяет установить время ожидания удаленного подключения к рабочему столу компьютера по сети. Возможные значения параметра от 5 до 600 секунд. Значение по умолчанию: «120». По истечении установленного времени запрос прерывается. **Примечание.** При инициировании подключения по VNC консоль ЕЦУ блокируется до момента подключения/отказа в подключении. Политика применяется на модулях: • Агент ЕЦУ Windows • Агент ЕЦУ Linux

5.4.11 Настройка политик сети

На вкладке «Политики» в категории «Сеть» настраиваются параметры работы сетевого взаимодействия.

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке политик сети.

Таблица 17. Политики сети

Время хранения сетевого кэша
Политика принимает значения от 5 минут до 14 дней и «Не используется». По умолчанию значение данной политики: «Не используется». Для увеличения скорости работы по сети СЗИ Dallas Lock 8.0 предоставляет возможность сохранения сетевого кэша с информацией об имеющихся в сети тех компьютеров, которые защищены Dallas Lock 8.0, и к которым уже было произведено обращение с данного ПК. Данная политика позволяет выбрать время хранения такого сетевого кэша. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.

Список незащищенных серверов
С помощью данной политики для увеличения скорости работы по сети, чтобы сократить количество обращений, СЗИ Dallas Lock 8.0 предоставляет возможность сохранить постоянный список ПК, которые не защищены СЗИ. Вводятся имена ПК и серверов или их IP-адреса через точку с запятой. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.

5.4.12 Настройка политик аппаратной идентификации

На вкладке «Политики» в категории «Аппаратная идентификация» производится включение считывателей аппаратных идентификаторов для модулей СЗИ Dallas Lock 8.0-К/С.

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке политик аппаратной идентификации.

Политики аппаратной идентификации принимают значения «Вкл.» и «Выкл.».

Доступна настройка следующих типов аппаратных идентификаторов:

- Считыватели Рутокен;
- Считыватели eToken;
- Считыватели TM COM-P (DS9097);
- Считыватели TM COM-A (DS9097U);
- Считыватели KT-TM;
- Считыватели JaCarta PKI;
- Считыватели JaCarta GOST;
- Считыватели HID IronLogic Z-2;
- Считыватели ESMART;
- USB flash drive;
- NFC-метки и смарт-карты.

На проверку идентификационной информации пользователя настройка политик аппаратной идентификации не влияет. Поэтому, если, например, настроить считыватель, задать пользователю аппаратный идентификатор, а после изменить значение политики для данного типа аппаратных считывателей на «Выкл.», то при входе данного пользователя аппаратный идентификатор все равно будет проверяться, и, соответственно, он не сможет войти в систему. Если пользователю задан аппаратный идентификатор, система защиты обязана его проверить, а если проверить нельзя, то допустить пользователя до информационных ресурсов система защиты не имеет права.

5.5 Задания ДБ

Команды, отправляемые с ЕЦУ Dallas Lock на модули, с ожидаемым результатом выполнения со стороны модуля называются в ЕЦУ Dallas Lock заданиями.

Управление заданиями осуществляется на вкладке «Задания» (рис. 80).

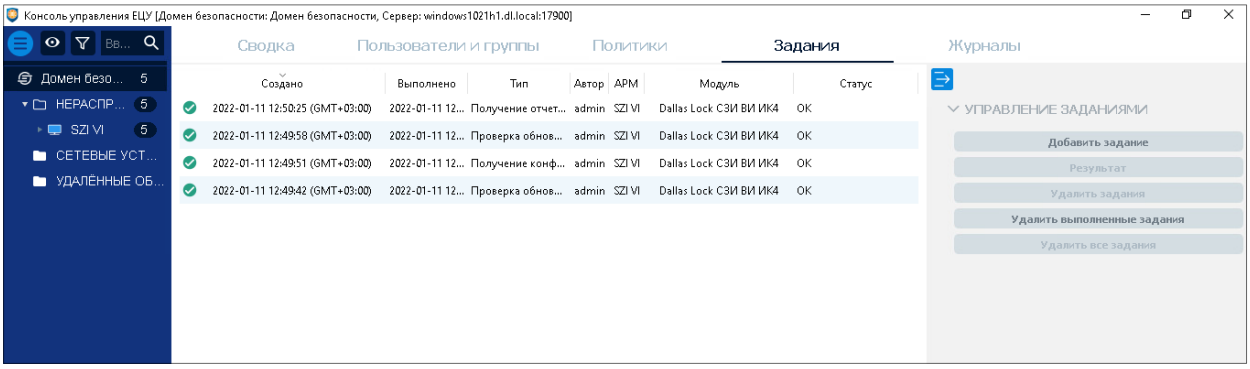

Рис. 80. Вкладка «Задания»

Список заданий на уровне ДБ представляет собой таблицу с полями:

1. «Создано» — содержит информацию о дате и времени создания задания, также в данном поле содержится иконка, которая указывает на статус выполнения задания:

— задание выполнено;

— задание ожидает выполнения;

— при выполнении задания произошла ошибка.

2. «Выполнено» — содержит дату и время выполнения задания.
3. «Тип» — содержит название задания.
4. «Автор» — содержит имя учетной записи пользователя ЕЦУ, создавшего задание.
5. «АРМ» — содержит имя ПК, для выполнения на котором создано данное задание.
6. «Модуль» — содержит информацию о типе модуля, для выполнения на котором создано данное задание.
7. «Статус» — указывает на статус выполнения задания.

5.5.1 Создание заданий

Для создания нового задания на уровне ДБ необходимо:

1. Выбрать ДБ в дереве консоли и перейти на вкладку «Задания».
2. Выбрать пункт «Добавить задание» на панели инструментов.
3. На экране появится окно мастера создания нового задания (рис. 81).

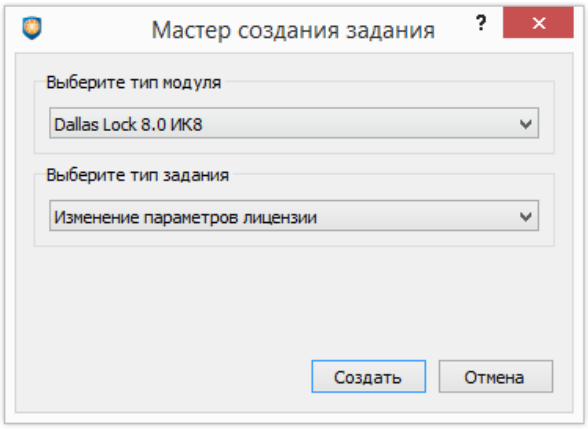

Рис. 81. Мастер создания задания

4. Выбрать тип модуля и тип задания.
5. Нажать кнопку «Создать».
6. При необходимости указать дополнительную информацию, необходимую для создания задания.

Очередь созданных заданий доступна при выборе объекта в дереве и переходе на вкладку «Задания».

Созданное задание ассоциируется с конкретным модулем в домене, поэтому при создании задания на уровне ДБ в списке появятся записи о заданиях по количеству в домене модулей того типа, который указан при создании задания. Типы заданий для каждого отдельного модуля перечислены в таблице ниже.

Если в Домене безопасности не зарегистрировано ни одного модуля того типа, который указан при создании задания, задание не создается и не попадает в очередь.

При создании дубликата не выполненного задания для модуля возникает предупреждение (рис. 82), происходит обновление задания, при этом старое задание удаляется и остается только более новое.

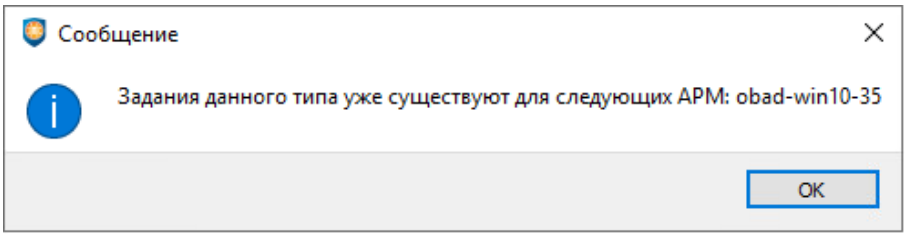

Рис. 82. Предупреждение о создании дубликата задания

Таблица 18. Типы заданий

Наименование модуля	Типы заданий
СЗИ Dallas Lock 8.0-K/C	• изменение параметров лицензии (изменяет номер лицензии и код технической поддержки); • получение конфигурации; • применение конфигурации; • проверка целостности
СЗИ НСД Dallas Lock Linux	• изменение параметров лицензии (изменяет номер лицензии и код технической поддержки)
Dallas Lock СЗИ ВИ	• изменение параметров лицензии (изменяет номер лицензии и код технической поддержки); • получение конфигурации; • получение отчета о конфигурации (*формат *.rtf*); • применение конфигурации; • проверка обновлений
СДЗ Dallas Lock	• очистка журнала; • получение конфигурации; • получение отчета об аппаратном обеспечении; • получение отчета по конфигурации; • применение конфигурации
WAF Dallas Lock	• восстановить резервную копию; • обновление базы разрешающих правил; • сбор журналов; • сброс к заводским настройкам; • создать резервную копию
Агент ЕЦУ	• отчет об аппаратном обеспечении; • удаление Агента ЕЦУ; • отчет о программном обеспечении
Kaspersky Endpoint Security	• обновление антивирусных баз; • сканирование клиентских АРМ

5.5.2 Результат выполнения задания

Модули выполняют полученные задания при первой возможности и отправляют результат на ЕЦУ Dallas Lock.

Для сохранения результата выполнения задания необходимо выбрать выполненное задание в списке и нажать на панели инструментов команду «Показать результат» или дважды щелкнуть левой кнопкой мыши по заданию.

5.5.3 Удаление заданий

Для удаления задания из списка необходимо выбрать задание и нажать на панели инструментов команду «Удалить выделенные задания».

Также на панели инструменты доступны команды для удаления нескольких заданий:

- «Удалить выполненные задания»;
- «Удалить все задания».

5.6 Журнал ДБ

Вкладка «Журналы» на уровне Домена безопасности позволяет просматривать следующие категории журналов ДБ (рис. 83):

«Журнал ЕЦУ» — отображаются регистрируемые события, связанные непосредственно с работой текущего ДБ ЕЦУ Dallas Lock;

«Журнал сессий» — отображается информация о создании и завершении сессии на АРМ;

«Журнал Syslog» — отображаются регистрируемые события, связанные с изменением конфигурации сетевых устройств, зарегистрированных в ДБ.

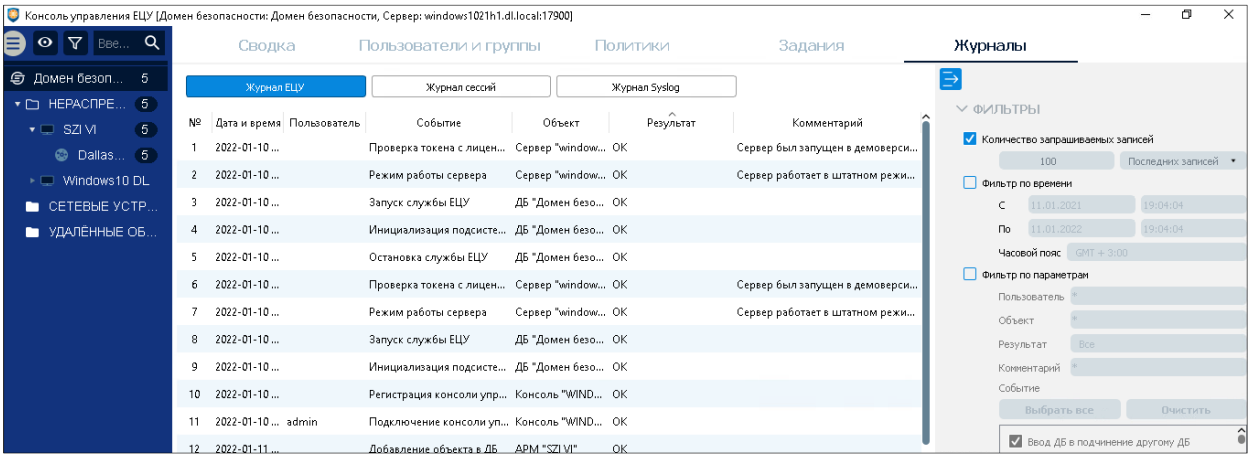

Рис. 83. Вкладка «Журналы» Домена безопасности

Примечание. Для корректной регистрации времени событий в журнале ДБ должна работать синхронизация времени, как на отдельном сервере, так и на каждом сервере, входящем в кластер ЕЦУ.

Примечание. Для хранения журналов во внешней базе данных необходимо использовать PostgreSQL версии 13 или выше.

Справа расположены панель инструментов «Фильтры» и панель инструментов «Действия».

Параметры фильтрации зависят от категории журнала. Сброс и применение выбранных фильтров осуществляется по команде «Сбросить» и «Применить» соответственно.

Отфильтрованные записи журнала можно сохранить в выбранном типе файла (TXT, CSV) с помощью команды «Экспортировать журнал» на панели инструментов «Действия». Экспортировать журнал можно учитывая текущую сортировку, для этого необходимо установить соответствующий флаг в окне «Экспорт журнала».

Для очистки выбранного журнала модуля используется команда «Очистить журнал» на панели инструментов «Действия».

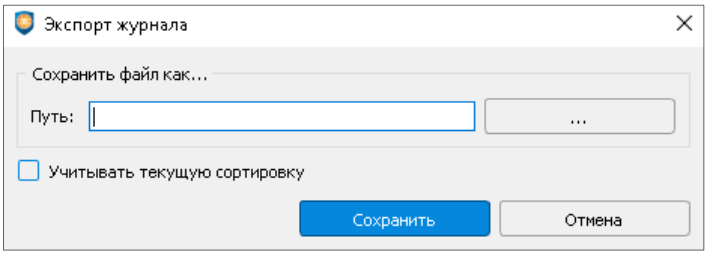

Рис. 84. Окно «Экспорт журнала»

Двойной клик по пункту журнала откроет окно с подробностями записи (рис. 85). Нажимая на кнопки «вверх» и «вниз» можно просматривать записи журнала.

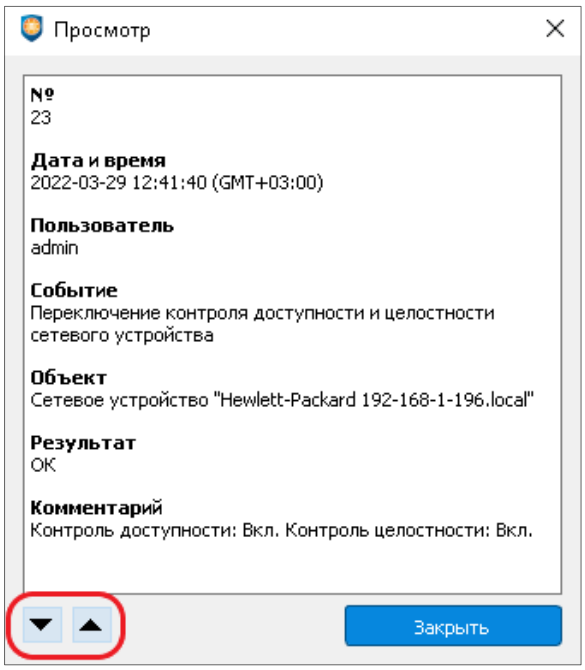

Рис. 85. Просмотр подробности записи журнала

6 ГРУППЫ ДОМЕНА БЕЗОПАСНОСТИ

6.1 Базовые группы

В дереве объектов Консоли ЕЦУ всегда присутствуют базовые группы, предназначенные для обеспечения состояния защищенности объектов Домена безопасности:

- нераспределенные объекты;
- сетевые устройства;
- удаленные объекты.

Удаление, переименование и перемещение базовых групп недоступно.

Примечание. При добавлении нового модуля в ДБ он всегда помещается в группу «Нераспределенные объекты» и при этом:

1. Модуль включается в группу в составе АРМ (за исключением модулей без АРМ).
2. Значения политик для него наследуются из политик группы «Нераспределенные объекты».
3. Списки учетных записей копируются из списка группы «Нераспределенные объекты».

Примечание. При добавлении нового сетевого устройства в ДБ оно всегда помещается в группу «Сетевые устройства».

Примечание. Группа «Удаленные объекты» предназначена для получения доступа к журналам объекта после удаления из ДБ. Восстановление объектов, перемещенных в группу «Удаленные объекты», недоступно.

В дальнейшем администратор ЕЦУ Dallas Lock может перенести модуль из базовой группы «Нераспределенные объекты» в любую другую группу (подгруппу). Подгруппы также можно перемещать в другие группы. Для этого можно перетащить значок нужного объекта кнопкой мыши в поле другого значка («Drag-and-drop»).

6.2 Настройка групп

Создать группу/подгруппу можно несколькими способами:

- выбрать элемент дерева ДБ (для расположения новой группы), нажать кнопку «Создать группу» на панели инструментов «Действия»;
- выбрать пункт «Создать группу» в контекстном меню нужного уровня дерева ДБ.

Введенное на этапе создания наименование группы, можно впоследствии изменить.

Перемещение группы в дереве осуществляется перетаскиванием значка кнопкой мыши в поле другого значка («Drag-and-drop»). Перемещение группы осуществляется со всеми вложенными объектами.

Удалить существующую группу можно с помощью кнопки «Удалить группу» на панели инструментов «Действия» или воспользовавшись контекстным меню в дереве ДБ. Удаление группы осуществляется со всеми вложенными объектами.

Каждая группа (подгруппа) в дереве объектов содержит одинаковые вкладки для индивидуальной настройки параметров для модулей, АРМ, сетевых устройств и подгрупп в составе данной группы (кроме базовых групп «Сетевые устройства» и «Удаленные объекты», для них доступна только вкладка «Сводка»).

6.2.1 Сводка для группы ДБ

Вкладка «Сводка» для выбранной группы в дереве объектов отображает общее состояние модулей и сетевых устройств, входящих в группу (рис. 86).

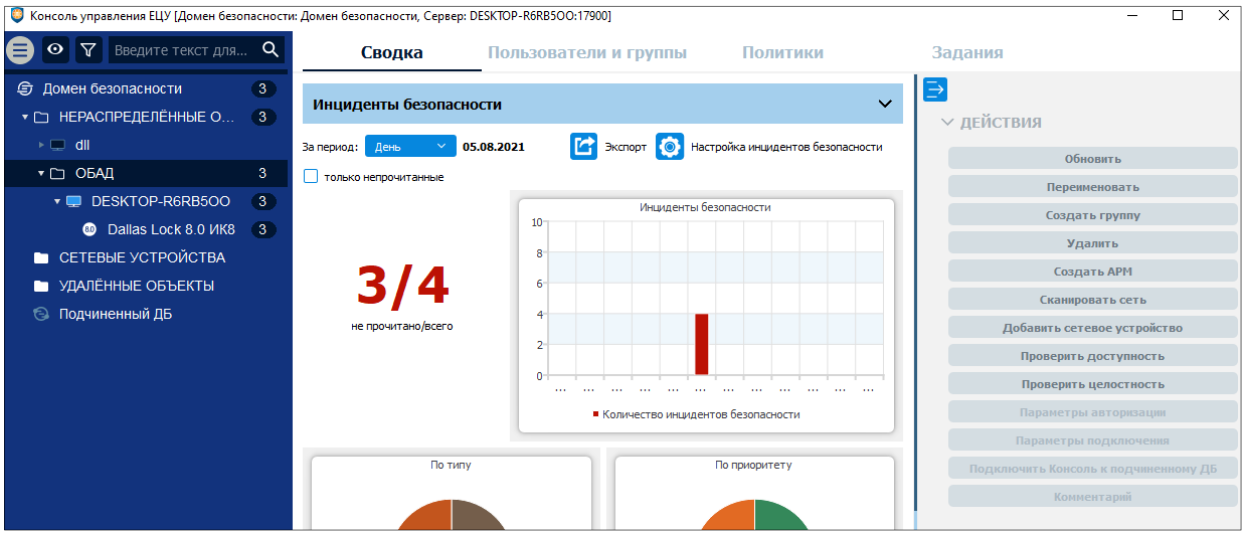

Рис. 86. Вкладка «Сводка» для группы ДБ

Управление данной вкладкой аналогично управлению вкладки «Сводка» на уровне ДБ.

На панели инструментов доступны следующие действия с группой:

1. Обновить информацию о группе.
2. Переименовать группу.
3. Добавить в состав группы (подгруппы) новую подгруппу.
4. Удалить группу из ДБ (все вложенные объекты группы перемещаются в базовую группу «Удаленные объекты»).
5. Создание АРМ в составе группы.
6. Сканирование сети для обнаружения модулей и сетевых устройств.
7. Добавление сетевого устройства.
8. Проверить доступность сетевых устройств.
9. Проверить целостность сетевых устройств.

На панели инструментов доступны следующие команды оперативного управления для группы (набор команд зависит от модулей, входящих в состав группы):

1. Выключить.
2. Перезагрузить.
3. Разблокировать пользователей.
4. Пересчитать целостность.
5. Собрать журналы.
6. Синхронизировать.
7. Системный журнал.
8. Включить аварийный режим.
9. Отключить аварийный режим.
10. Сбросить блокировки.
11. Обновить.
12. Удаленное включение.

Примечание. Результат выполнения команд оперативного управления не отражается в Журналах ЕЦУ. Также не предусмотрены всплывающие и прочие уведомления о результатах выполнения команд оперативного управления.

6.2.2 Пользователи и группы для группы ДБ

Вкладка «Пользователи и группы» на уровне группы ДБ содержит списки глобальных учетных записей и групп пользователей группы ДБ.

Учетные записи группы ДБ

Категория «Пользователи» содержит список учетных записей пользователей группы ДБ (рис. 87).

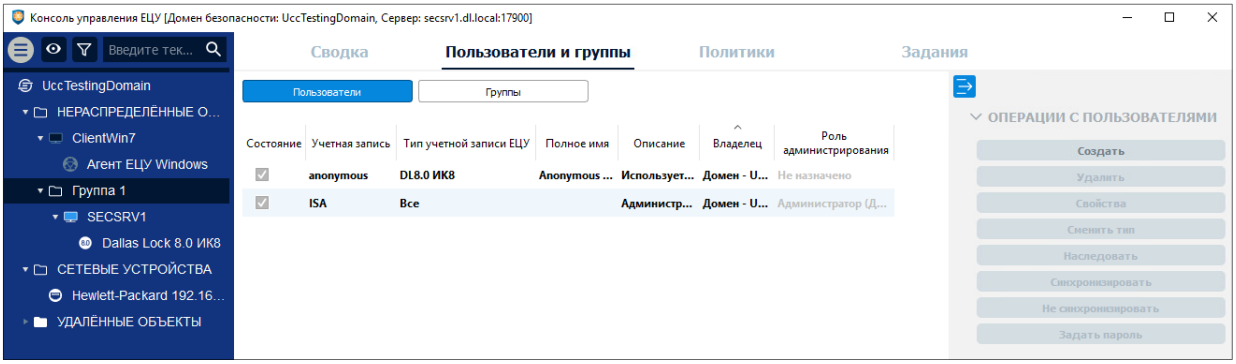

Рис. 87. Список учетных записей пользователей группы ДБ

Управление пользователями на уровне группы ДБ производится аналогично управлению пользователями для ДБ (см. «Параметры пользователей»).

Поле «Состояние» на уровне группы принимает следующий вид:

- ☑ — отмеченное флагом поле означает, что данная учетная запись пользователя имеет доступ на уровне группы ДБ, при этом «Состояние» задано (переопределено) на данном уровне дерева;
- ☑ — отмеченное флагом поле означает, что данная учетная запись пользователя имеет доступ на уровне группы ДБ, при этом «Состояние» наследуется с уровня выше в дереве;
- ☐ — пустое поле означает, что учетная запись отключена для работы на уровне группы ДБ, при этом «Состояние» задано (переопределено) на данном уровне дерева;
- ☐ — пустое поле означает, что учетная запись отключена для работы на уровне группы ДБ, при этом «Состояние» наследуется с уровня выше в дереве.

Примечание. Значение поля «Состояние» не отражает состояние учетной записи пользователей на вложенных в группу объектах. Например, учетная запись может быть отключена для работы на уровне группы (поле «Состояние» — пустое), но иметь доступ на уровне включенного в нее АРМ (стоит флаг в поле «Состояние»).

При этом, при изменении состояния учетной записи на уровне выше в дереве, состояние принудительно изменяется на вложенных объектах. Например, после отключения для работы учетной записи на уровне группы, работа учетной записи отключается для всех вложенных подгрупп, АРМ (модулей в составе АРМ) и модулей без АРМ.

На уровне группы ДБ в категории «Пользователи» на вкладке «Пользователи и группы» доступно:

- создание глобальных пользователей (см. «Создание пользователей ДБ», «Регистрация доменных пользователей в ДБ», «Регистрация доменных пользователей по маске»);
- удаление глобальных и доменных пользователей (см. «Удаление пользователей ДБ»);
- просмотр и настройка параметров глобальных и доменных пользователей (см. «Параметры пользователей»);
- смена типа учетной записи пользователя, в зависимости от того, для модулей какого типа применяется данная учетная запись пользователя;
- возможность выбора: «Синхронизировать» или «Не синхронизировать» учетную запись с модулями;
- смена пароля учетной записи пользователя (см. «Назначение пароля»).

Группы пользователей группы ДБ

Дополнительным инструментом управления правами учетных записей группы ДБ — «Группы». Этот инструмент функционирует аналогично «Локальным группам» в ОС семейства Windows и доступен в категории «Группы» на вкладке «Пользователи и группы» (рис. 88).

Рис. 88. Список групп пользователей группы ДБ

Управление группами пользователей на уровне группы ДБ производится аналогично управлению группами пользователей для ДБ (см. «Параметры групп пользователей»).

У модулей существует также свой список групп пользователей, в котором также можно выбрать необходимые для доступа к работе на модуле.

За данную функцию отвечает поле «Состояние». Поле «Состояние» на уровне группы домена безопасности принимает следующий вид:

- ☑ — отмеченное флагом поле означает, что данная группа пользователей имеет доступ на уровне группы ДБ, при этом «Состояние» задано (переопределено) на данном уровне дерева;
- ☑ — отмеченное флагом поле означает, что данная группа пользователей имеет доступ на уровне группы ДБ, при этом «Состояние» наследуется с уровня выше в дереве;
- ☐ — пустое поле означает, что группа пользователей отключена для работы на уровне группы ДБ, при этом «Состояние» задано (переопределено) на данном уровне дерева;
- ☐ — пустое поле означает, что группа пользователей отключена для работы на уровне группы ДБ, при этом «Состояние» наследуется с уровня выше в дереве.

Примечание. Значение поля «Состояние» не отражает состояние группы пользователей на вложенных в группу объектах. Например, учетная запись может быть отключена для работы на уровне группы (поле «Состояние» — пустое), но иметь доступ на уровне включенного в нее АРМ (стоит флаг в поле «Состояние»).

При этом, при изменении состояния группы пользователей на уровне выше в дереве, состояние принудительно изменяется на вложенных объектах. Например, после отключения для работы группы пользователей на уровне группы, работа группы пользователей отключается для всех вложенных подгрупп, АРМ (модулей в составе АРМ) и модулей без АРМ.

На уровне группы ДБ в категории «Группы» на вкладке «Пользователи и группы» доступны:

- создание глобальных групп пользователей (см. «Создание групп пользователей»);
- удаление глобальных групп пользователей (см. «Удаление групп пользователей»);
- просмотр и настройка параметров групп пользователей (см. «Параметры групп пользователей»);
- смена типа учетных записей группы, в зависимости от того, для модулей какого типа применяется данная группа пользователей;
- установка наследования с помощью параметра «Наследовать»;
- выбор: «Синхронизировать» или «Не синхронизировать» учетную запись с модулями;
- просмотр свойств групп.

6.2.3 Политики для группы ДБ

Вкладка «Политики» на уровне группы позволяет редактировать параметры безопасности на уровне группы (подгруппы) (рис. 89).

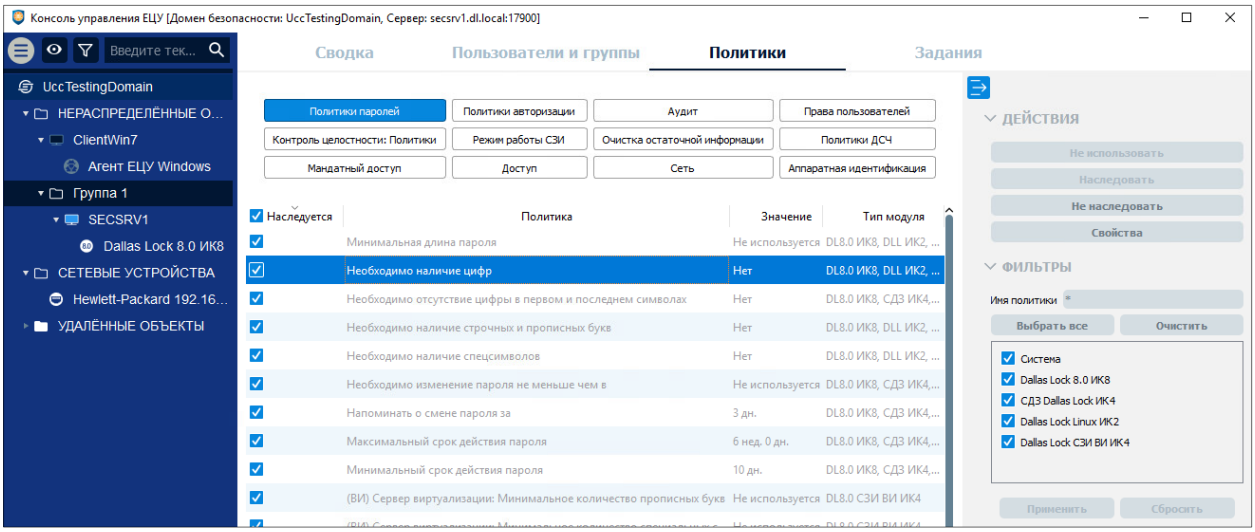

Рис. 89. Политики для групп Домена безопасности

Настройка политик для группы (подгруппы) производится аналогично настройке политик для ДБ (см. «Политики ДБ»). Для применения параметров на модулях необходима синхронизация.

Политики могут наследовать установленные настройки (от ДБ или от группы, в состав которой входит данная группа (подгруппа)) или принимать индивидуальные значения следующим образом:

1. Политики, для которых отмечено наследование, примут значения, установленные для родительского объекта в дереве объектов ЕЦУ: значения для ДБ или группы. В этом случае политики будут отображаться нечетким серым цветом.
2. Политики, для которых выбраны и установлены оригинальные настройки, будут отображаться четким черным цветом.

Для того, чтобы установить или снять наследование настроек, имеются следующие возможности:

1. Для того, чтобы все параметры наследовали значения, установленные для родительского объекта дерева, необходимо поставить флаг в поле «Наследуется» (рис. 90).

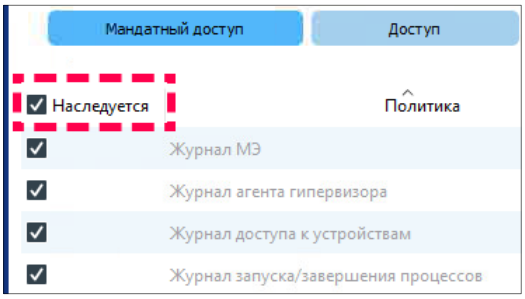

Рис. 90. Включение наследования политик объекта

2. Если снять флаг из поля «Наследуется», то все параметры одновременно станут обозначены как индивидуально настроенные (рис. 91).

Рис. 91. Выключение наследования политик объекта

3. Для отдельно выбранной политики имеется возможность выбрать оригинальное значение, сняв/поставив флаг в поле «Наследуется» в строке с данной политикой или изменив значение политики в редакторе.

Если часть политик наследуется, а часть имеет оригинальное значение, поле «Наследуется» имеет значение ▣.

6.2.4 Задания для группы ДБ

Вкладка «Задания» на уровне группы позволяет управлять заданиями на уровне группы (подгруппы) Домена безопасности (рис. 92).

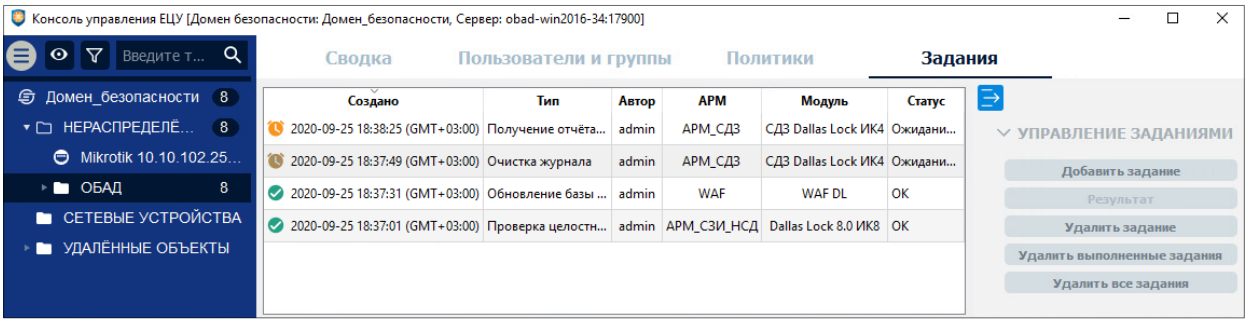

Рис. 92. Задания для групп Домена безопасности

Управление заданиями на уровне группы ДБ производится аналогично управлению заданиями для ДБ (см. «Задания ДБ»).

7 АРМ ДОМЕНА БЕЗОПАСНОСТИ ЕЦУ

В ЕЦУ Dallas Lock АРМ используется как способ представления совокупности нескольких модулей в качестве единой машины (рис. 93).

Рис. 93. АРМ в дереве ЕЦУ Dallas Lock

АРМ может включать в себя модули следующих типов:

- СЗИ Dallas Lock 8.0-K/C;
- СЗИ НСД Dallas Lock Linux;
- СДЗ Dallas Lock;
- СЗИ ВИ Dallas Lock;
- Агент ЕЦУ.

7.1 Настройка АРМ

Создать АРМ в Консоли ЕЦУ можно с помощью кнопки «Создать АРМ» на панели инструментов «Действия» или воспользовавшись контекстным меню в дереве ДБ. При создании АРМ потребуется ввести наименование, которое можно впоследствии изменить.

Перемещение АРМ в дереве осуществляется перетаскиванием значка кнопкой мыши в поле другого значка («Drag-and-drop»). Перемещение АРМ осуществляется со всеми вложенными модулями.

Удалить существующее АРМ можно с помощью кнопки «Удалить» на панели инструментов «Действия» или воспользовавшись контекстным меню в дереве ДБ. Удаление АРМ осуществляется со всеми вложенными объектами.

Каждое АРМ в дереве объектов содержит одинаковые вкладки для индивидуальной настройки параметров для модулей в составе данного АРМ.

7.1.1 Сводка АРМ

Вкладка «Сводка» для выбранного АРМ в дереве объектов отображает общее состояние модулей, входящих в АРМ (рис. 94).

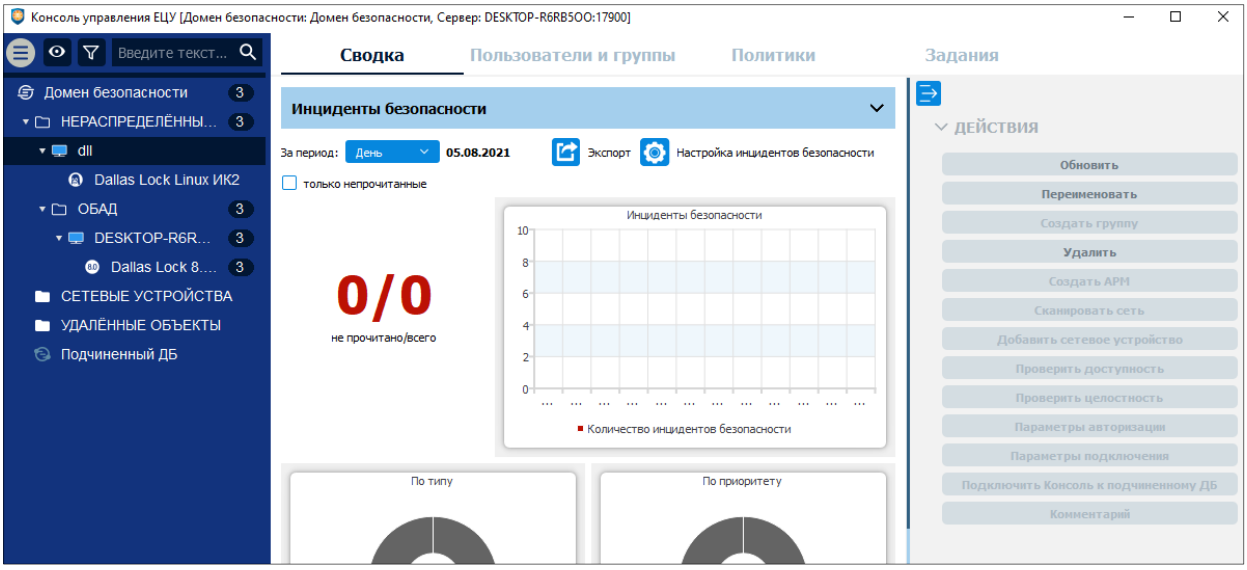

Рис. 94. Вкладка «Сводка» АРМ

На панели инструментов доступны следующие действия с АРМ:

1. Обновить.
2. Переименовать АРМ.
3. Удалить АРМ.

На панели инструментов доступны следующие команды оперативного управления для АРМ:

1. Выключить.
2. Перезагрузить.
3. Разблокировать пользователей.
4. Пересчитать целостность.
5. Собрать журналы.
6. Синхронизировать.
7. Удаленное управление.

Набор команд оперативного управления для каждого АРМ зависит от входящих в него модулей.

Примечание. Результат выполнения команд оперативного управления не отражается в Журналах ЕЦУ. Также не предусмотрены всплывающие и прочие уведомления о результатах выполнения команд оперативного управления.

7.1.2 Пользователи и группы АРМ

Вкладка «Пользователи и группы» для выбранного АРМ содержит списки глобальных и доменных учетных записей и групп пользователей АРМ (рис. 95).

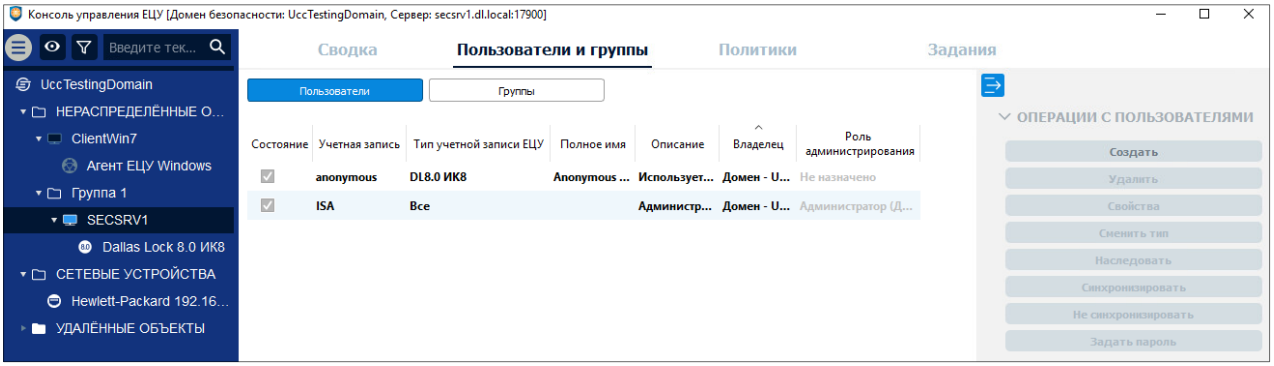

Рис. 95. Вкладка «Пользователи и группы» АРМ

Настройка пользователей для АРМ производится аналогично настройке пользователей и групп для группы ДБ (см. «Пользователи и группы для группы ДБ»). Для применения параметров на модулях необходима синхронизация.

7.1.3 Политики АРМ

Вкладка «Политики» для выбранного АРМ позволяет редактировать параметры безопасности на уровне АРМ (рис. 96).

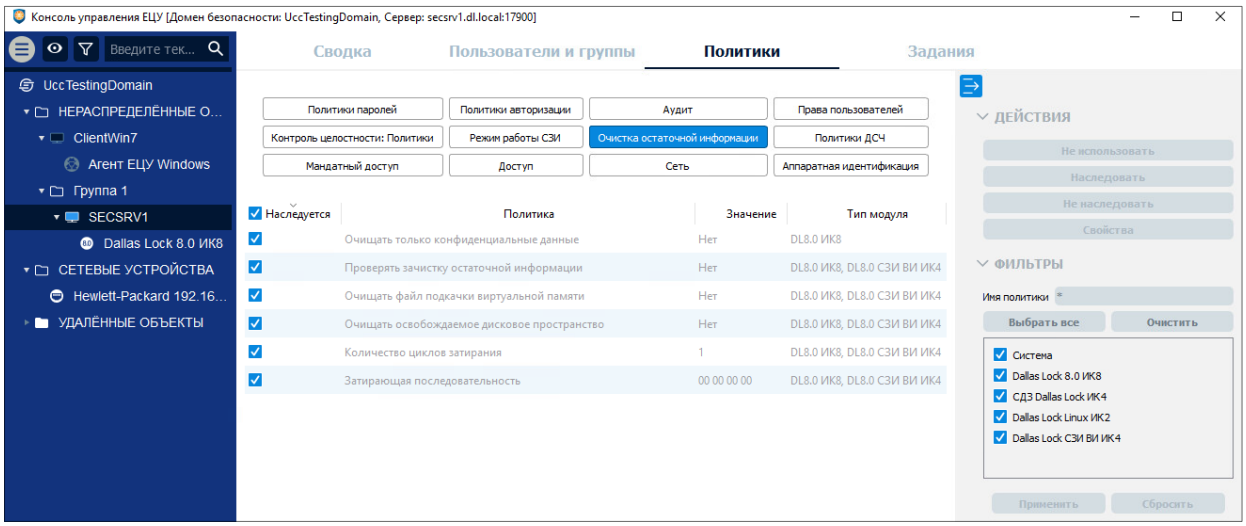

Рис. 96. Вкладка «Политики» АРМ

Настройка политик для АРМ производится аналогично настройке политик для группы ДБ (см. «Политики для группы ДБ»). Для применения параметров на модулях необходима синхронизация.

7.1.4 Задания АРМ

Вкладка «Задания» для выбранного АРМ позволяет управлять заданиями на уровне АРМ (рис. 97).

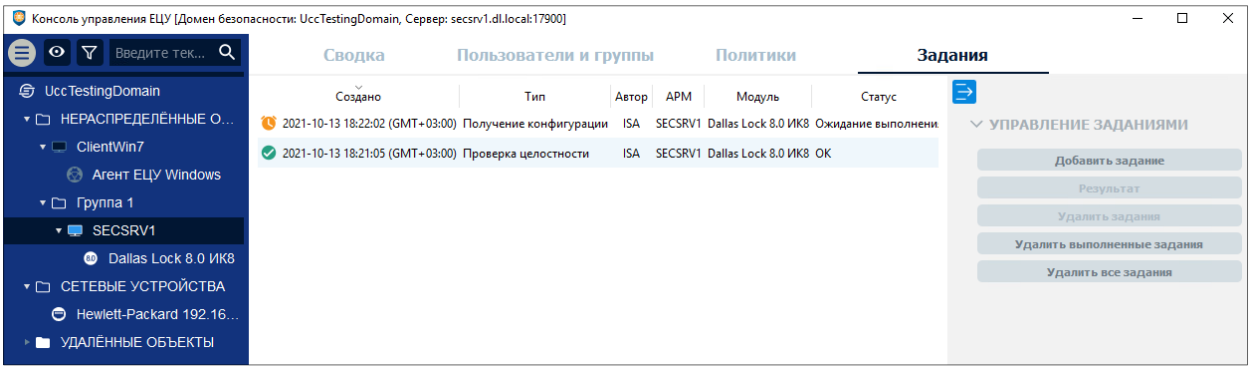

Рис. 97. Вкладка «Задания» АРМ

Управление заданиями на уровне АРМ производится аналогично управлению заданиями для ДБ (см. «Задания ДБ»).

8 МОДУЛИ ДОМЕНА БЕЗОПАСНОСТИ ЕЦУ

8.1 Настройка модуля

Для добавления нового модуля в Домен безопасности ЕЦУ путем сканирования диапазона сетевых адресов (данная функция доступна для модулей СЗИ Dallas Lock 8.0, СЗИ НСД Dallas Lock Linux, Агент ЕЦУ), необходимо:

1. На уровне Домена безопасности или группы (подгруппы) на вкладке «Сводка» на панели инструментов «Действия» нажать кнопку «Сканировать сеть» или воспользоваться контекстным меню в дереве ДБ.
2. Появится окно «Сканирование сети», в котором необходимо выбрать вкладку «Модуль», ввести диапазон IP-адресов для сканирования и нажать кнопку «Сканировать» (рис. 98).

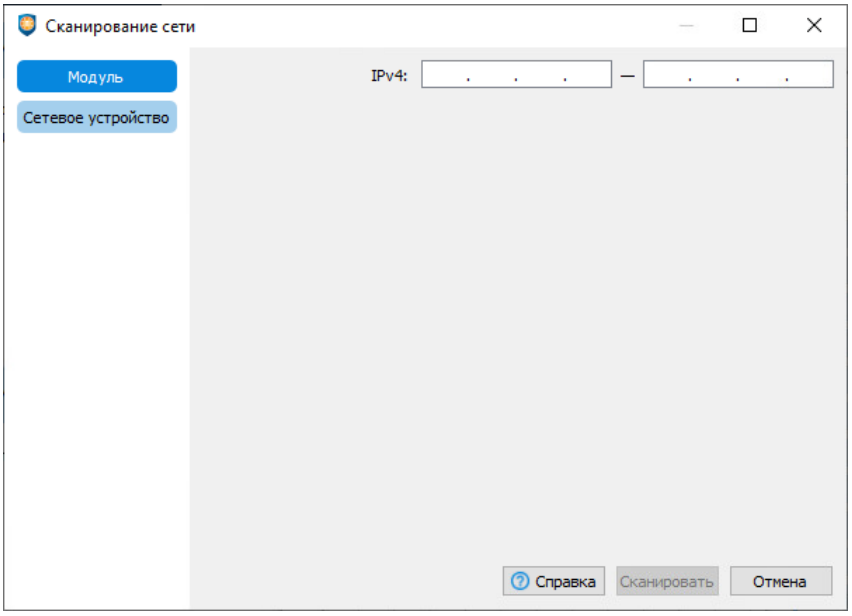

Рис. 98. Окно «Сканирование сети»

3. По завершению процесса сканирования из списка обнаруженных объектов можно выбрать те модули, которые необходимо зарегистрировать в ДБ, либо установить флаг возле столбца «АРМ», для выбора всех обнаруженных модулей (рис. 99).

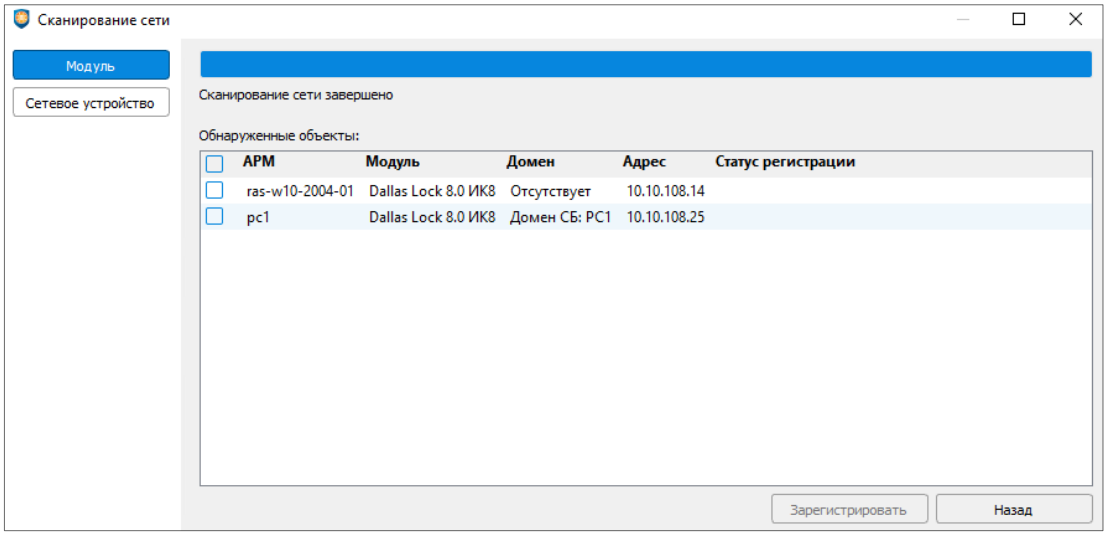

Рис. 99. Выбор объектов для регистрации в ДБ

После выбора регистрируемых модулей нажать кнопку «Зарегистрировать».

4. Появится окно «Регистрация модулей», в котором нужно ввести авторизационные данные администратора модуля и ключ доступа к ДБ (рис. 100).

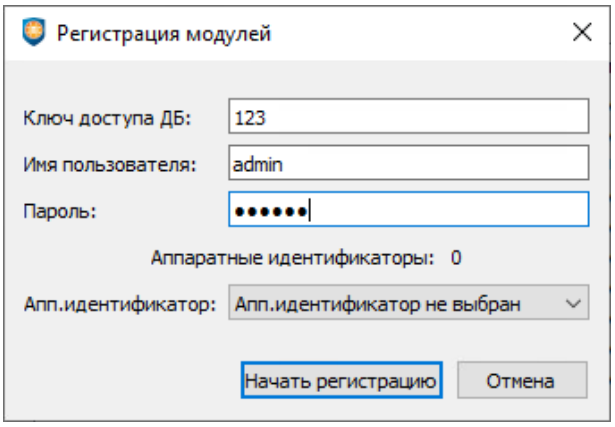

Рис. 100 Ввод данных для регистрации

Нажать кнопку «Начать регистрацию» после ввода всех данных.

5. Если введенные данные верны, то в статусе регистрации отобразится результат «ОК», и зарегистрированные модули появятся в дереве Домена безопасности в базовой группе «Нераспределенные объекты».

Примечание. Зарегистрировать модули в ДБ ЕЦУ получится, только при условии, что на АРМ, где установлены данные модули, настроено разрешающее правило фильтрации на TCP-порты 17901 и 17903 на входящее соединение.

Перемещение модуля в дереве осуществляется перетаскиванием значка кнопкой мыши в поле другого значка («Drag-and-drop»).

Имеется возможность добавить комментарий к модулю, для этого нужно нажать кнопку «Комментарий» на панели «Действия» или воспользоваться контекстным меню в дереве ДБ (рис. 101). Добавленный комментарий отобразится в разделе «Информация об объекте» вкладки «Сводка».

Примечание. Максимальная длина комментария к модулю составляет 256 символов.

Для вывода модуля из Домена безопасности ЕЦУ необходимо:

1. Выбрать пункт «Удалить модуль» из контекстного меню данного модуля в дереве ДБ (рис. 101), или воспользоваться командой «Удалить» на панели инструментов «Действия» вкладки «Сводка» на уровне модуля в дереве ДБ (рис. 102).

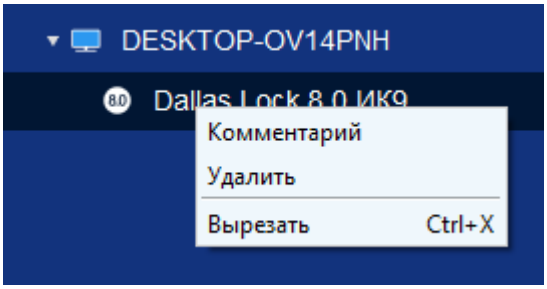

Рис. 101. Удаление модуля посредством контекстного меню

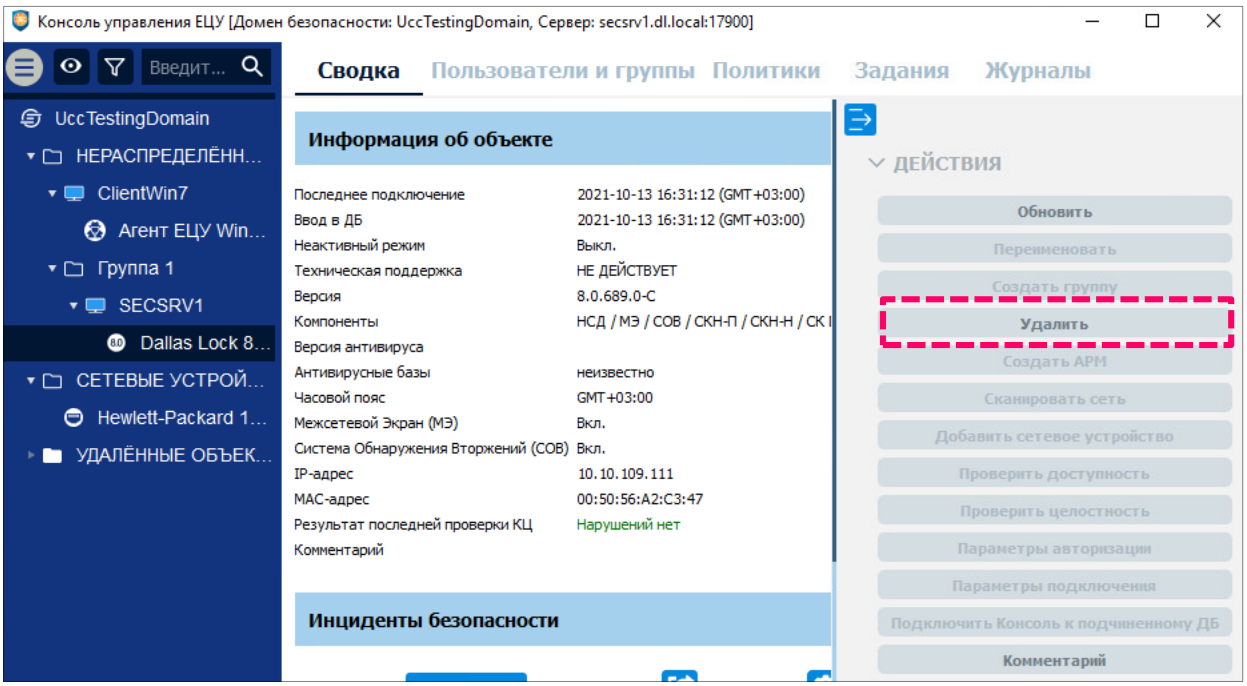

Рис. 102. Удаление посредством панели «Действия»

2. Удаленный модуль переместится в базовую группу «Удаленные объекты» дерева ДБ.
   Каждый модуль в дереве объектов содержит вкладки для индивидуальной настройки параметров в зависимости от его типа.

Примечание. В ЕЦУ реализована возможность работы с модулями, расположенными за NAT, в рамках одной сессии. Как только сессия завершится, связь с модулем разорвется. В следующий раз ЕЦУ сможет связаться с модулем, когда модуль создаст новую сессию.

8.1.1 Сводка модуля

Вкладка «Сводка» на уровне модуля отображает общее состояние модуля (рис. 103).

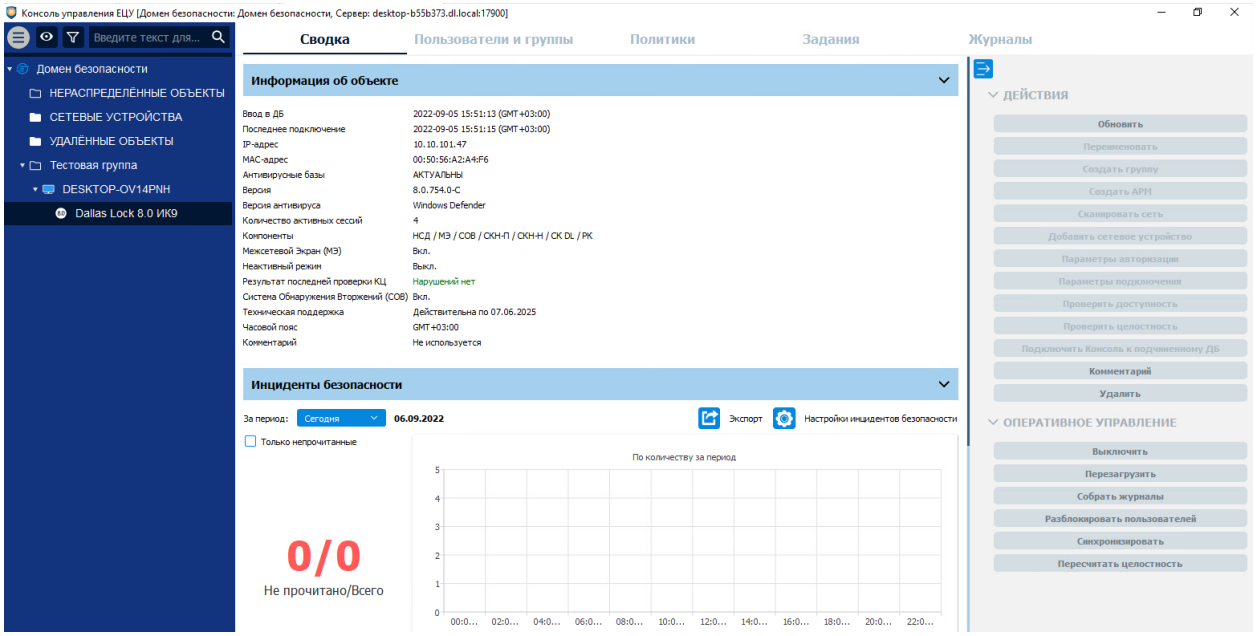

Рис. 103. Вкладка «Сводка» модуля

Вкладка сводка на уровне модуля включает в себя разделы:

- информация об объекте;
- инциденты безопасности.

Состав параметров, выводимых в разделе «Информация об объекте» зависит от типа модуля.

Информация в разделе «Инциденты безопасности» формируется по аналогии с остальными объектами дерева ДБ (см. «Инциденты безопасности»).

Состав команд оперативного управления зависит от типа модуля.

Примечание. Результат выполнения команд оперативного управления не отражается в Журналах ЕЦУ. Также не предусмотрены всплывающие и прочие уведомления о результатах выполнения команд оперативного управления.

8.1.2 Пользователи и группы модуля

Вкладка «Пользователи и группы» на уровне модуля содержит список глобальных и доменных пользователей и групп, наследуемых с уровней выше по иерархии и созданных на уровне данного модуля, а также модульных пользователей (рис. 104).

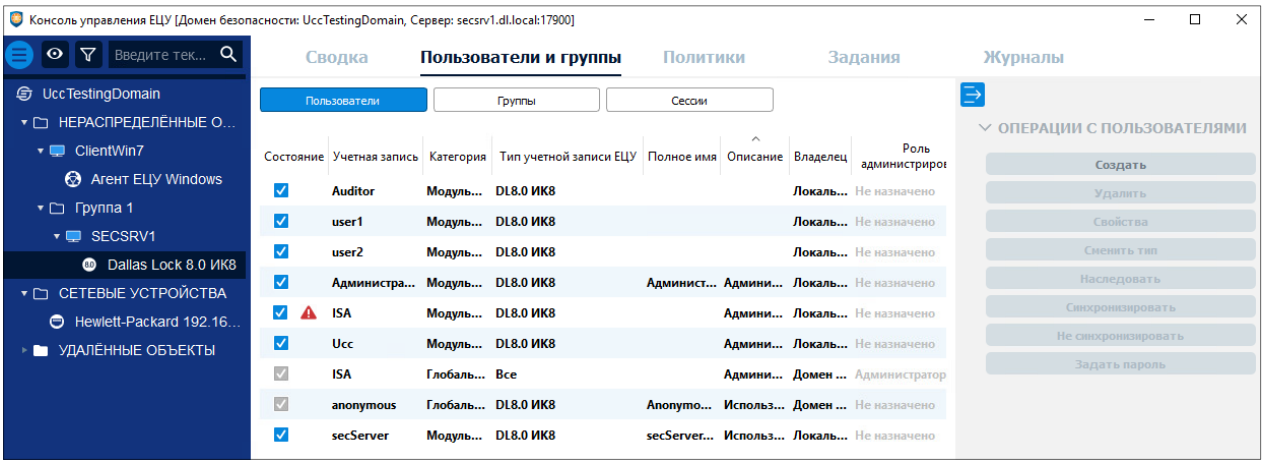

Рис. 104. Вкладка «Пользователи и групп» модуля

Управление глобальными и доменными пользователями и группами на уровне модуля производится аналогично управлению пользователями и группами на уровне группы домена безопасности (см. «Пользователи и группы для группы ДБ»).

Примечание. Глобальным учетным записям, создаваемым на уровне модуля, автоматически присваивается поле «Тип учетной записи ЕЦУ», соответствующий типу данного модуля.

Для пользователей и групп на уровне модуля поле «Категория» отображается в общем списке пользователей и групп. Поле «Категория» принимает значения «Глобальная» и «Модульная».

Изменить категорию пользователя или группы средствами консоли ЕЦУ нельзя.

Существующие до момента ввода в ДБ ЕЦУ на модуле пользователи и группы после ввода модуля под управление ЕЦУ регистрируются в качестве модульных пользователей и групп.

Имя модульного пользователя или название модульной группы может совпадать с именем существующих в домене безопасности глобальных и доменных пользователей и групп. В таком случае приоритет при синхронизации будет иметь модульный пользователь или группа соответственно. Приоритет при синхронизации подразумевает, что такой пользователь или группа будут переданы на модуль с параметрами, настроенными для модульного пользователя или группы соответственно. В интерфейсе консоли ЕЦУ такие модульные учетные записи и группы выделены значком (рис. 105).

Рис. 105. Совпадение имен модульного и глобального пользователя

Примечание. После вывода модуля из ДБ все группы и пользователи остаются в списках на модуле. При повторном вводе модуля в ДБ такие пользователи и группы будут зарегистрированы в ЕЦУ с категорией «Модульная» и будут иметь приоритет при синхронизации.

Для модульных пользователей не может быть назначена роль на администрирование ДБ.

Модульные учетные записи могут быть включены в глобальные группы пользователей.

Для применения параметров на модуле необходима синхронизация.

8.1.3 Политики модуля

Вкладка «Политики» для выбранного модуля позволяет редактировать параметры безопасности на уровне модуля (рис. 106).

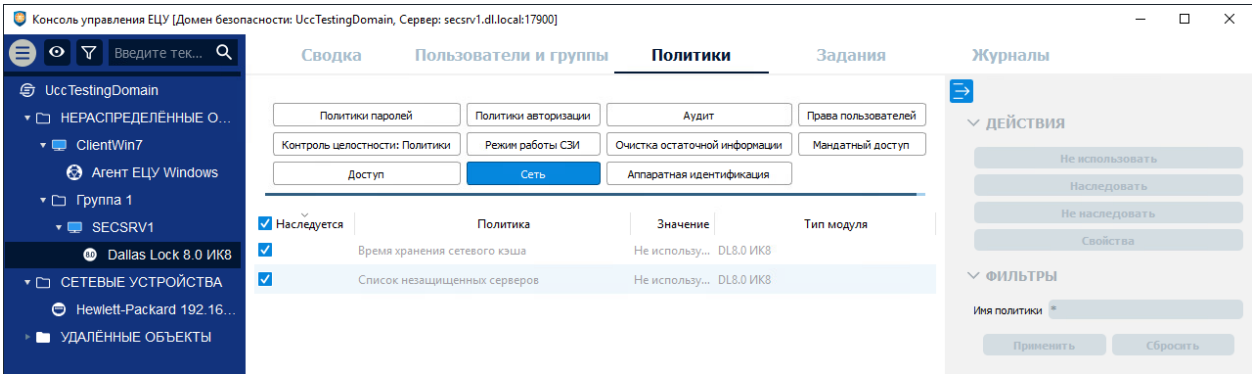

Рис. 106. Вкладка «Политики» модуля

На уровне модуля в списке доступны только политики, актуальные для данного типа модуля ЕЦУ.

Настройка политик для модуля производится аналогично настройке политик для группы ДБ (см. «Политики для группы ДБ»).

Для применения параметров на модулях необходима синхронизация.

8.1.4 Задания модуля

Вкладка «Задания» на уровне модуля позволяет управлять заданиями для модуля (рис. 107).

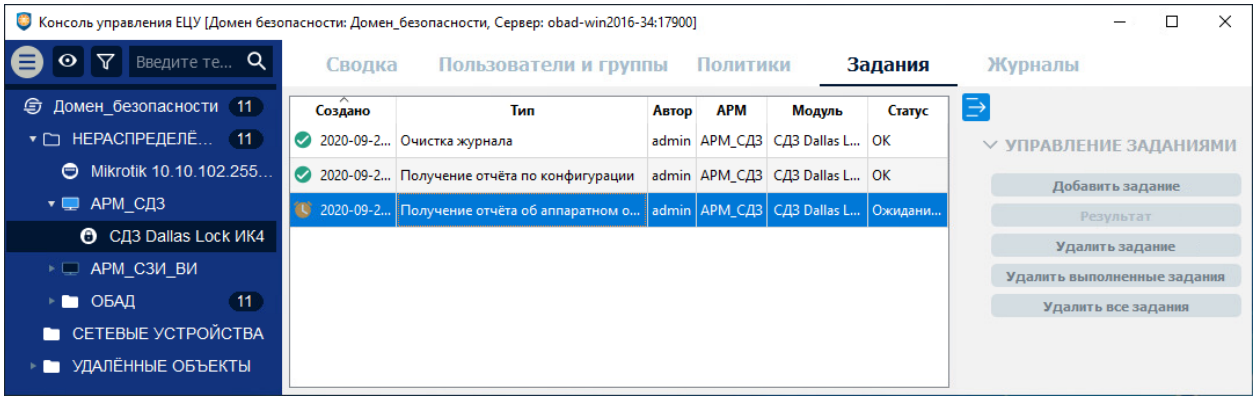

Рис. 107. Вкладка «Задания» модуля

На уровне модуля доступны задания, актуальные для данного типа модуля ЕЦУ.

Управление заданиями на уровне модуля производится аналогично управлению заданиями для ДБ (см. «Задания ДБ»).

8.1.5 Журналы модуля

Вкладка «Журналы» для выбранного модуля позволяет просматривать журналы безопасности модуля (рис. 108).

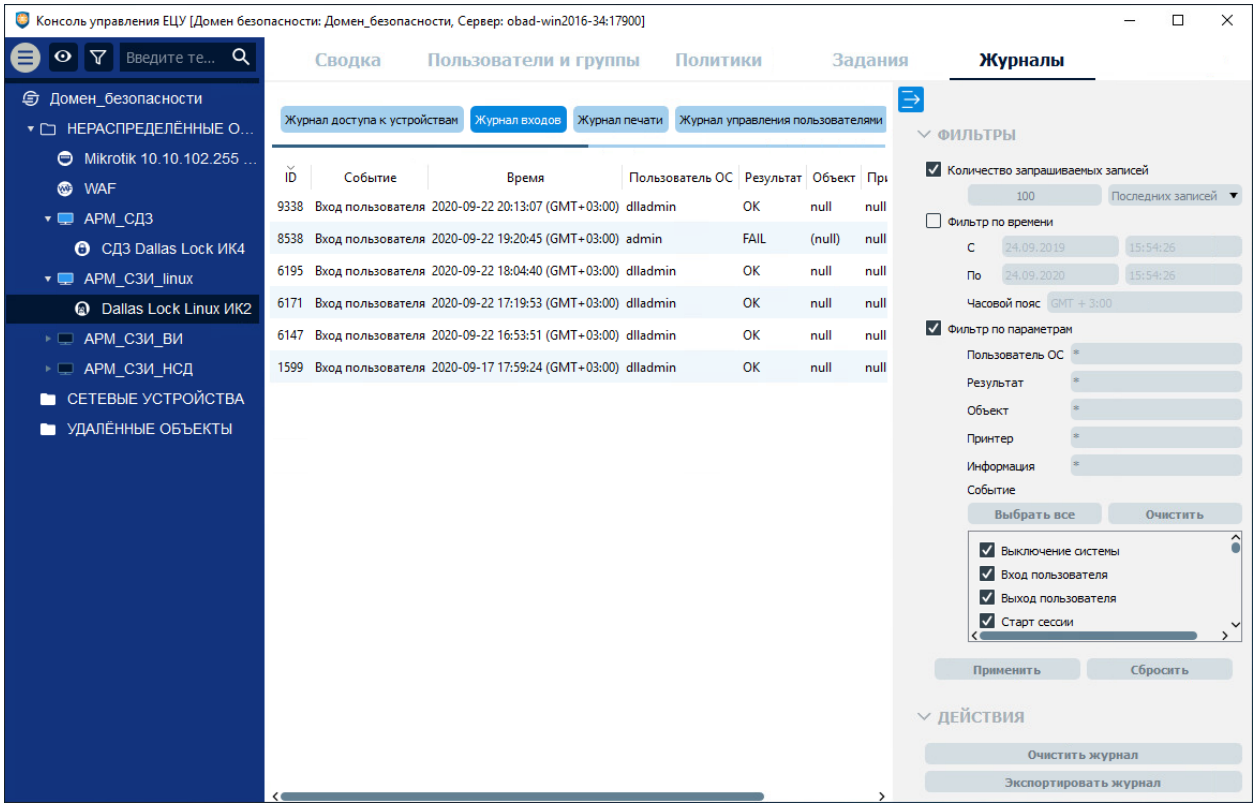

Рис. 108. Вкладка «Журналы» модуля

Категории журналов на вкладке соответствуют названиям журналов на модулях.

Справа расположены панель инструментов «Фильтры» и панель инструментов «Действия».

Параметры фильтрации зависят от категории журнала. Сброс и применение выбранных фильтров осуществляется по команде «Сбросить» и «Применить» соответственно.

Отфильтрованные записи журнала можно сохранить в выбранную папку в нужном типе файла (TXT, CSV), с помощью команды «Экспортировать журнал» на панели инструментов «Действия».

Для очистки журнала модуля используется команда «Очистить журнал».

9 МОДУЛЬ СЗИ DALLAS LOCK 8.0-C/K

9.1 Ввод модуля в ДБ

Ввести модуль СЗИ Dallas Lock 8.0 в Домен безопасности можно следующими способами:

- в процессе установки СЗИ Dallas Lock 8.0;
- через оболочку администратора СЗИ Dallas Lock 8.0;
- с помощью консоли ЕЦУ (см. «Настройка модуля»).

Внимание! При вводе модуля СЗИ Dallas Lock 8.0 в ДБ должен быть соблюден ряд условий:

- в ЛВС должен быть работающий сервер ЕЦУ;
- между модулем и сервером ЕЦУ должен быть свободный обмен пакетами по TCP/IP порту 17900.

Внимание! После ввода модуля СЗИ Dallas Lock 8.0 под управление ЕЦУ значения параметров безопасности подлежат синхронизации со значениями политик ЕЦУ для базовой группы «Нераспределенные объекты».

9.1.1 Ввод модуля в ДБ в процессе установки Dallas Lock 8.0

В процессе установки Dallas Lock 8.0 в окне ввода параметров присутствуют поля для ввода модуля в ДБ на данном этапе (рис. 109).

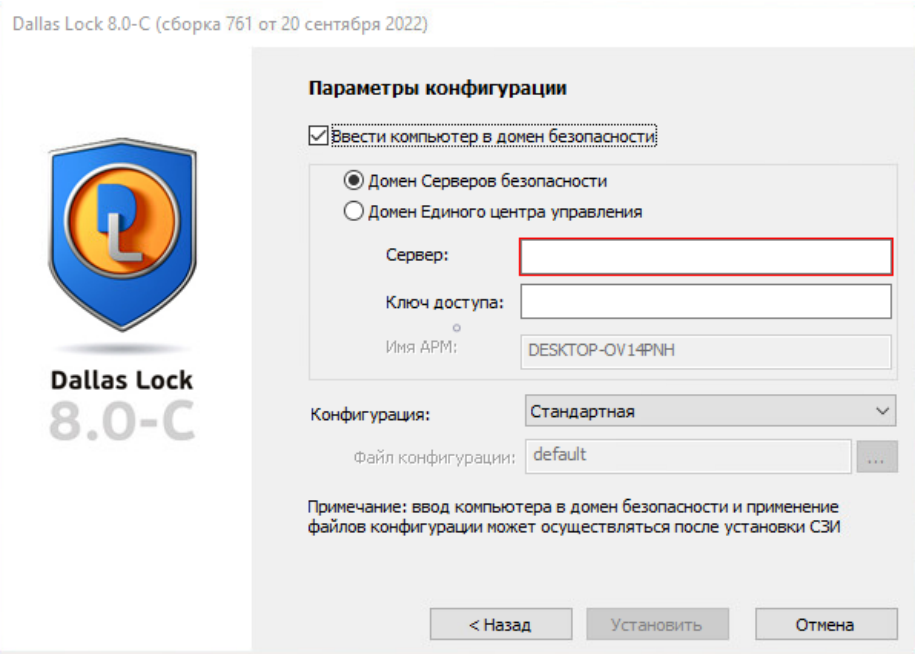

Рис. 109. Параметры установки системы защиты

Необходимо поставить флаг «Ввести компьютер в домен безопасности». Далее, необходимо выбрать пункт «Домен Единого центра управления». В соответствующие поля необходимо ввести имя сервера ЕЦУ, ключ доступа к ДБ и имя АРМ, в составе которого необходимо ввести модуль, и нажать кнопку «Далее». Если имя сервера ЕЦУ введено неверно, то по завершению установки СЗИ в области уведомлений появится сообщение об ошибке ввода компьютера в Домен безопасности (рис. 110).

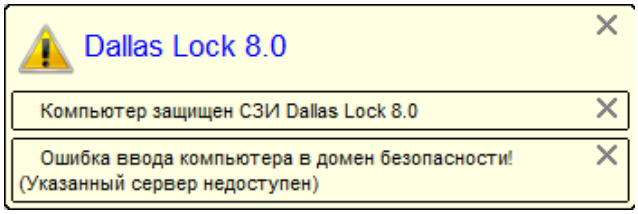

Рис. 110. Ошибка ввода компьютера в ДБ

Если процесс ввода модуля в ДБ прошел успешно, то в дереве объектов Домена безопасности в группе «Нераспределенные объекты» появится новый АРМ с указанным именем, в котором зарегистрирован модуль СЗИ Dallas Lock 8.0.

9.1.2 Ввод установленного модуля Dallas Lock 8.0 в ДБ

Для ввода модуля в ДБ через оболочку администратора необходимо:

1. Убедиться, что сервер ЕЦУ доступен по сети.
2. Запустить оболочку администратора Dallas Lock 8.0 на модуле.
3. Открыть вкладку «Параметры безопасности» → категория «Вход». Выбрать параметр «Домен безопасности» и нажать на «Свойства» панели «Действия». Откроется окно «Настройки домена безопасности» (рис. 111).

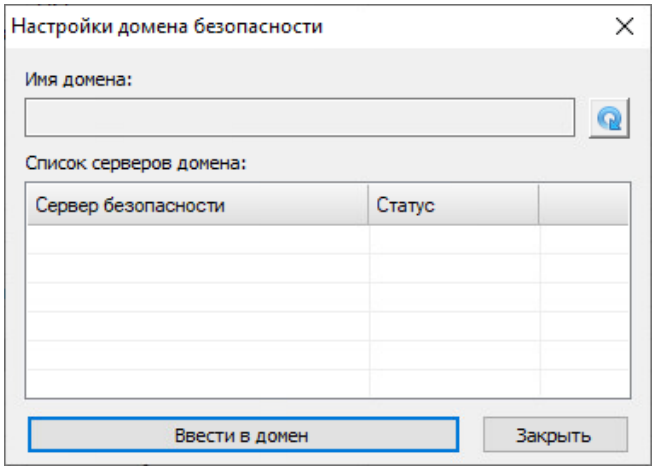

Рис. 111. Настройки ДБ

4. Нажать кнопку «Ввести в домен». Откроется окно ввода клиента в домен безопасности (рис. 112), где необходимо:
   - выбрать пункт «Домен Единого центра управления»;
   - ввести имя сервера ЕЦУ;
   - указать ключ доступа к данному ДБ;
   - указать имя АРМ, в составе которого необходимо ввести модуль.

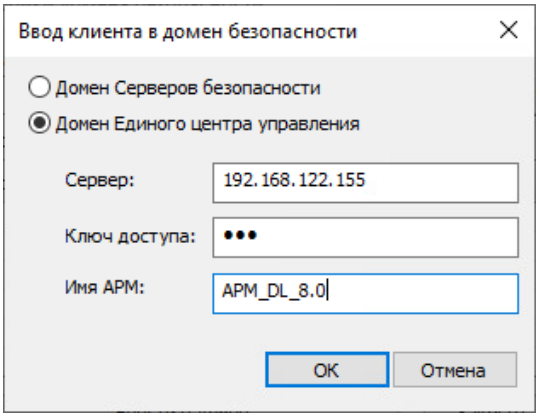

Рис. 112. Ввод компьютера в ДБ ЕЦУ

Далее необходимо нажать кнопку «ОК», и, в случае успеха, через некоторое время появится сообщение о том, что модуль успешно введен в ДБ (рис. 113).

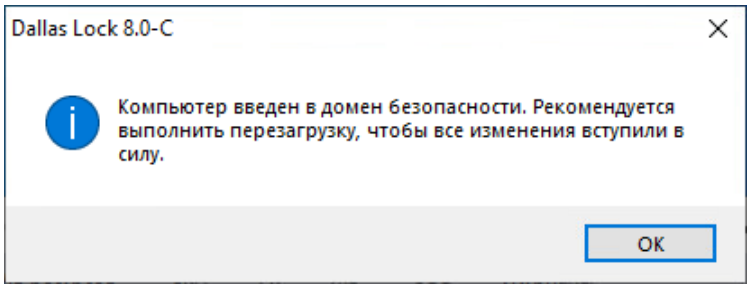

Рис. 113. Сообщение об успешном вводе модуля в ДБ

5. Перезагрузить ПК для подключения и синхронизации модуля с ДБ.

В дереве объектов Домена безопасности в группе «Нераспределенные объекты» появится новый АРМ с указанным именем, в котором зарегистрирован модуль СЗИ Dallas Lock 8.0.

9.2 Вывод модуля из ДБ

Вывести модуль СЗИ Dallas Lock 8.0 из Домена безопасности можно следующими способами:

- с помощью консоли ЕЦУ (см. «Настройка модуля»);
- через оболочку администратора СЗИ Dallas Lock 8.0.

Для вывода модуля через оболочку администрирования необходимо:

1. Запустить оболочку администрирования на модуле.

2. Открыть вкладку «Параметры безопасности» → категория «Вход». Выбрать параметр «Домен безопасности» и нажать на «Свойства» панели «Действия». Откроется окно «Настройки домена безопасности» (рис. 114).

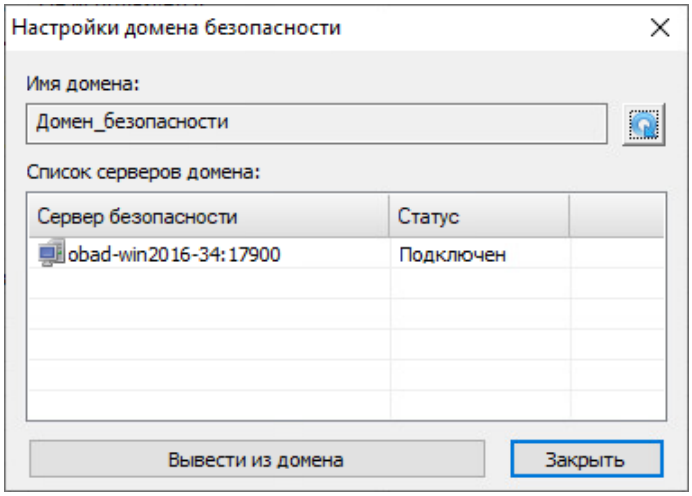

Рис. 114. Настройки ДБ

3. Нажать «Вывести из домена». Откроется окно для подтверждения вывода модуля из ДБ (рис. 115).

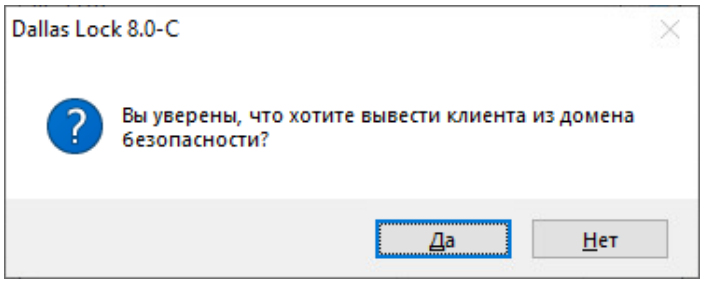

Рис. 115. Вывод модуля из ДБ

4. Нажать «Да». Появится сообщение о том, что модуль успешно выведен из ДБ (рис. 116).

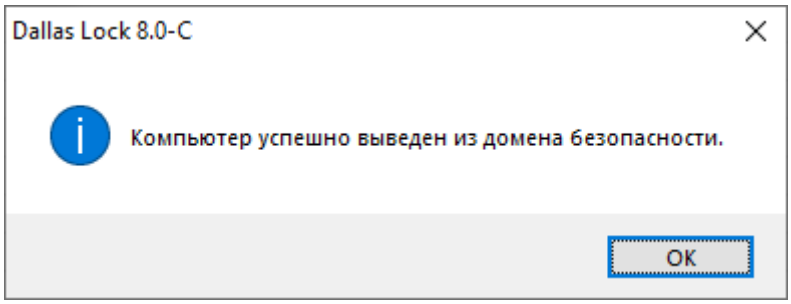

Рис. 116. Сообщение об успешном выводе модуля из ДБ

В консоли ЕЦУ удаленный модуль переместится в базовую группу «Удаленные объекты» дерева ДБ.

Примечание. При отсутствии сетевого подключения к Службе ЕЦУ, модуль может быть выведен из Домена безопасности ЕЦУ принудительно. При этом, в Консоли ЕЦУ такой модуль продолжит отображаться, но его статус будет «Недоступен».

Поэтому, каждый модуль, выведенный из состава ДБ во время отсутствия связи со Службой ЕЦУ, необходимо дополнительно удалять вручную из Консоли ЕЦУ.

9.3 Удаленное развертывание СЗИ Dallas Lock 8.0

Существует возможность выполнить установку или удаление Dallas Lock 8.0 централизованно на один или несколько компьютеров, расположенных в одной ЛВС.

Удаленная установка возможна в следующих вариантах:

- централизованно — для группы компьютеров, имеющих одинаковые имена и пароли администратора ОС;
- для компьютеров, имеющих индивидуальные имя и пароль администратора ОС, удаленную установку следует выполнять отдельно от других.

9.3.1 Удаленное развертывание с помощью консоли ЕЦУ

Примечание. По умолчанию в операционных системах начиная с Windows 7 доступ к удаленному компьютеру под локальной учетной записью запрещен. Подробную информацию об этом ограничении можно найти на официальном сайте Справки и поддержки компании Microsoft по адресу https://support.microsoft.com/kb/951016 (на английском языке).

Для разрешения удаленного подключения под локальной учетной записью необходимо в редакторе реестра по пути HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System создать ключ типа dword с именем LocalAccountTokenFilterPolicy со значением «1» («LocalAccountTokenFilterPolicy»=dword:00000001) и перезагрузить компьютер. В крупных сетях с AD данное значение можно распространить через политики.

Внимание! По умолчанию удаленное развертывание выполняется через порт 445. Для этого на целевых ТС в Брандмауэре Windows необходимо разрешить входящие подключения для порта 445.

Внимание! Для нескольких целевых ТС централизованную удаленную установку можно осуществить только при выполнении следующих условий:

- целевые ТС входят в тот же домен AD или LDAP, что и АРМ с ЕЦУ Dallas Lock;
- известны имя пользователя и пароль доменной учетной записи с правами администратора домена.

Внимание! Для ввода клиента в домен безопасности ЕЦУ в поле определения домена указывается имя пользователя и домен, в связи с чем на клиенте СЗИ НСД Dallas Lock 8.0 не допускается наличие пробела в имени пользователя ОС.

Внимание! На клиенте СЗИ НСД Dallas Lock 8.0 не поддерживаются полные имена домена — не допускается наличие точки в имени домена. При необходимости указании доменного логина в мастере разворачивания DL8.0 используйте запись вида *domain\user*.

Для удаленной установки СЗИ НСД Dallas Lock 8.0, необходимо выполнить следующие шаги:

1. Перед централизованной установкой необходимо разместить на компьютере, на котором запущена консоль ЕЦУ, дистрибутив СЗИ НСД Dallas Lock 8.0.
2. Запустить консоль ЕЦУ от имени администратора.
3. Далее необходимо открыть главное меню консоли ЕЦУ → «Утилиты» → «Удаленное развертывание DL 8.0».

В открывшемся окне необходимо добавить целевые ТС для удаленного развертывания. ТС можно добавить одним из следующих способов, через:

- ручной ввод адреса — для этого нужно заполнить поля «Порт» и «Введите IP-адрес или сетевое имя компьютера», затем нажать кнопку «Добавить компьютер» (рис. 117);
- импорт из файла — нажать «Импорт из файла» и прикрепить текстовый файл со списком IP-адресов целевых ТС.

Примечание. Для файла с IP-адресами возможен следующий формат списка: в каждой строке файла может быть указан только один IP-адрес без дополнительных символов. Пример:

192.168.0.1
192.168.0.35
10.10.112.55

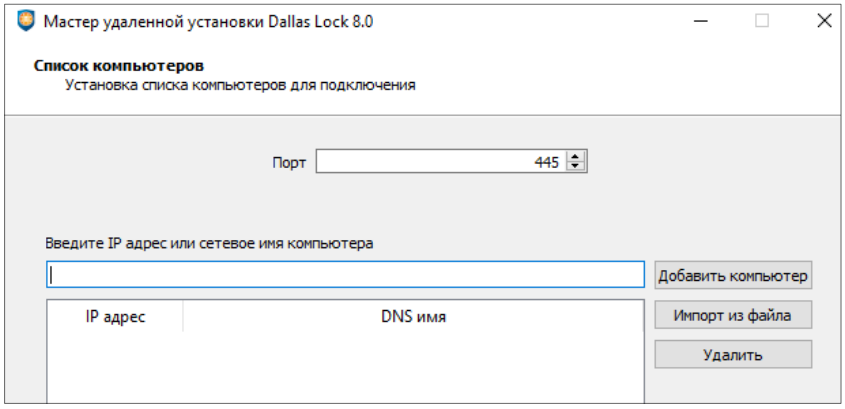

Рис. 117. Список целевых ТС для удаленного развертывания СЗИ НСД Dallas Lock 8.0

Кнопка «Удалить» необходима для удаления добавленных ранее IP-адресов.

После добавления целевых ТС в список, необходимо нажать кнопку «Далее».

4. Заполнить параметры установки, которые будут применены к модулям в процессе активации СЗИ НСД Dallas Lock 8.0 (рис. 118):
   - логин и пароль администратора ОС на целевых ТС;
   - логин и пароль суперпользователя (опционально).

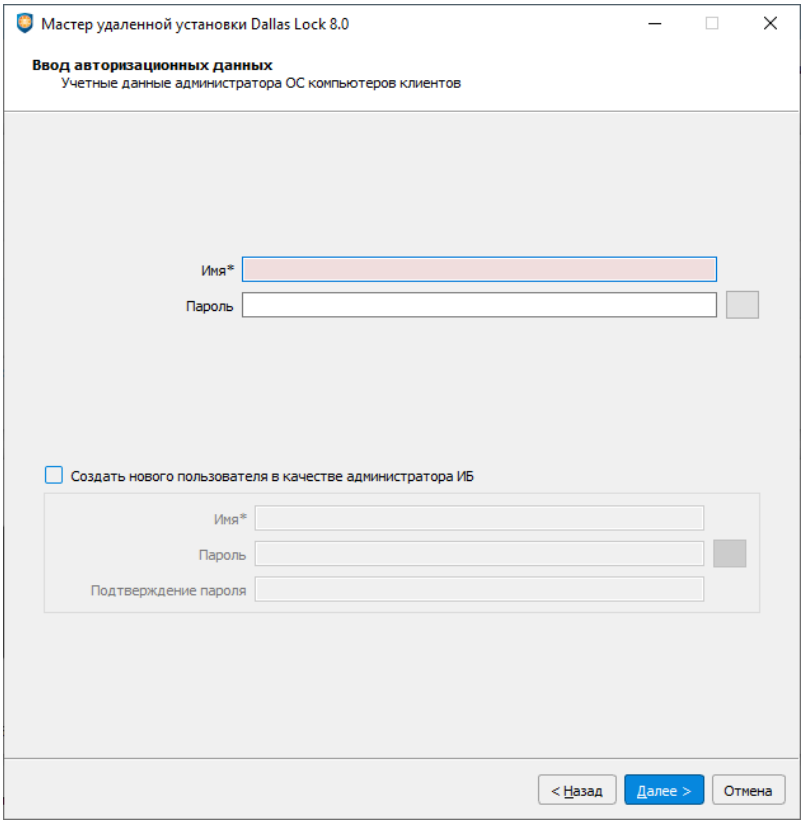

Рис. 118. Параметры установки СЗИ НСД Dallas Lock 8.0

После заполнения всех необходимых полей нужно нажать кнопку «Далее».

5. В следующем окне (рис. 119) необходимо указать:

- путь к исходному дистрибутиву СЗИ НСД Dallas Lock 8.0;
- номер лицензии, который указан на обложке футляра;
- код технической поддержки, который указан в письме, отправленном на электронную почту.

При необходимости применения определенной конфигурации для дистрибутива, можно поставить флаг «Сохранять настройки от предыдущей установки» или указать путь к файлу конфигурации для СЗИ Dallas Lock 8.0. Если поле не отмечено флагом и не указан путь к файлу конфигурации, применяется конфигурация «По умолчанию», что имеет смысл только при обновлении.

Для ввода модулей в Домен безопасности ЕЦУ сразу после установки, можно поставить флаг «Ввод в домен безопасности ЕЦУ», указать имя сервера ЕЦУ и ключ доступа к ДБ. Затем нажать «Далее».

Если данные для ввода модуля в ДБ ЕЦУ (в том числе ключ доступа) были указаны неверно, то установка будет приостановлена. Кнопка «Далее» будет неактивна до тех пор, пока данные для ввода в ДБ ЕЦУ не будут введены верно. Чтобы продолжить установку без ввода модуля в ДБ ЕЦУ необходимо снять флаг «Ввод в домен безопасности ЕЦУ».

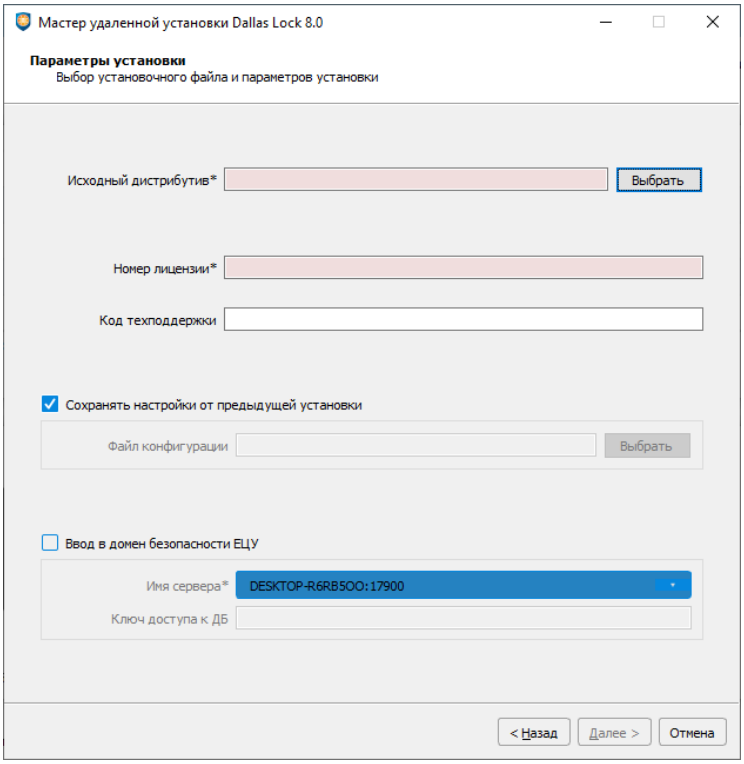

Рис. 119. Выбор установочного файла СЗИ НСД Dallas Lock 8.0

6. В следующем окне (рис. 120) можно настроить дополнительные параметры установки, такие как:

- перезагрузка удаленного компьютера после установки. Поставленный в окне флаг позволяет автоматически перезагрузить компьютер после завершения установки СЗИ Dallas Lock 8.0 по истечению установленного времени, иначе компьютер должен быть перезагружен пользователем самостоятельно;
- сообщение для пользователей. Сообщение, указанное в данном окне, будет повторяться с заданным интервалом, для пользователей, на чьих компьютерах производится установка СЗИ Dallas Lock 8.0.

Затем нажать кнопку «Установить».

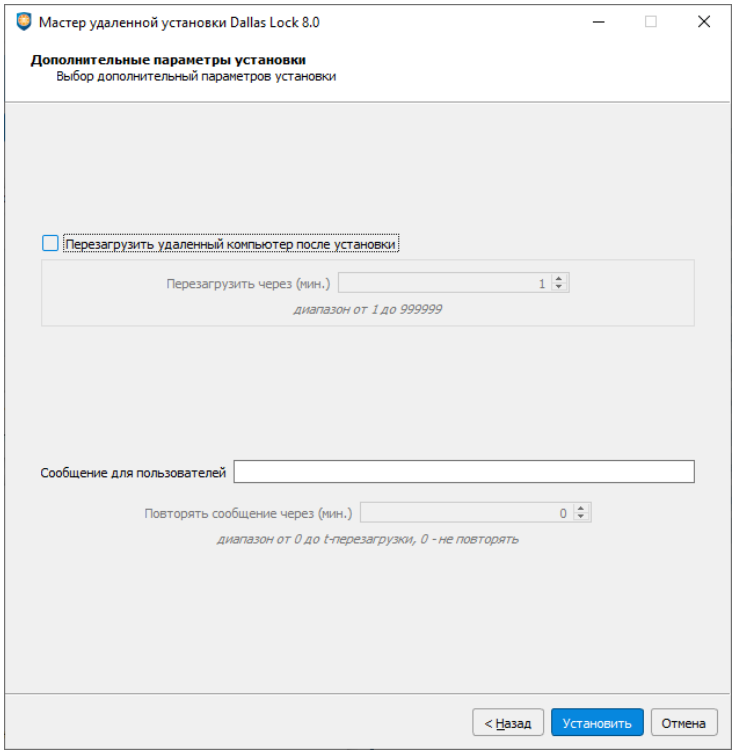

Рис. 120. Дополнительные параметры установки СЗИ НСД Dallas Lock 8.0

7. Далее можно просматривать состояние процесса установки для каждого клиента (рис. 121).

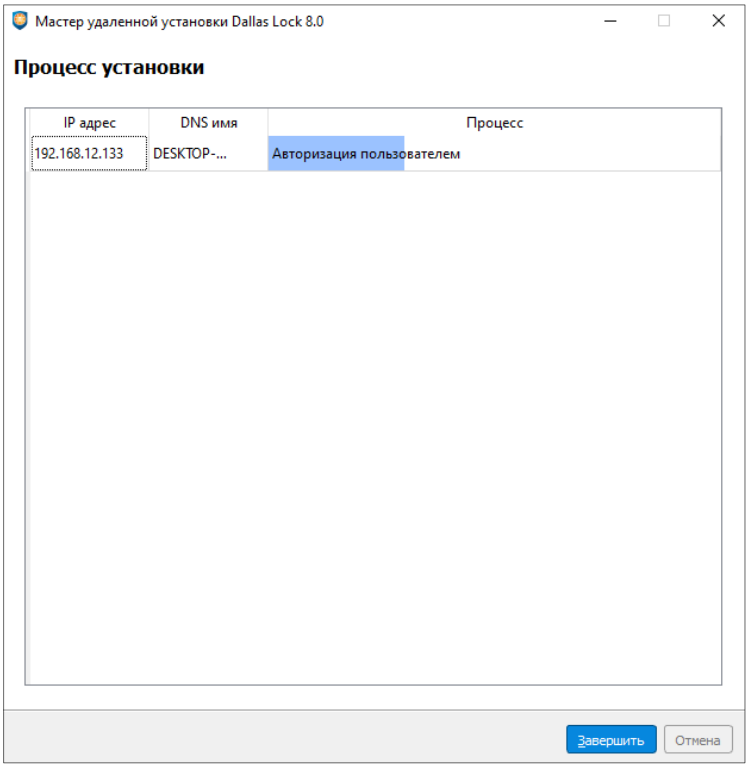

Рис. 121. Информация о ходе централизованной установки средствами ЕЦУ

8. По окончанию процесса централизованной установки появятся соответствующие комментарии удачного или не удачного завершения операции.

9.3.2 Централизованная установка средствами Active Directory

Средствами Microsoft Windows возможна централизованная установка Dallas Lock 8.0 на рабочие станции, входящие в состав Контроллера домена. Необходимые для установки действия включают в себя:

- Формирование файла установки в консоли ЕЦУ.
- Создание точки распространения на Контроллере домена.
- Создание объекта групповой политики для централизованной установки средствами AD.
- Конфигурация и применение групповой политики.

9.3.2.1 Подготовка msi-дистрибутива DL8.0 для AD

В ЕЦУ существует возможность подготовить дистрибутив СЗИ Dallas Lock 8.0 для установки средствами Active Directory.

Перед началом подготовки дистрибутива необходимо на компьютере, на котором запущена консоль ЕЦУ, разместить дистрибутив СЗИ Dallas Lock 8.0.

Примечание. Возможность создания дистрибутива СЗИ Dallas Lock 8.0 для установки средствами Active Directory в консоли запущенной под ОС Linux заблокирована. Создание дистрибутива возможно только под ОС Windows.

Для выполнения подготовки дистрибутива необходимо открыть главное меню консоли ЕЦУ → «Утилиты» → «Подготовить дистрибутив DL8.0 для AD». Появится окно «Мастер подготовки дистрибутива Dallas Lock 8.0 для Active Directory» (рис. 122).

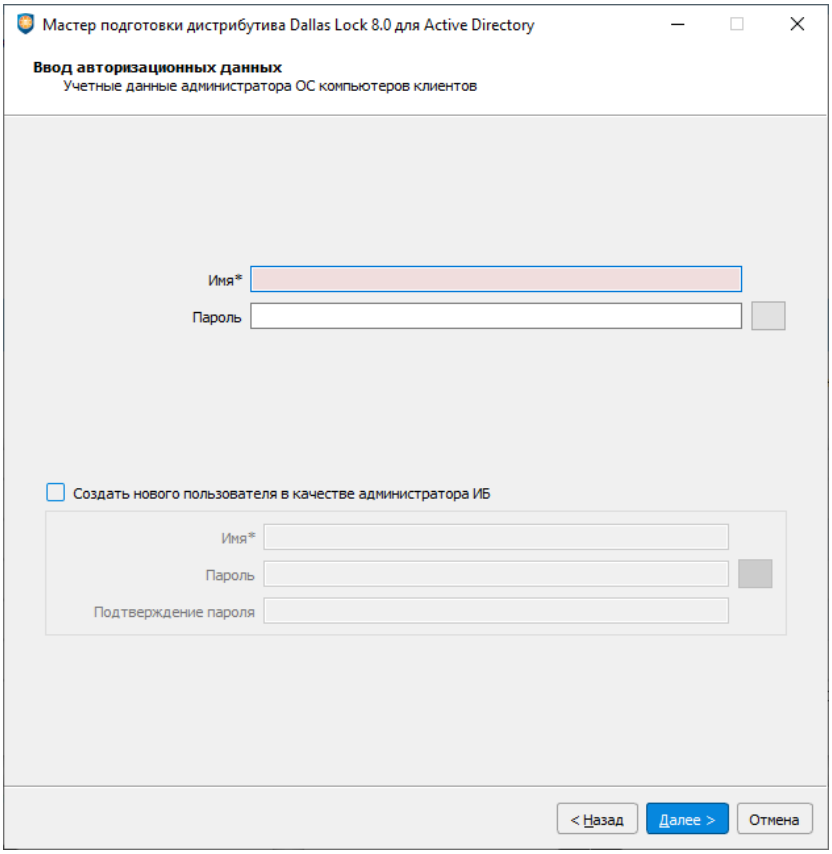

Рис. 122. Начало подготовки дистрибутива СЗИ Dallas Lock 8.0 для AD

В окне обязательно указать учетные данные администратора ОС компьютеров клиентов.

Также существует возможность поставить флаг «Создать нового пользователя в качестве администратора ИБ», задать имя учетной записи администратора информационной безопасности

и пароль для нее. В результате будет принудительно создана учетная запись пользователя, которая будет выступать в роли суперадминистратора после установки (обновления) СЗИ Dallas Lock 8.0.

После заполнения всех обязательных полей в правом нижнем углу станет доступна кнопка «Далее» для перехода к следующему шагу подготовки дистрибутива.

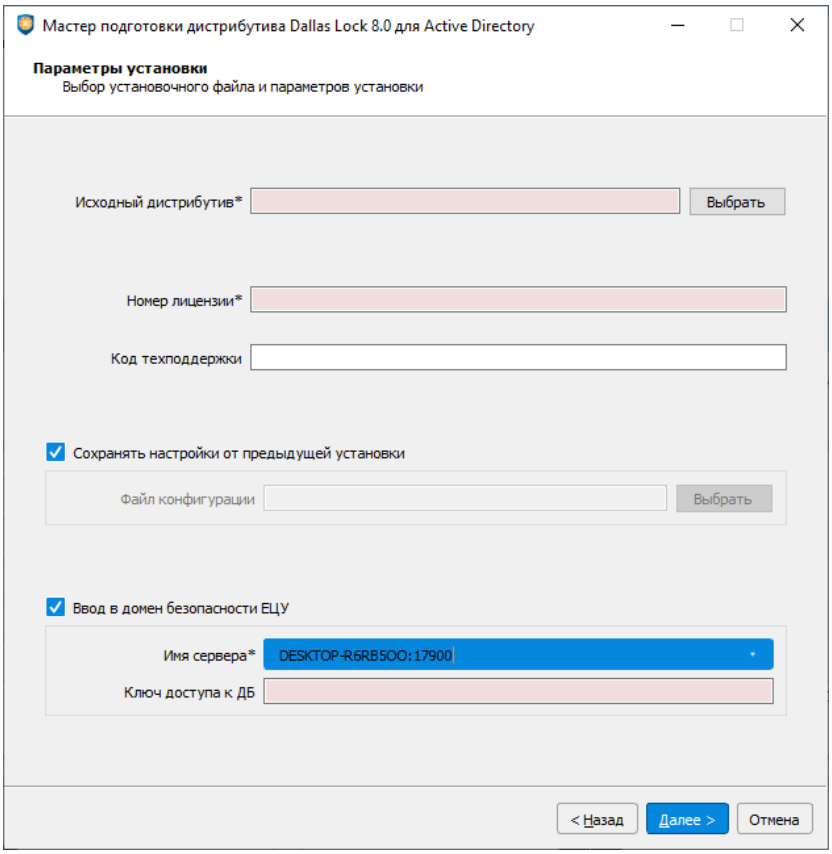

Рис. 123. Ввод параметров для дистрибутива

На втором шаге подготовки дистрибутива необходимо указать параметры удаленной установки, которые будут применены к целевым ТС после активации СЗИ Dallas Lock 8.0 (рис. 123):

- путь к исходному дистрибутиву СЗИ НСД Dallas Lock 8.0;
- номер лицензии, который указан на обложке футляра;
- код технической поддержки, который указан в письме, отправленном на электронную почту.

При необходимости применения определенной конфигурации для дистрибутива, можно поставить флаг «Сохранять настройки от предыдущей установки» или указать путь к файлу конфигурации для СЗИ Dallas Lock 8.0. Если поле не отмечено флагом и не указан путь к файлу конфигурации, применяется конфигурация «По умолчанию», что имеет смысл только при обновлении.

При необходимости ввода в домен ЕЦУ можно поставить флаг «Ввод в домен безопасности ЕЦУ», указать имя сервера ЕЦУ и ключ доступа к ДБ.

После заполнения всех обязательных полей в правом нижнем углу станет доступна кнопка «Далее» для перехода к следующему шагу подготовки дистрибутива.

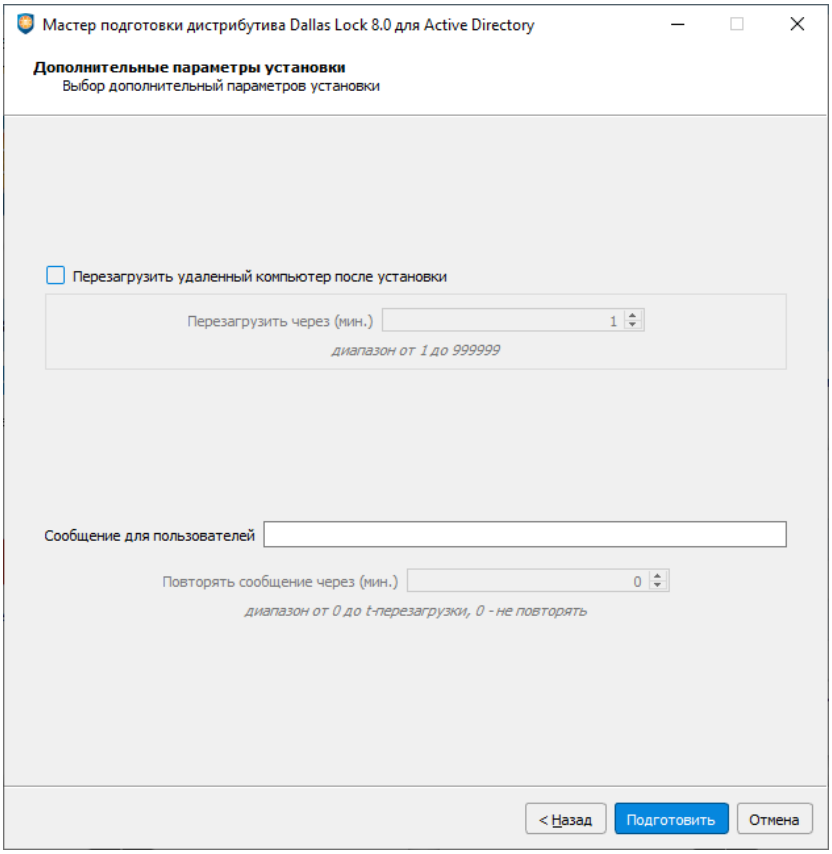

Рис. 124. Настройка параметров перезагрузки

На следующем шаге подготовки дистрибутива указываются параметры перезагрузки при инсталляции (рис. 124).

Поставленный в окне флаг «Перезагрузить удаленный компьютер после установки» позволяет автоматически перезагрузить компьютер после завершения установки СЗИ Dallas Lock 8.0 по истечению установленного времени, иначе компьютер должен быть перезагружен пользователем самостоятельно.

Также в данном окне задается произвольное сообщение и интервал, через который оно будет повторяться, для пользователей, на чьих компьютерах производится установка СЗИ.

Для продолжения подготовки дистрибутива нажать «Подготовить», после чего появится окно, в котором необходимо указать директорию для сохранения дистрибутива.

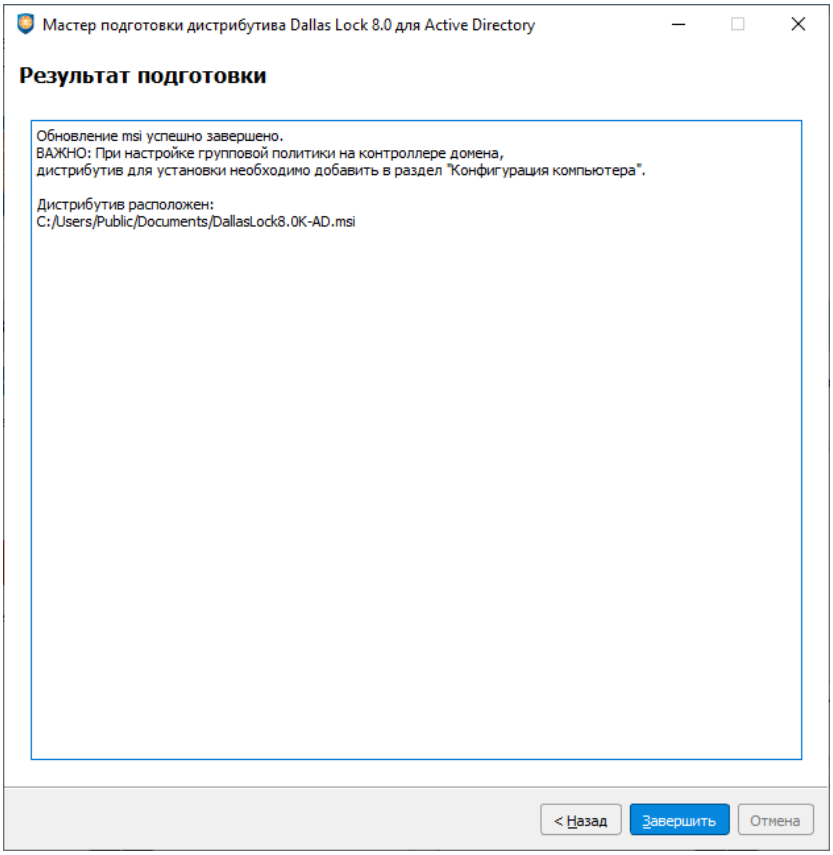

Рис. 125. Завершение подготовки дистрибутива

Появится окно с сообщением об успешном обновлении дистрибутива для установки AD. Дистрибутив будет расположен по пути, указанному в окне (рис. 125).

Подготовленный дистрибутив необходимо перенести на контроллер домена Windows Server, с которого будет производиться удаленная установка.

Далее необходимо приступить к настройкам непосредственно на контроллере домена в службах AD.

9.3.2.2 Создание объекта групповой политики

На контроллере домена необходимо создать объект групповой политики для развертывания Dallas Lock 8.0.

1. Для этого в службах AD необходимо открыть оснастку «Active Directory — пользователи и компьютеры». Далее найти или создать подразделение, которое будет содержать компьютеры, на которые требуется установить систему защиты (рис. 126, рис. 127).

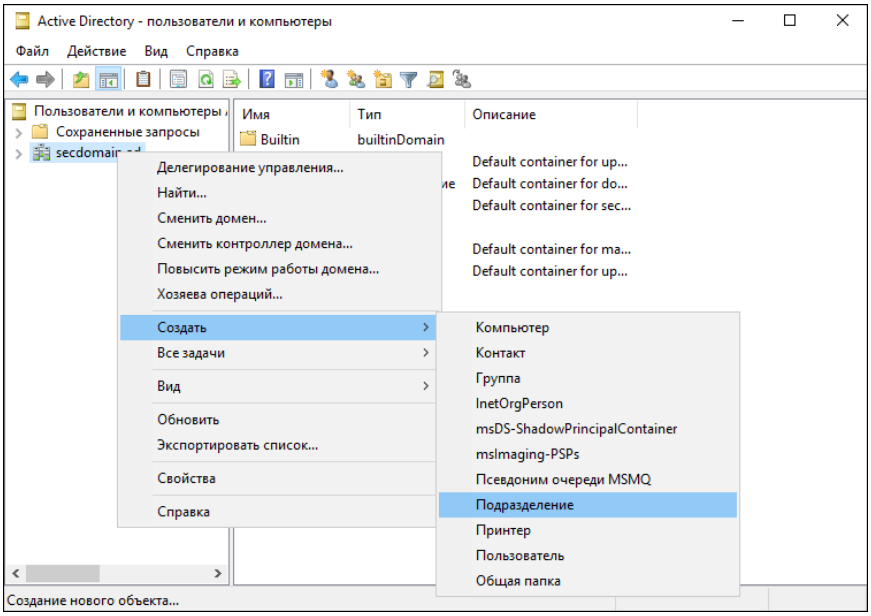

Рис. 126. Создание подразделения в AD

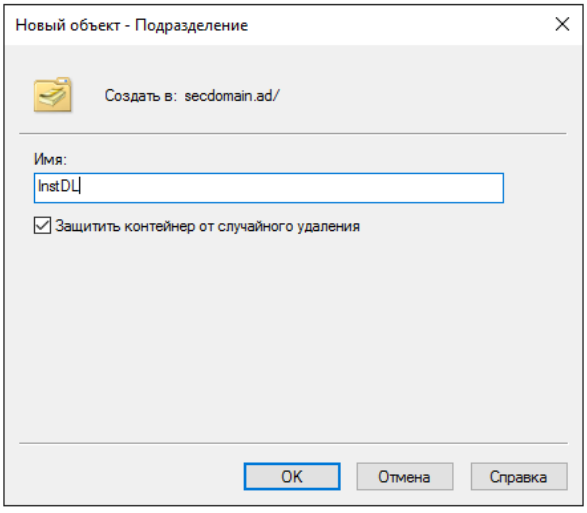

Рис. 127. Имя нового подразделения в AD

2. В это подразделение перенести необходимые компьютеры с помощью функции из контекстного меню «Переместить» (рис. 128, рис. 129).

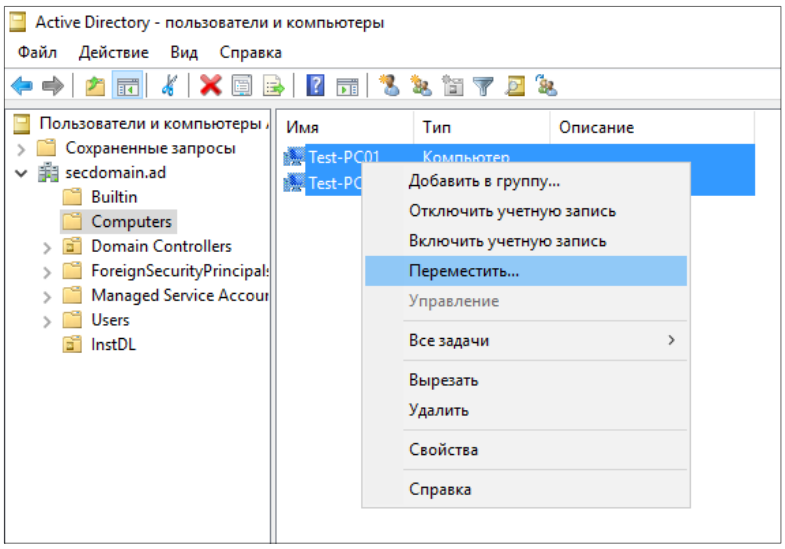

Рис. 128. Пункт контекстного меню «Переместить…»

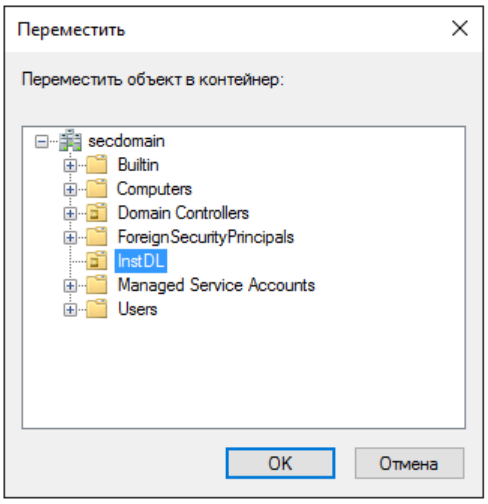

Рис. 129. Перенос рабочих станций в подразделение

В созданном подразделении появится список с необходимыми компьютерами.
Таким образом, создан объект групповой политики для развертывания ПО.

Внимание! Для корректной удаленной установки msi-файла СЗИ Dallas Lock 8.0, подразделение следует создавать именно для компьютеров, а не для пользователей.

9.3.2.3 Создание групповой политики

Теперь для выбранного подразделения необходимо создать групповую политику, с помощью которой и будет происходить удаленная установка системы защиты.
Создание и редактирование групповых политик объектов AD в Windows Server осуществляется из отдельной консоли.

1. Для создания групповой политики в Windows Server необходимо открыть оснастку (или консоль) «Управление групповой политикой». В дереве консоли необходимо развернуть узел необходимого домена и, выбрав созданное подразделение, правой кнопкой мыши нажать пункт меню «Создать объект групповой политики в этом домене и связать его...» (рис. 130).

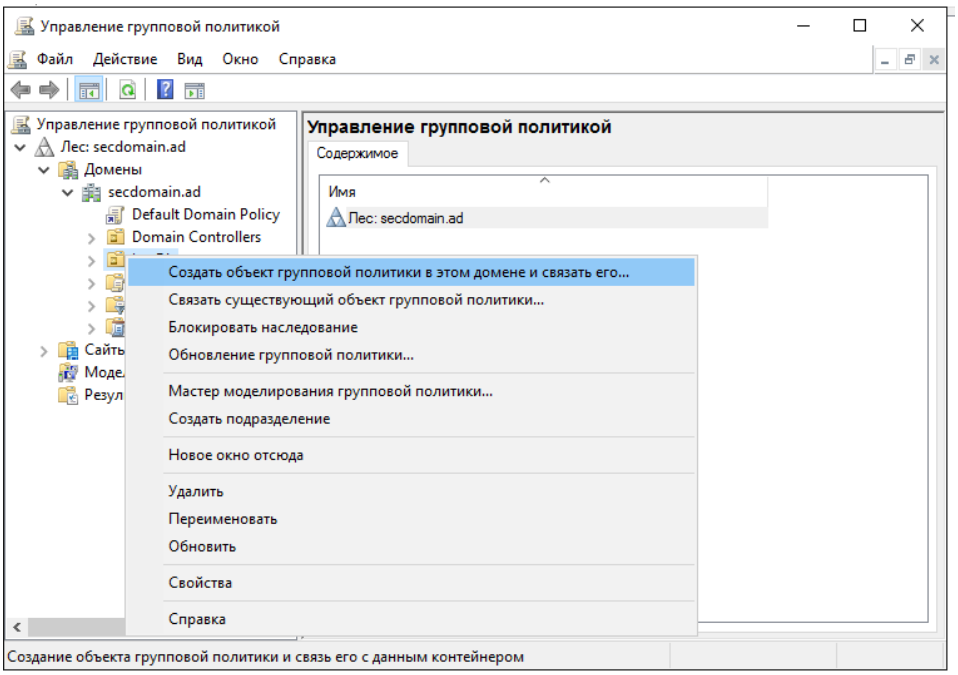

Рис. 130. Консоль управления групповой политикой на Windows Server

2. В появившемся окне необходимо ввести имя новой групповой политики. В поле с исходным объектом групповой политики ничего выбирать не следует. В списке объектов появится созданная групповая политика (рис. 131).

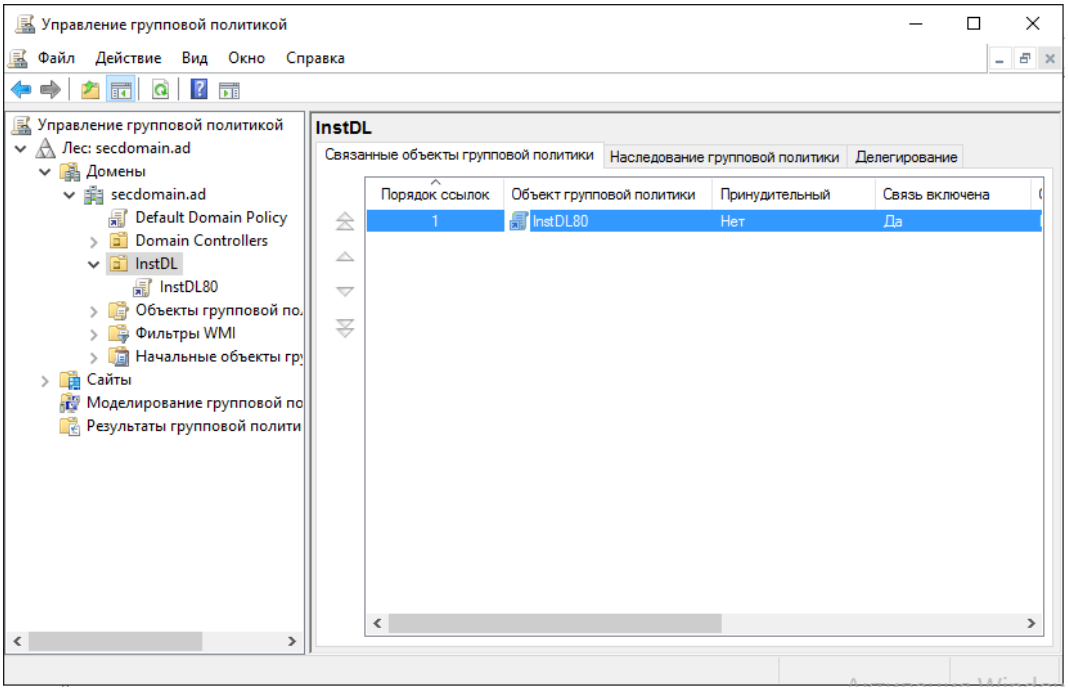

Рис. 131. Новый объект групповой политики, связанный с подразделением

3. Таким образом создана групповая политика для подразделения компьютеров в ОС Windows Server.

9.3.2.4 Создание источника установки

Теперь необходимо определить так называемый источник распространения пакета или установки сформированного msi-файла на сервере Windows. Это должна быть общая сетевая папка, к которой разрешен доступ следующим группам пользователей:

- администраторы;
- прошедшие проверку;
- пользователи домена.

Рекомендуется использовать в качестве точки распространения контейнер местонахождения самой групповой политики. Определить путь к папке со скриптами групповой политики можно различными способами.

1. Вначале необходимо определить уникальное имя групповой политики.

   В ОС Windows Server определить уникальное имя (уникальный код) групповой политики можно через **консоль управления групповыми политиками**, выделив необходимую политику и открыв вкладку свойств «Сведения» (рис. 132).

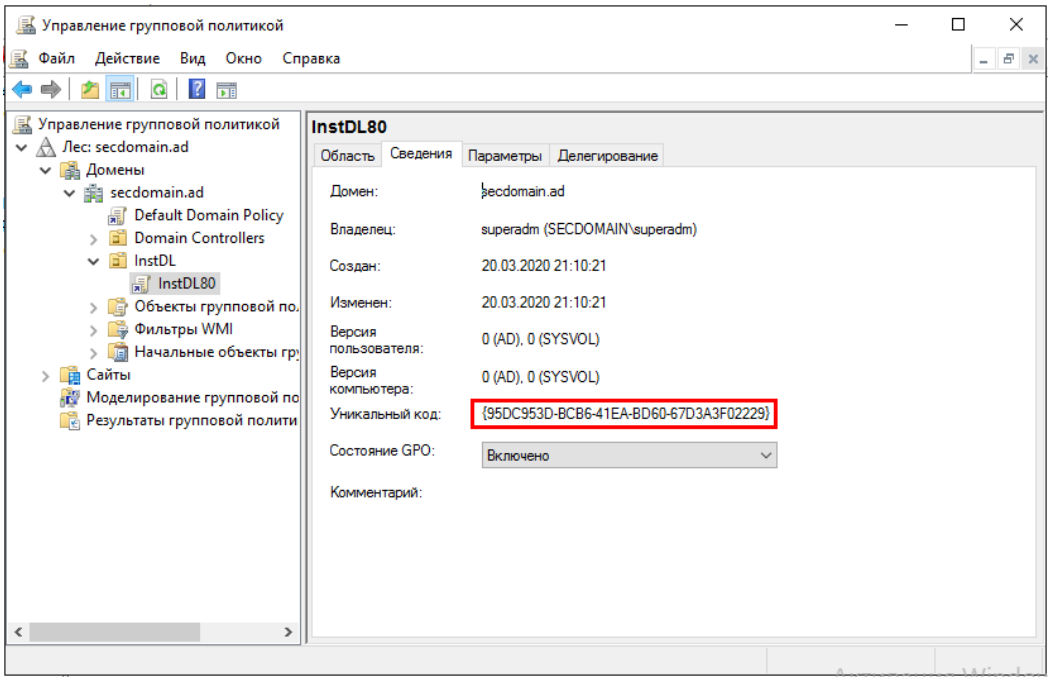

Рис. 132. Новый объект групповой политики, связанный с подразделением

Папки-контейнеры групповых политик располагаются в системной папке *«SYSVOL»*. Эта папка является общей папкой в составе одного домена службы каталогов AD. Поэтому ее свойства соответствуют единой точке распространения.

2. Далее необходимо определить сетевую папку с созданной соответствующей групповой политикой для удаленной установки системы защиты (рис. 133).

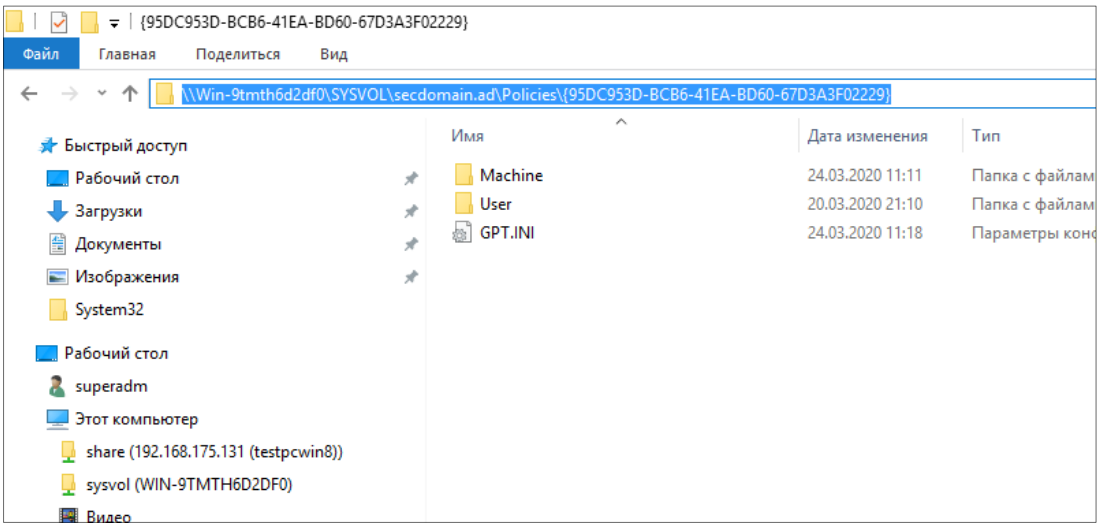

Рис. 133. Расположение папки-контейнера групповой политики

В папках групповых политик располагается каталог Adm, содержащий шаблоны *.ADM, используемые в объектах групповой политики, а также папки MACHINE и USER, включающие в себя файлы со специальными параметрами.

3. В папке MACHINE необходимо расположить созданный на ЕЦУ дистрибутив для СЗИ Dallas Lock 8.0 (msi-файл) (рис. 134).

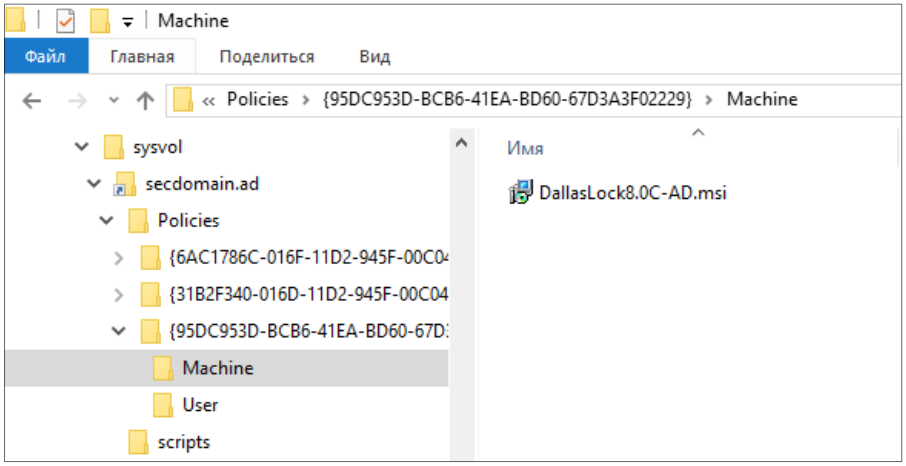

Рис. 134. Перенос msi-дистрибутива в папку групповой политики

Таким образом, был создан источник удаленной установки системы защиты Dallas Lock 8.0, который в контексте Microsoft имеет название «Точка распространения».

9.3.2.5 Настройка групповой политики

Теперь необходимо изменить созданный объект групповой политики для развертывания ПО.

1. В Windows Server редактор объектов групповой политики открывается в консоли управления групповыми политиками. Необходимо выбрать созданную политику правым щелчком мыши и нажать в появившемся контекстном меню «Изменить» (рис. 135).

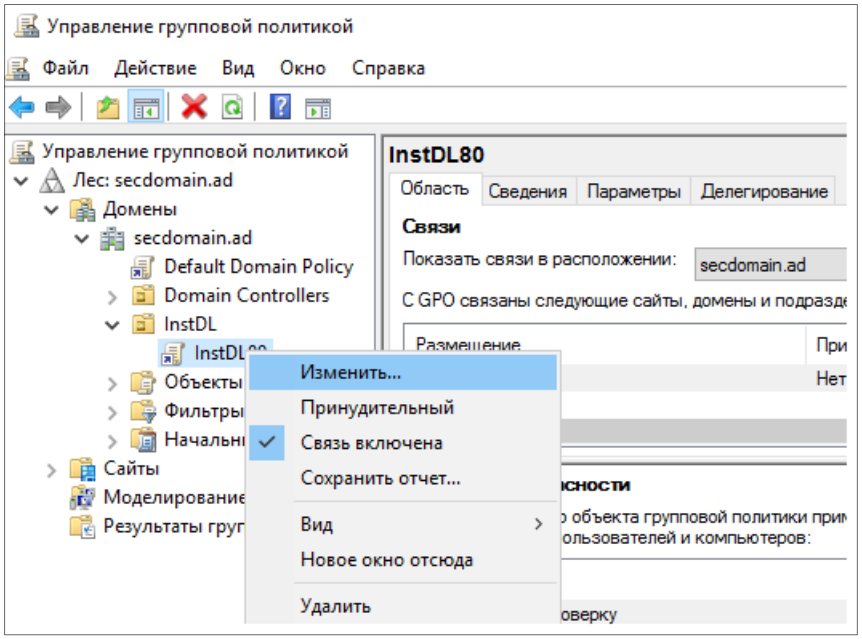

Рис. 135. Вызов контекстного меню в Консоли управления групповой политикой

Откроется необходимое окно редактора. В данном окне в дереве параметров требуется выбрать установку программ (рис. 136).

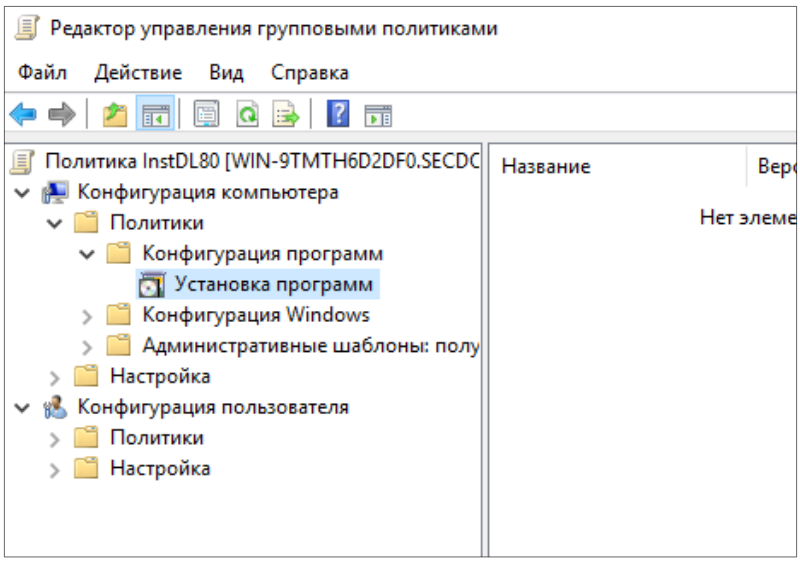

Рис. 136. Окно редактора групповой политики

2. Далее в правом поле окна установки программ с помощью контекстного меню создать пакет установки: нажать последовательно «Создать», «Пакет...» (рис. 137).

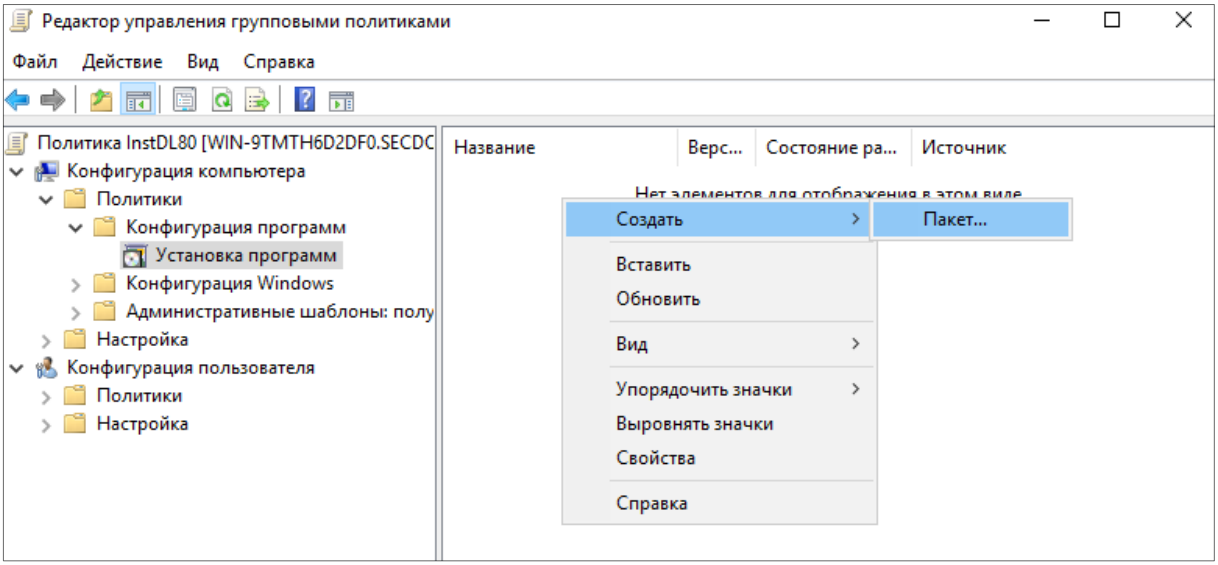

Рис. 137. Создание пакета конфигурации

3. С помощью проводника Windows добавить сетевой путь к распространяемому установочному пакету в общей папке (пакету установщика в точке распространения), который был расположен там ранее (рис. 138).

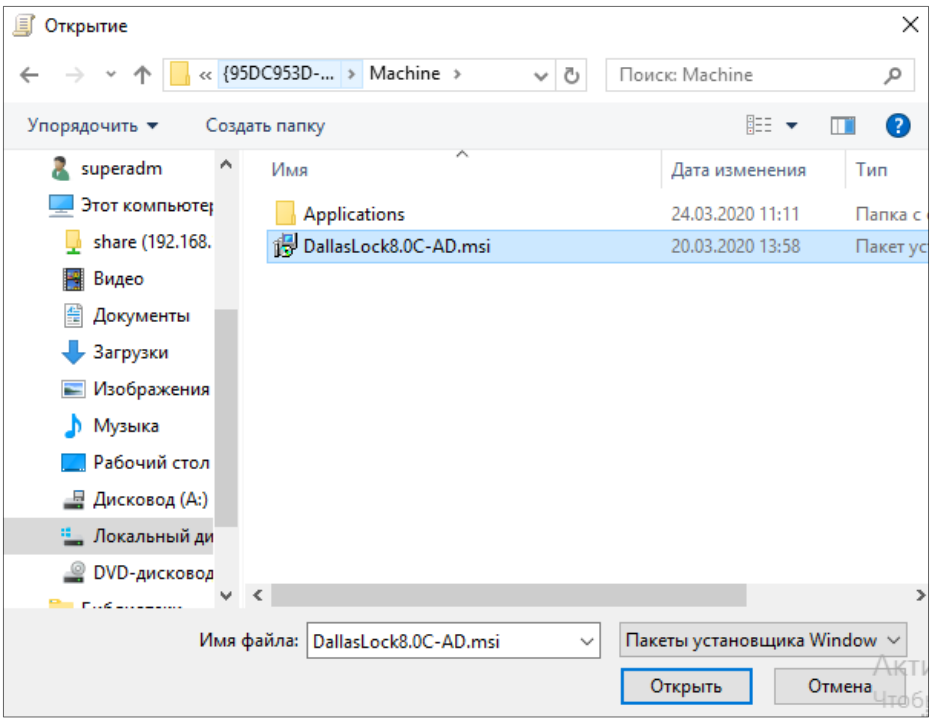

Рис. 138. Выбор расположения пакета установки

4. Выбрать msi-пакет и нажать кнопку «Открыть».
5. В диалоговом окне выбора метода развертывания программ необходимо выбрать вариант «назначенный» и нажать «OK» (рис. 139).

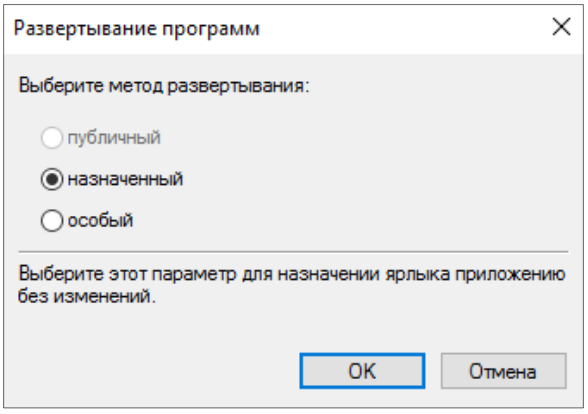

Рис. 139. Выбор метода развертывания программ

Система развернет сформированный файл установки. Выбранный общий установочный пакет появится на правой панели редактора объектов групповой политики (рис. 140).

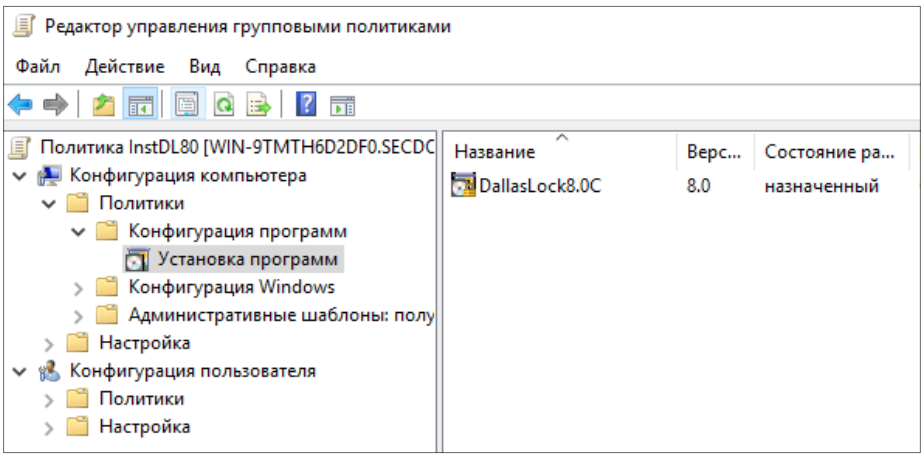

Рис. 140. Появление назначенного пакета установки в окне конфигурации

Таким образом, произведена конфигурация для групповой политики удаленной установки системы защиты Dallas Lock 8.0.
Теперь установочный пакет будет устанавливаться из общей сетевой папки на компьютеры, входящие в состав подразделения с назначенной групповой политикой, удаленно, при загрузке ОС. Установка будет происходить с двумя перезагрузками этих компьютеров. Первая необходима для применения назначенной политики. Вторая — как условие установки Dallas Lock 8.0 — принудительная перезагрузка.
После второй перезагрузки вход уже будет осуществляться на защищенный системой Dallas Lock 8.0 компьютер.

9.4 Настройка модуля СЗИ Dallas Lock 8.0

В дереве Домена безопасности ЕЦУ присутствуют зарегистрированные в ДБ модули СЗИ Dallas Lock 8.0 в составе АРМ.
Значки объектов, обозначающих модули DL8.0, зависят от состояния модуля и могут принимать следующий вид:

— модуль подключен;

— модуль подключен и работает в «Неактивном режиме СЗИ»;

— связь с модулем отсутствует.

Настройки на уровне модуля отображаются на нескольких основных вкладках.

9.4.1 Синхронизация

Для приведения в соответствие значениям параметров, выставленным на ЕЦУ, на модуле СЗИ Dallas Lock 8.0 необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между ЕЦУ и модулем:

- при включении модуля;
- периодически (см. «Параметры работы модулей»);
- по команде пользователя:
  - из консоли ЕЦУ;
  - из оболочки администрирования модуля СЗИ Dallas Lock 8.0.

Синхронизация по команде из консоли ЕЦУ

Команда «Синхронизировать» в консоли ЕЦУ для модуля СЗИ Dallas Lock 8.0 доступна на вкладке «Сводка» на уровне модуля в дереве Домена безопасности на панели инструментов «Оперативное управление» (рис. 141).

Рис. 141. Кнопка «Синхронизировать»

Синхронизация по команде из оболочки администрирования DL8.0

Для проведения синхронизации с Доменом безопасности ЕЦУ по команде из оболочки администрирования модуля СЗИ Dallas Lock 8.0 на клиентском ПК необходимо выполнить следующие шаги:

1. Запустить оболочку администрирования СЗИ Dallas Lock 8.0.
2. Открыть основное меню нажатием кнопки .
3. Выбрать пункт дополнительного меню «Синхронизировать с Доменом безопасности».

9.4.2 Сбор журналов

Для получения в ЕЦУ записей журналов, ведущихся на модуле СЗИ Dallas Lock 8.0, необходимо проведение сбора журналов. Сбор журналов может быть проведен при условии наличия сетевого подключения между ЕЦУ и модулем:

- при включении модуля;
- периодически (см. «Параметры работы модулей»);
- по команде пользователя:
  - из консоли ЕЦУ;
  - из оболочки администрирования модуля СЗИ Dallas Lock 8.0.

Сбор журналов по команде из консоли ЕЦУ

Команда «Собрать журналы» в консоли ЕЦУ для модуля СЗИ Dallas Lock 8.0 доступна на вкладке «Сводка» на уровне модуля в дереве Домена безопасности на панели инструментов «Оперативное управление» (рис. 142).

Рис. 142. Кнопка «Собрать журналы»

Отправка журналов по команде из оболочки администрирования DL8.0

Для отправки журналов в Домен безопасности ЕЦУ по команде из оболочки администрирования модуля СЗИ Dallas Lock 8.0 на клиентском ПК необходимо выполнить следующие шаги:

1. Запустить оболочку администрирования СЗИ Dallas Lock 8.0.
2. Открыть основное меню нажатием кнопки .

3. Выбрать пункт дополнительного меню «Отправить журналы в Домен безопасности».

9.4.3 Сводка модуля СЗИ Dallas Lock 8.0

Вкладка «Сводка» на уровне модуля СЗИ Dallas Lock 8.0 отображает общее состояние модуля (рис. 143).

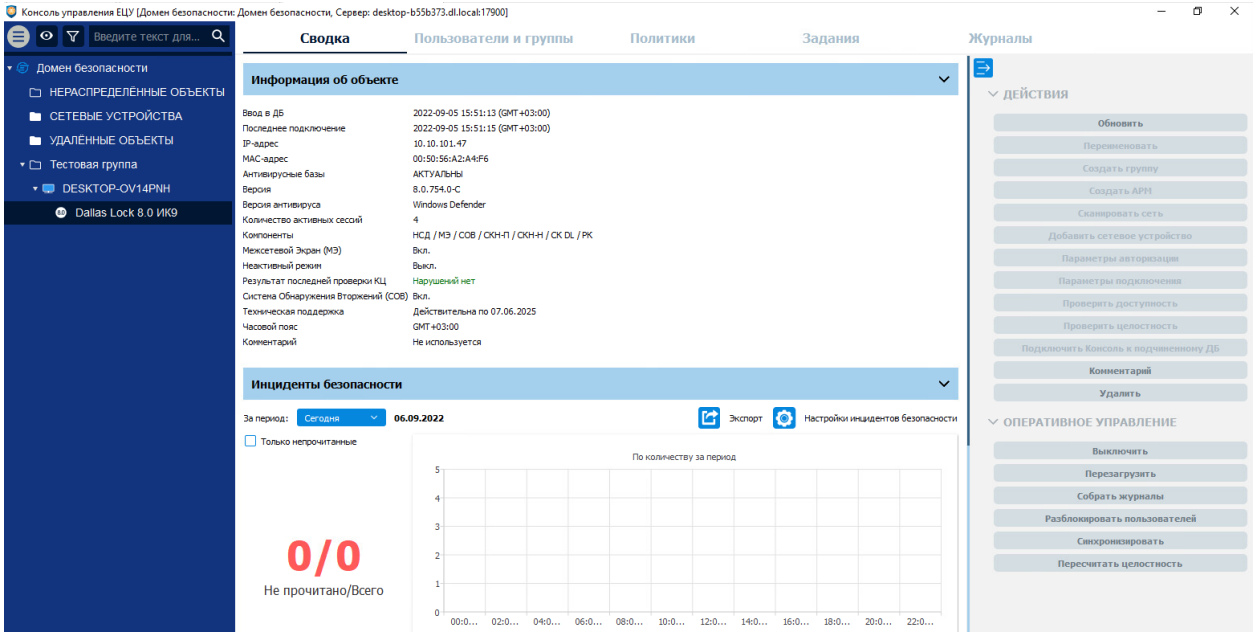

Рис. 143. Вкладка «Сводка»

Доступны следующие разделы информационной панели.

Информация об объекте

В верхней части информационной панели отображается следующая информация о текущем состоянии модуля:

- информация о дате и времени последнего подключения модуля;
- информация о дате и времени ввода модуля в ДБ;
- статус неактивного режима СЗИ;
- статус технической поддержки;
- версия Dallas Lock 8.0;
- активные компоненты Dallas Lock 8.0;
- версия антивируса;
- статус антивирусных баз;
- часовой пояс модуля;
- состояние межсетевого экрана;
- состояние системы обнаружения вторжений;
- IP-адрес;
- MAC-адрес;
- результат последней проверки КЦ;
- комментарий к модулю;
- количество активных сессий

Инциденты безопасности

Отображается список инцидентов безопасности модуля с графической панелью. Доступна фильтрация отображаемых событий по периоду и настройка отображения диаграмм (см. «Настройка инцидентов безопасности»).

Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное. Поле «Комментарий» доступно для редактирования.

Доступны следующие действия с модулем на панели инструментов:

1. Обновить.
2. Удалить.
3. Комментарий.

Доступны следующие команды оперативного управления на панели инструментов:

1. Выключить.
2. Перезагрузить.
3. Разблокировать пользователей.
4. Пересчитать целостность.
5. Собрать журналы.
6. Синхронизировать.

Примечание. Если лицензия модуля СЗИ Dallas Lock 8.0 не включает в себя такие компоненты как МЭ и СОВ, то информация по этим компонентам не будет отображаться на вкладке «Сводка» в разделе «Информация об объекте».

Пункты с информацией об Антивирусном ПО, также не будут отображаться на вкладке «Сводка», так как за взаимодействие с Антивирусным ПО отвечает компонент СОВ модуля СЗИ Dallas Lock 8.0.

9.4.4 Пользователи и группы модуля СЗИ Dallas Lock 8.0

Вкладка «Пользователи и группы» на уровне модуля СЗИ Dallas Lock 8.0 содержит список глобальных и доменных пользователей и групп, наследуемых с уровней выше по иерархии и созданных на уровне данного модуля, а также модульных пользователей.

Управление пользователями и группами на уровне модуля СЗИ Dallas Lock 8.0 производится аналогично описанному управлению пользователями и группами в разделе «Пользователи и группы модуля». Для применения изменений на модулях необходима синхронизация.

9.4.5 Политики модуля СЗИ Dallas Lock 8.0

На уровне модуля СЗИ Dallas Lock 8.0 в списке на вкладе «Политики» доступны только политики, актуальные для СЗИ Dallas Lock 8.0 (см. «Политики ДБ»).

Настройка политик для модуля производится аналогично настройке политик для группы ДБ (см. «Политики для группы ДБ»). Для применения параметров на модулях необходима синхронизация.

9.4.6 Задания модуля СЗИ Dallas Lock 8.0

На уровне модуля СЗИ Dallas Lock 8.0 в списке на вкладе «Задания» доступны для создания только задания, актуальные для СЗИ Dallas Lock 8.0 (рис. 144):

- изменение параметров лицензии;
- получение конфигурации;
- применение конфигурации;
- проверка целостности.

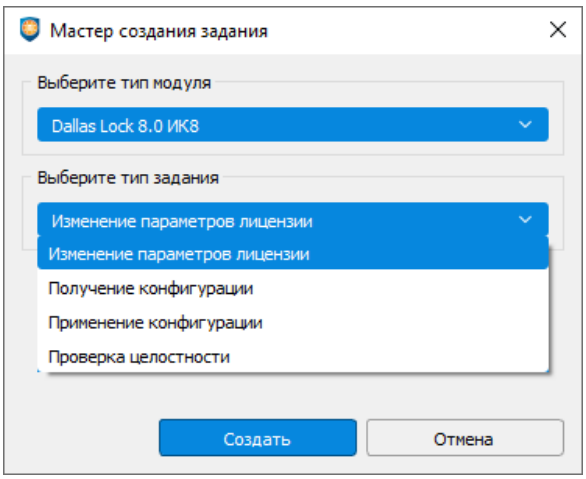

Рис. 144. Мастер создания задания для модуля СЗИ Dallas Lock 8.0

Работа с заданиями для модуля СЗИ Dallas Lock 8.0 производится аналогично настройке заданий для ДБ (см. «Задания ДБ»). Для выполнения задания требуется синхронизация с модулем.

9.4.7 Журналы модуля СЗИ Dallas Lock 8.0

Вкладка «Журналы» для модуля СЗИ Dallas Lock 8.0 позволяет просматривать журналы безопасности модуля (рис. 145).

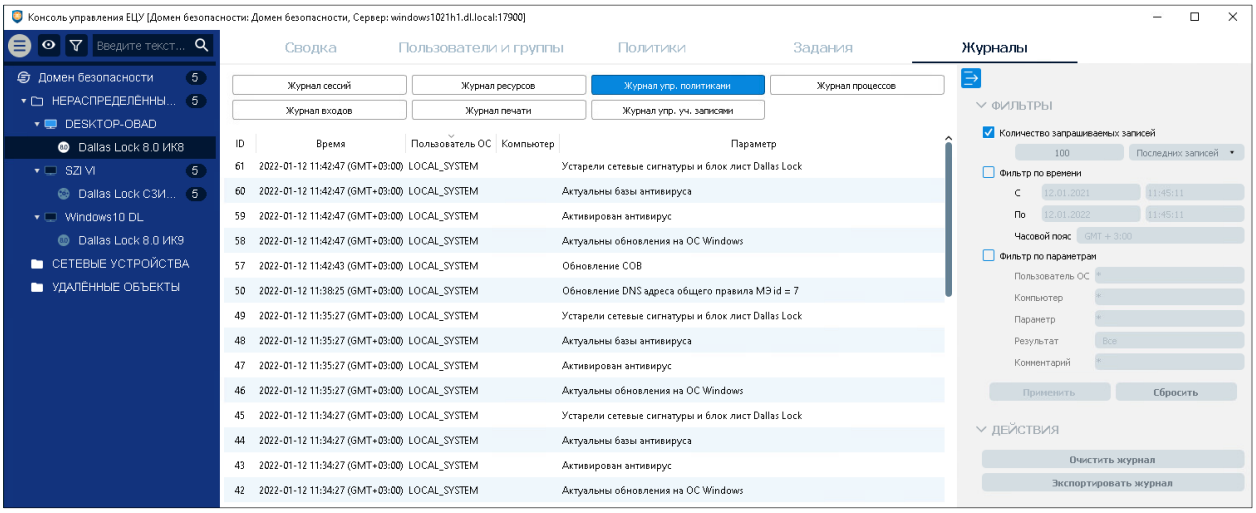

Рис. 145. Вкладка «Журналы»

Для модуля СЗИ Dallas Lock 8.0 доступны:

- «Журнал сессий»;
- «Журнал ресурсов»;
- «Журнал управления политиками»;
- «Журнал процессов»;
- «Журнал входов»;
- «Журнал печати»;
- «Журнал управления учетными записями».

Работа с журналами модулей описана в разделе «Журналы модуля».

Для получения записей журналов с модуля требуется выполнение сбора журналов.

10 МОДУЛЬ СЗИ НСД DALLAS LOCK LINUX

10.1 Ввод модуля в ДБ

Ввести модуль СЗИ НСД Dallas Lock Linux в Домен безопасности можно следующими способами:

- через графическую оболочку администратора Dallas Lock Linux;
- через консольную оболочку администратора Dallas Lock Linux;
- с помощью консоли ЕЦУ (см. «Настройка модуля»).

Внимание! При вводе модуля СЗИ НСД Dallas Lock Linux в ДБ должен быть соблюден ряд условий:

- в ЛВС должен быть работающий сервер ЕЦУ;
- между модулем и сервером ЕЦУ должен быть свободный обмен пакетами по TCP/IP порту 17900.

Внимание! После ввода модуля СЗИ НСД Dallas Lock Linux под управление ЕЦУ значения параметров безопасности подлежат синхронизации со значениями политик ЕЦУ для базовой группы «Нераспределенные объекты».

10.1.1 Ввод модуля в ДБ посредством графической оболочки модуля

Для ввода модуля в ДБ через графическую оболочку администратора необходимо:

1. Убедиться, что сервер ЕЦУ доступен по сети.
2. Запустить графическую оболочку администрирования (GUI) на модуле и авторизоваться.
3. Перейти на вкладку «Параметры безопасности» и выбрать категорию «Основные настройки».
4. Запустить поле «Настройка домена безопасности», где во вкладке «Единый центр управления Dallas Lock» необходимо указать (рис. 146):
   - «АРМ» — сетевое имя или прочее говорящее название для сетевого узла, которое будет отображаться в панели ЕЦУ в списке управляемых объектов;
   - «ДБ ЕЦУ» — сетевое имя или IP-адрес сетевого узла, на котором установлена служба ЕЦУ;
   - «Ключ доступа» — ключ доступа к ДБ (может быть пустым).

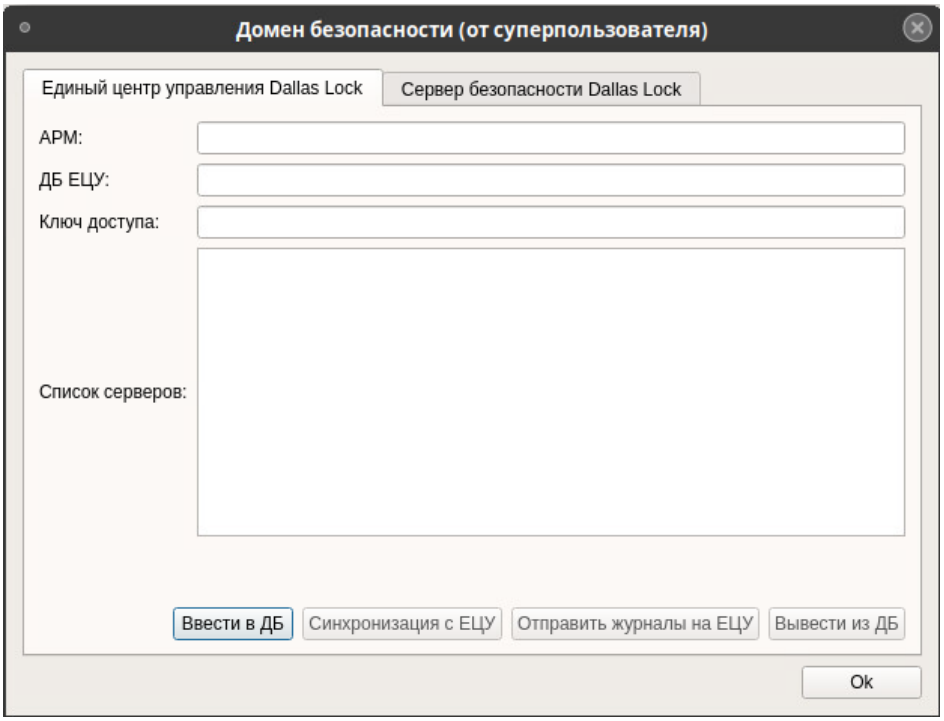

Рис. 146. Окно «Домен безопасности»

5. Далее необходимо нажать кнопку «Ввести в ДБ».

Если указанные поля не заполнены, кнопка «Ввести в ДБ будет недоступна для нажатия».
Результат успешного выполнения: «Модуль успешно зарегистрирован в Домене Безопасности».
В Консоли ЕЦУ в группе дерева ДБ «Нераспределенные объекты» появится новый АРМ с указанным именем, в котором зарегистрирован модуль СЗИ НСД Dallas Lock Linux.

10.1.2 Ввод модуля в ДБ посредством консольной оболочки модуля

Для ввода модуля в ДБ через консольную оболочку администратора необходимо:

1. Убедиться, что сервер ЕЦУ доступен по сети.
2. Запустить консольную оболочку администрирования на модуле путем выполнения команды *«ishl»* и авторизоваться.
3. Перейти в меню централизованного управления, выполнив команду *«management-dll»*. После ввода команды система перейдет в меню централизованного управления.
4. В меню централизованного управления для перехода в подменю подключения к домену безопасности, выполнить команду *«connect-domain»*. После ввода команды система перейдет в раздел подключения к домену безопасности «*connect-domain*».
5. Далее консольное приложение будет ожидать ввода управляющих команд данной подсистемы, список команд приведен в Таблице 19.

Таблица 19

№	Команда	Описание
1	*net-name <значение>*	Сетевое имя или IP-адрес сетевого узла, на котором установлена Служба ЕЦУ. При указании сетевого имени или IP-адреса важно указать номер порта
2	*name <значение>*	Сетевое имя или прочее говорящее название для сетевого узла, которое будет отображаться в панели ЕЦУ в списке управляемых объектов
3	*key <значение>*	Ключ доступа к ДБ ЕЦУ

6. Применить внесенные изменения, выполнив команду *execute*.
7. В результате успешного выполнения появится сообщение:
   «*Command 'connect-domain' executed successfully*» — модуль успешно введен в ДБ.

10.2 Вывод модуля из ДБ

Вывести модуль СЗИ НСД Dallas Lock Linux из Домена безопасности можно следующими способами:

- с помощью Консоли ЕЦУ (см. «Настройка модуля»);
- через графическую оболочку администратора Dallas Lock Linux;
- через консольную оболочку администратора Dallas Lock Linux.

Примечание. При отсутствии сетевого подключения к Службе ЕЦУ, модуль может быть выведен из Домена безопасности ЕЦУ принудительно. При этом, в Консоли ЕЦУ такой модуль продолжит отображаться, но его статус будет «Недоступен».

Поэтому, каждый модуль, выведенный из состава ДБ во время отсутствия связи со Службой ЕЦУ, необходимо дополнительно удалять вручную из Консоли ЕЦУ.

10.2.1 Вывод посредством графической оболочки модуля

Для вывода модуля через оболочку администрирования необходимо:

1. Запустить графическую оболочку администрирования (GUI) на модуле и авторизоваться.
2. Перейти на вкладку «Параметры безопасности» и выбрать категорию «Основные настройки».
3. Запустить поле «Настройка домена безопасности».
4. Нажать кнопку «Вывести из ДБ» (рис. 147).

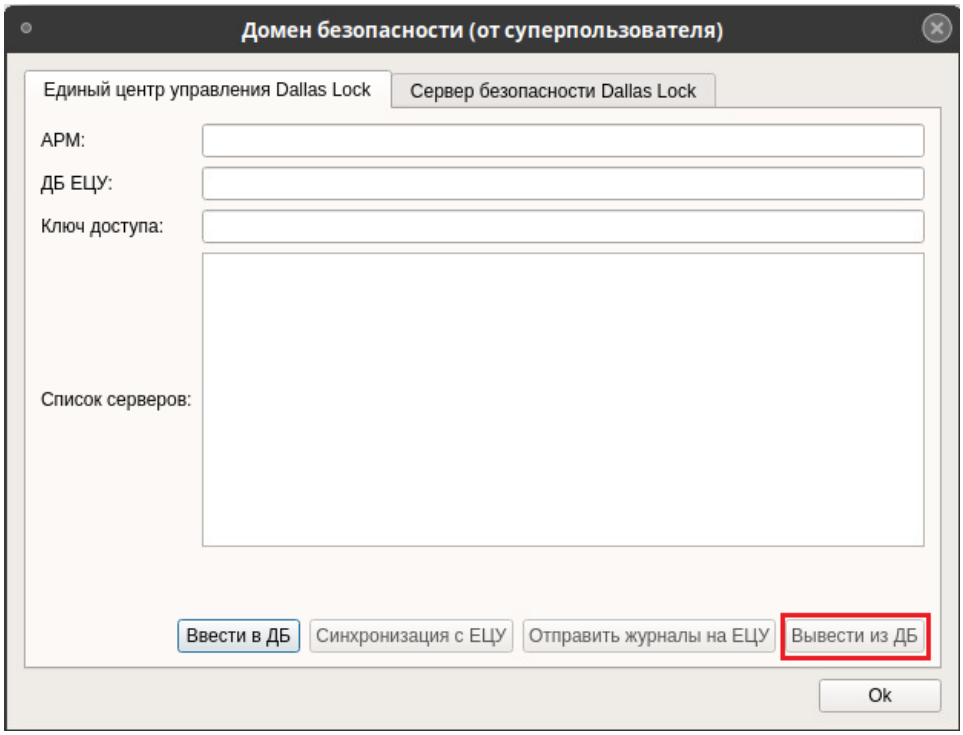

Рис. 147. Вывод модуля из ДБ

Если процесс вывода модуля из ДБ прошел успешно, то через некоторое время поля с информацией о Домене безопасности станут доступными для редактирования.

В Консоли ЕЦУ удаленный модуль переместится в базовую группу «Удаленные объекты» дерева ДБ.

10.2.2 Вывод посредством консольной оболочки модуля

Для вывода модуля из ДБ через консольную оболочку администратора необходимо:

1. Запустить консольную оболочку администрирования на модуле путем выполнения команды «*ishl*» и авторизоваться.
2. Перейти в меню централизованного управления, выполнив команду «*management-dll*». После ввода команды система перейдет в раздел централизованного управления «*management-dll*».
3. В меню централизованного управления выполнить команду «*disconnect-domain*», установив для атрибута значение *force*/*yes*.
   Пример:
   disconnect-domain force <enter>
4. В результате успешного выполнения появится сообщение:
   «*Unregistration success*» — модуль успешно выведен из ДБ.

В Консоли ЕЦУ удаленный модуль переместится в базовую группу «Удаленные объекты» дерева ДБ.

10.3 Удаленное развертывание СЗИ НСД Dallas Lock Linux

Существует возможность централизованно выполнить установку или удаление СЗИ НСД Dallas Lock Linux для одного или нескольких компьютеров, расположенных в одной ЛВС.

Внимание! Для нескольких целевых ТС централизованную удаленную установку можно осуществить только при выполнении следующих условий:

- целевые ТС входят в тот же домен AD или LDAP, что и АРМ с ЕЦУ Dallas Lock;
- известны имя пользователя и пароль доменной учетной записи с правами администратора домена.

Внимание! В процессе удаленной установки СЗИ НСД Dallas Lock Linux на клиентах автоматически создается учетная запись администратора Dallas Lock Linux с именем «dlladmin» и паролем «dlladmin». После установки рекомендуется сменить пароль администратора «dlladmin».

Удаленная установка возможна в следующих вариантах:

- для группы компьютеров, имеющих одинаковые имена и пароли администратора ОС;
- для компьютеров, имеющих индивидуальные имя и пароль администратора ОС, удаленную установку следует выполнять отдельно от других.

Внимание! Необходимо выполнение следующих требований для удаленных операций:

1. Наличие доступа к сети Интернет у целевых ТС.
2. При удаленном развертывании СЗИ НСД Dallas Lock Linux предварительно на целевых ТС необходимо установить и настроить SSH-сервер. Рекомендуется использовать OpenSSH сервер. Установка клиента и сервера OpenSSH выполняется следующим образом.

   Для Ubuntu в терминале необходимо выполнить команды:
   - «*sudo apt-get install openssh-server openssh-client*».

   Для Debian, Astra Linux, ALT Linux в терминале необходимо выполнить команды:
   - «*su* (*sudo* для Astra Linux) *apt-get install openssh-server openssh-client*».

   Для CentOS, Fedora, RHEL, ЛотОС необходимо выполнить в терминале команды:
   - «*su -c “yum install openssh-server openssh-client”*».

   Для запуска службы OpenSSH необходимо выполнить команды:
   - для Ubuntu «*sudo systemctl start ssh*»;
   - для Debian «*su -c “systemctl start ssh”*»;
   - для CentOS, Fedora, RHEL, ЛотОС «*su -c “systemctl start sshd.service”*»;
   - для Astra Linux «*sudo systemctl start ssh*»;
   - для ALT Linux «*su -c “systemctl start ssh”*».
3. По умолчанию пользователь root не имеет права на вход по SSH. Для того, чтобы разрешить ему вход, необходимо отредактировать конфигурационный файл sshd.
   - открываем на редактирование файл: «/etc/ssh/sshd_config»;
   - ищем строку: «#PermitRootLogin no»;
   - снимаем знак комментария «#»;
   - изменяем значение на «yes» (PermitRootLogin yes);
   - то же самое делаем со строкой «#PasswordAuthentication no»;
   - снимаем знак комментария «#»;
   - изменяем значение на «yes» (PasswordAuthentication yes);
   - перезапускаем демон sshd (команда «*systemctl restart sshd*»).

   Для Ubuntu, Debian, CentOS, Fedora, RHEL, Astra Linux:
   - открываем на редактирование файл «/etc/ssh/sshd_config»;
   - ищем строку «PermitRootLogin no»;
   - изменяем значение на «yes» (PermitRootLogin yes);
   - перезапускаем демон sshd (для Ubuntu, Debian, Astra Linux — команда «*systemctl restart ssh*», для CentOS, Fedora, RHEL — команда «*systemctl restart sshd*»).

   Для ALT Linux:
   - открываем на редактирование файл «/etc/openss/sshd_config»;
   - ищем строку «PermitRootLogin no»;
   - изменяем значение на «yes» (PermitRootLogin yes);
   - перезапускаем демон sshd (команда «*systemctl -c «restart ssh*»).

   После удаленной установки СЗИ НСД Dallas Lock Linux необходимо отключить SSH-сервер на целевых ТС.

Для удаленной установки СЗИ НСД Dallas Lock Linux, необходимо выполнить следующие шаги:

1. На целевых ТС проверить список поддерживаемых протоколов по ssh — выполнить команду «*ssh*

–Q cipher».

Если в списке поддерживаемых протоколов нет следующих алгоритмов: 3des-cbc, aes192-cbc, aes128-cbc, arcfour128, arcfour, то в конфигурационный файл необходимо прописать «Ciphers +3des-cbc,aes192-cbc,aes128-cbc,arcfour128,arcfour»[8]. Сохранить файл после внесенных изменений.

Примечание. ЕЦУ Dallas Lock для связи с модулем СЗИ НСД Dallas Lock Linux использует алгоритмы шифрования «3des-cbc, aes192-cbc, aes128-cbc, arcfour128, arcfour», на стороне модуля Linux список поддерживаемых алгоритмов может несущественно отличаться, и при этом удаленная установка СЗИ НСД Dallas Lock Linux все равно будет возможна.

После выполнения всех настроек в конфигурационном файле сервис sshd необходимо перезапустить.

2. Перед централизованной установкой необходимо разместить на компьютере, на котором запущена консоль ЕЦУ, дистрибутив Dallas Lock Linux.
3. Необходимо открыть главное меню Консоли ЕЦУ → «Утилиты» → «Удаленное развертывание DL Linux».

   В открывшемся окне необходимо добавить целевые ТС для удаленного развертывания. ТС можно добавить одним из следующих способов, через:

   - ручной ввод адреса — для этого нужно заполнить поля «Порт» и «Введите IP-адрес или сетевое имя компьютера», затем нажать кнопку «Добавить компьютер» (рис. 148);
   - импорт из файла — нажать «Импорт из файла» и прикрепить текстовый файл со списком IP-адресов целевых ТС.

     Примечание. Для файла с IP-адресами возможен только следующий формат списка: в каждой строке файла может быть указан только один IP-адрес без дополнительных символов.

     Пример:

     192.168.0.1
     192.168.0.35
     10.10.112.55

[8] В ряде ОС символ «+» может не восприниматься, и строка будет считаться некорректной.

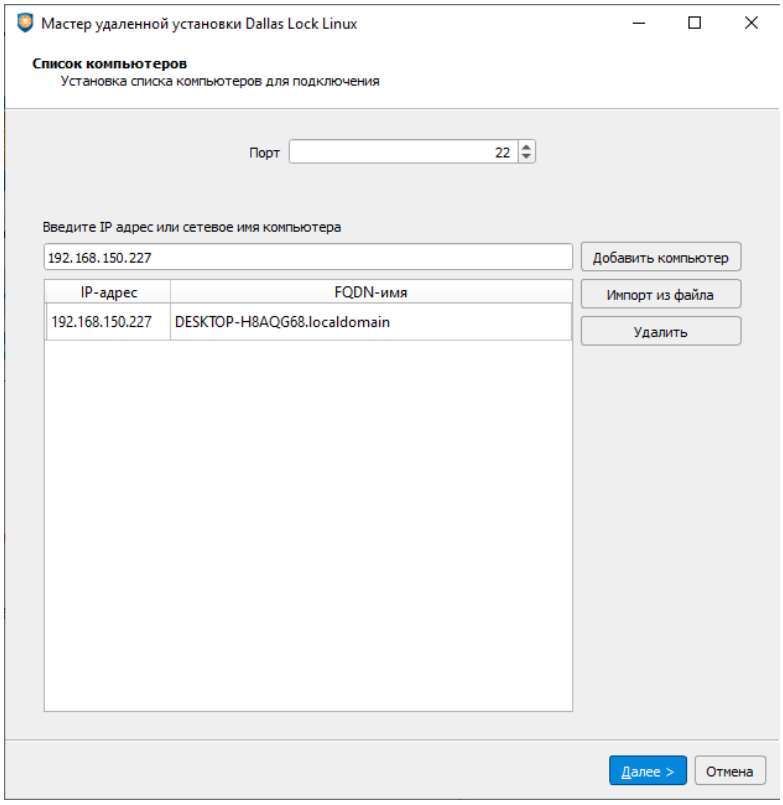

Рис. 148. Список целевых ТС для удаленного развертывания СЗИ НСД Dallas Lock Linux

После добавления целевых ТС в список необходимо нажать кнопку «Далее».

4. Заполнить параметры установки, которые будут применены к модулям в процессе активации СЗИ НСД Dallas Lock Linux (рис. 149):
   - логин и пароль администратора ОС на целевых ТС;
   - логин и пароль суперпользователя (опционально).

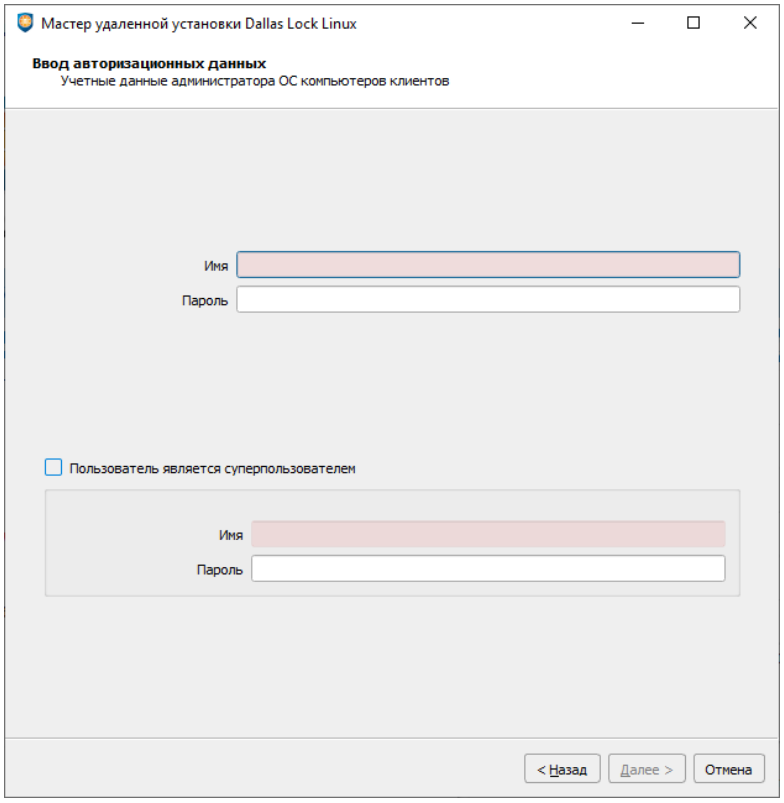

Рис. 149. Параметры установки СЗИ НСД Dallas Lock Linux

После заполнения всех необходимых полей нужно нажать кнопку «Далее».

5. В следующем окне (рис. 150) необходимо указать:

- путь к исходному дистрибутиву СЗИ НСД Dallas Lock Linux;
- номер лицензии, который указан на обложке футляра;
- дополнительные ключи установки;
- параметры для ввода модулей в Домен безопасности ЕЦУ Dallas Lock после установки (опционально).

В качестве дополнительных ключей установки можно указать следующие атрибуты:

Атрибут	Описание
--confim	Спросить перед запуском встроенного скрипта
--quiet	Не печатать ничего кроме сообщений об ошибках
--accept	Принять номер лицензии
--noexec	Не запускать встроенный скрипт
--noexec-cleanup	Не запускать встроенный скрипт очистки
--keep	Не удалять данные о целевой директории после выполнения встроенного скрипта
--noprogress	Не показывать прогресс в процессе декомпрессии
--nox11	Данный атрибут не используется в процессе установки СЗИ НСД
--nochown	Не давать доступ к распакованным файлам текущему пользователю
--chown	Рекурсивно назначить доступ к распакованным файлам текущему пользователю
--nodiskspace	Не проверять доступное место на диске
--target dir	Извлечь непосредственно в целевую директорию (по абсолютной или относительной ссылке). Этот каталог может быть подвергнут рекурсивной обработке (см. *nochown)*

--tar arg1 [arg2 ...]	Доступ к содержимому архива через команду *tar*. Во встроенный скрипт будут переданы следующие аргументы
--ssl-pass-src src	Использовать указанный scr в качестве источника пароля для расшифровки данных с помощью OpenSLL, см. «Аргументы парольной фразы» в руководстве OpenSLL. По умолчанию пользователю предлагается ввести пароля для расшифровки на текущем терминале
--cleanup-args args	Аргументы встроенного скрипта очистки. Для передачи нескольких аргументов требуется заключать их в кавычки
--kvers4	Установочному скрипту будет передана инструкция — использовать 4 версию ядра ОС. При этом, вместо стандартной версии ядра ОС, которая устанавливается по умолчанию, будет установлена указанная версия ядра ОС
--kvers5	Установочному скрипту будет передана инструкция — использовать 5.10 версию ядра ОС. При этом, вместо стандартной версии ядра ОС, которая устанавливается по умолчанию, будет установлена указанная версия ядра ОС
--arm-name=name	Указать под каким именем будет зарегистрирован АРМ в Домене безопасности ЕЦУ
--ucc-addr=address	Указать IP-адрес или сетевое имя компьютера Домена безопасности ЕЦУ
--ucc-key=key	Указать ключ Домена безопасности ЕЦУ
--grub-pass=password	Установить пароль GRUB для суперпользователя по умолчанию — *dlladmin*
--just-check	Не устанавливать, а только проверить поддержку хост-системы

Дополнительные ключи установки указываются в поле через пробел.

Пример:

--nochown --kvers5

Для ввода модулей в Домен безопасности ЕЦУ сразу после установки, можно поставить флаг «Ввод в домен безопасности ЕЦУ», указать имя сервера ЕЦУ и ключ доступа к ДБ. Затем нажать «Установить».

Если данные для ввода модуля в ДБ ЕЦУ (в том числе ключ доступа) были указаны неверно, то установка будет приостановлена. Кнопка «Установить» будет неактивна до тех пор, пока данные для ввода в ДБ ЕЦУ не будут введены верно. Чтобы продолжить установку без ввода модуля в ДБ ЕЦУ необходимо снять флаг «Ввод в домен безопасности ЕЦУ».

Затем нажать кнопку «Установить».

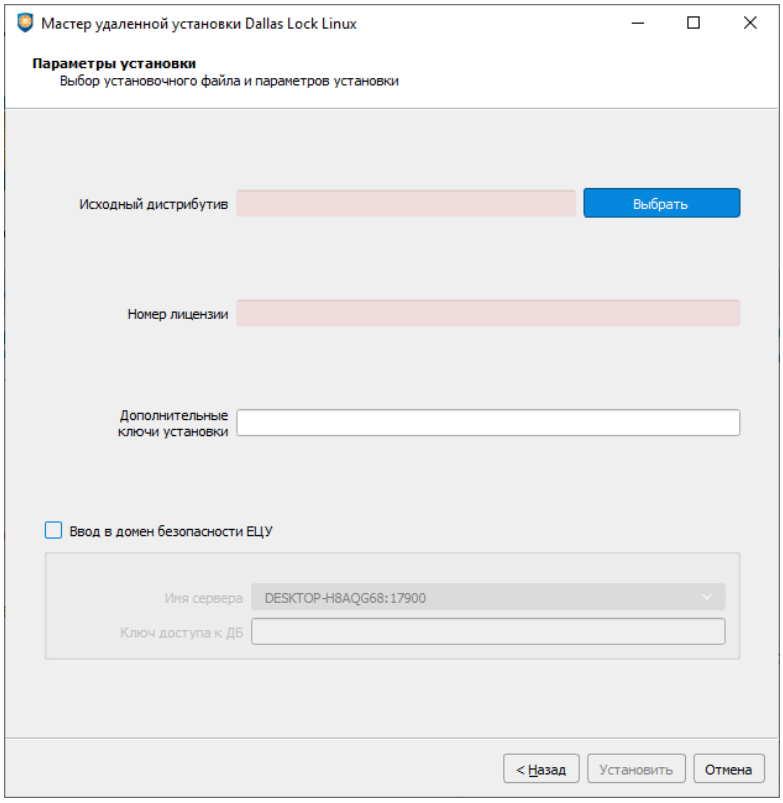

Рис. 150. Информация о ходе централизованной установки средствами ЕЦУ

6. Далее можно просматривать состояние процесса установки для каждого клиента (рис. 151).

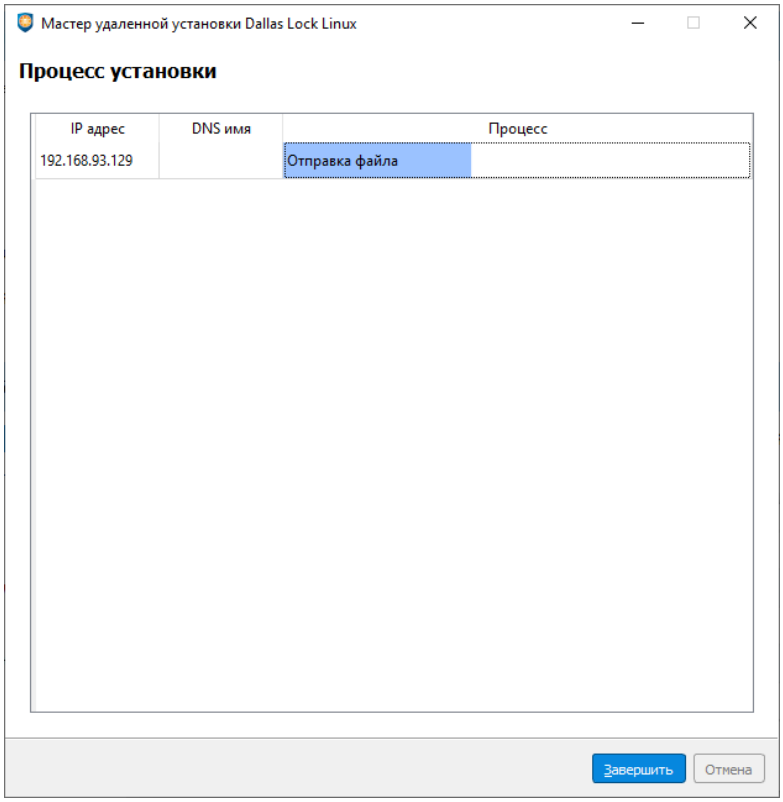

Рис. 151. Информация о ходе централизованной установки средствами ЕЦУ

7. По окончанию процесса централизованной установки появятся соответствующие комментарии удачного или не удачного завершения операции.

Примечание. Во время централизованной установки лог-файл процесса установки может быть переполнен. Прекращение ведения данного процесса не влияет на результат установки. В случае необходимости данный лог-файл можно найти на целевом клиенте.

В дереве объектов ДБ ЕЦУ появятся значки новых АРМ и модулей.

Примечание. Если установленный модуль Dallas Lock Linux не появился в дереве объектов ДБ ЕЦУ, то необходимо осуществить его ввод в ДБ ЕЦУ вручную.

10.4 Настройка модуля СЗИ НСД Dallas Lock Linux

В дереве Домена безопасности ЕЦУ Dallas Lock присутствуют зарегистрированные в ДБ модули СЗИ НСД Dallas Lock Linux в составе АРМ.

Значки объектов, обозначающих модули СЗИ НСД Dallas Lock Linux, зависят от состояния модуля и могут принимать следующий вид:

— модуль подключен;

— связь с модулем отсутствует.

Настройки на уровне модуля отображаются на нескольких основных вкладках.

10.4.1 Синхронизация

Для приведения в соответствие значениям параметров, выставленным на ЕЦУ Dallas Lock, на модуле СЗИ НСД Dallas Lock Linux необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между ЕЦУ Dallas Lock и модулем:

- при включении модуля;
- периодически (см. «Параметры работы модулей»);
- по команде пользователя:
  - из Консоли ЕЦУ;
  - из графической оболочки модуля СЗИ НСД Dallas Lock Linux.

Синхронизация по команде из консоли ЕЦУ

Команда «Синхронизировать» в Консоли ЕЦУ для модуля СЗИ НСД Dallas Lock Linux доступна на вкладке «Сводка» на уровне модуля в дереве Домена безопасности на панели инструментов «Оперативное управление» (рис. 152).

Рис. 152. Кнопка «Синхронизировать»

Синхронизация по команде из графической оболочки СЗИ НСД Dallas Lock Linux

Для проведения синхронизации с Доменом безопасности ЕЦУ по команде из графической оболочки модуля СЗИ НСД Dallas Lock Linux на клиентском ПК необходимо выполнить следующие шаги:

1. Запустить графическую оболочку СЗИ НСД Dallas Lock Linux и авторизоваться.
2. Перейти на вкладку «Централизованное управление».
3. Нажать кнопку «Синхронизация с ЕЦУ» (рис. 153).

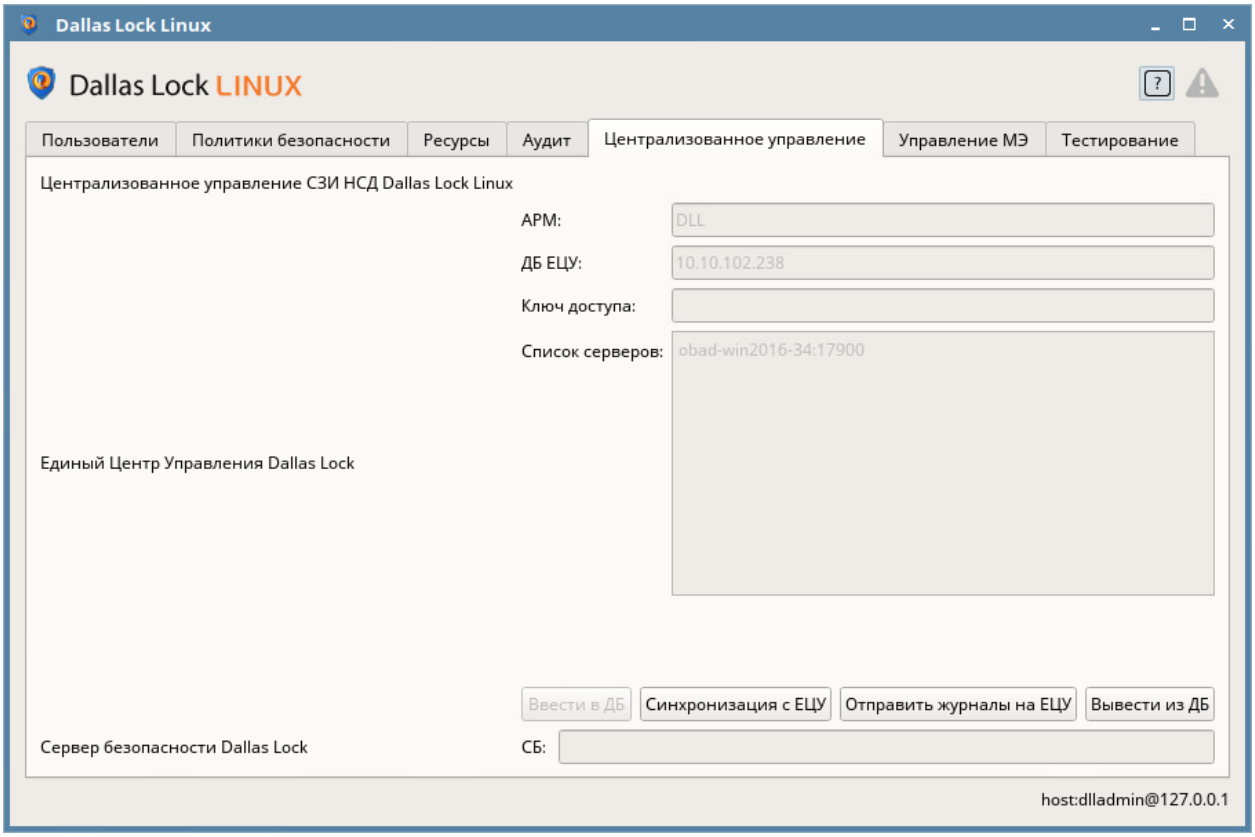

Рис. 153. Кнопка «Синхронизация с ЕЦУ»

10.4.2 Сбор журналов

Для получения в ЕЦУ Dallas Lock записей журналов, ведущихся на модуле СЗИ НСД Dallas Lock Linux, необходимо проведение сбора журналов. Сбор журналов может быть проведен при условии наличия сетевого подключения между ЕЦУ и модулем:

- при включении модуля;
- периодически (см. «Параметры работы модулей»);
- по команде пользователя:
  - из Консоли ЕЦУ;
  - из графической оболочки модуля СЗИ НСД Dallas Lock Linux.

Сбор журналов по команде из консоли ЕЦУ

Команда «Собрать журналы» в Консоли ЕЦУ для модуля СЗИ НСД Dallas Lock Linux доступна на вкладке «Сводка» на уровне модуля в дереве Домена безопасности на панели инструментов «Оперативное управление» (рис. 154).

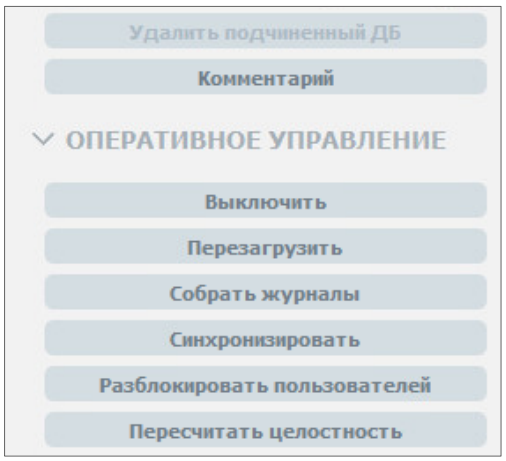

Рис. 154. Кнопка «Собрать журналы»

Отправка журналов по команде из графической оболочки администратора

Для отправки журналов в Домен безопасности ЕЦУ Dallas Lock по команде из графической оболочки модуля СЗИ НСД Dallas Lock Linux на клиентском ПК необходимо выполнить следующие шаги:

1. Запустить графическую оболочку СЗИ НСД Dallas Lock Linux и авторизоваться.
2. Перейти на вкладку «Централизованное управление».
3. Нажать кнопку «Отправить журналы на ЕЦУ» (рис. 155).

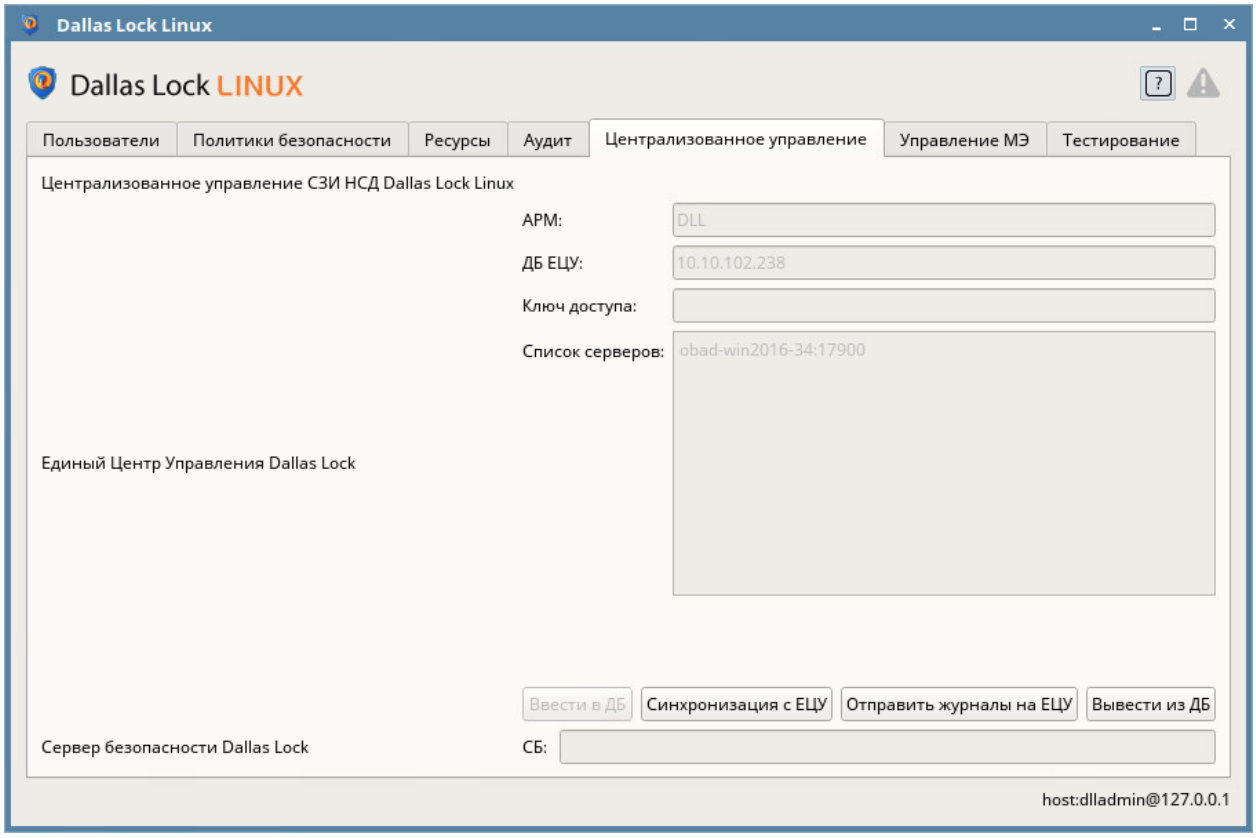

Рис. 155. Кнопка «Отправить журналы на ЕЦУ»

10.4.3 Сводка модуля СЗИ НСД Dallas Lock Linux

Вкладка «Сводка» на уровне модуля СЗИ НСД Dallas Lock Linux отображает общее состояние модуля (рис. 156).

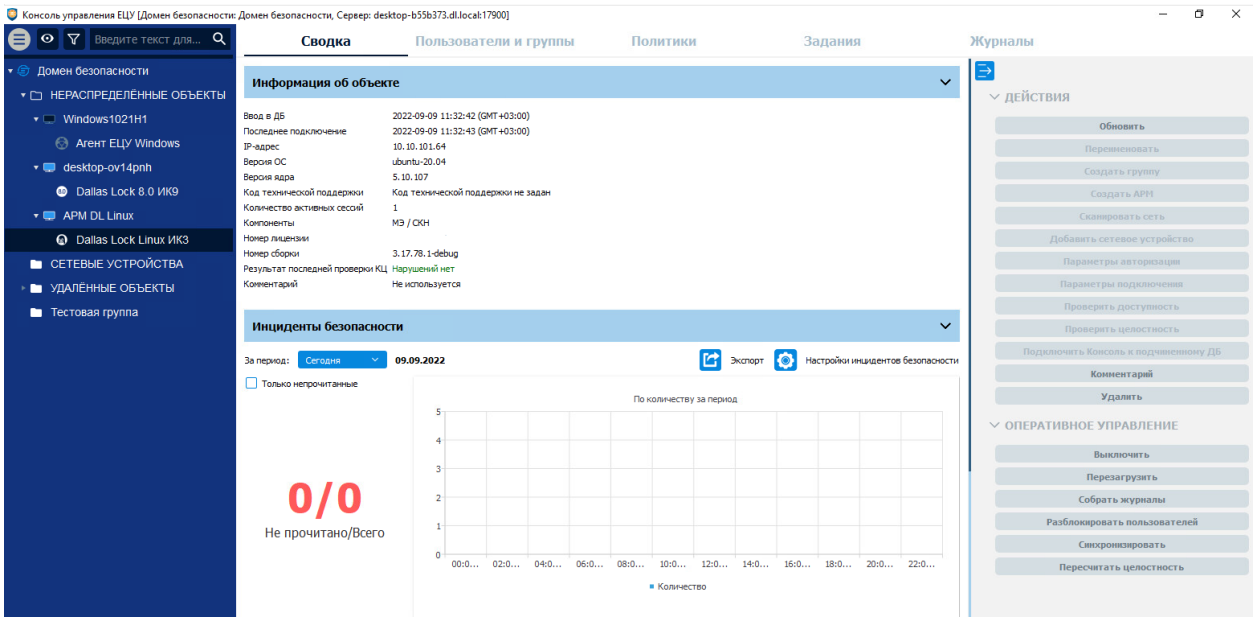

Рис. 156. Вкладка «Сводка»

Доступны следующие разделы информационной панели.

Информация об объекте

В верхней части информационной панели отображается следующая информация о текущем состоянии модуля:

- информация о дате и времени последнего подключения модуля;
- информация о дате и времени ввода модуля в ДБ;
- номер сборки;
- версия операционной системы;
- версия ядра;
- компоненты;
- номер лицензии;
- код технической поддержки;
- IP-адрес;
- результат последней проверки КЦ;
- количество активных сессий;
- комментарий.

Инциденты безопасности

Отображается список инцидентов безопасности модуля с графической панелью. Доступна фильтрация отображаемых событий по периоду и настройка отображения диаграмм (см. «Настройка инцидентов безопасности»).

Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное. Поле «Комментарий» доступно для редактирования.

Доступны следующие действия с модулем на панели инструментов:

1. Обновить.
2. Удалить модуль.
3. Комментарий.

Доступны следующие команды оперативного управления на панели инструментов:

1. Синхронизировать.
2. Выключить.
3. Перезагрузить.
4. Разблокировать пользователей.
5. Пересчитать целостность.

6. Собрать журналы.

10.4.4 Пользователи и группы модуля СЗИ НСД Dallas Lock Linux

Вкладка «Пользователи и группы» на уровне модуля СЗИ НСД Dallas Lock Linux содержит список глобальных и доменных пользователей и групп, наследуемых с уровней выше по иерархии и созданных на уровне данного модуля, а также модульных пользователей.
Управление пользователями и группами на уровне модуля СЗИ НСД Dallas Lock Linux производится аналогично описанному управлению пользователями и группами в разделе «Пользователи и группы модуля». Для применения изменений на модулях необходима синхронизация.

10.4.5 Политики модуля СЗИ НСД Dallas Lock Linux

На уровне модуля СЗИ НСД Dallas Lock Linux в списке на вкладе «Политики» доступны только политики, актуальные для СЗИ НСД Dallas Lock Linux (см. «Политики ДБ»).
Настройка политик для модуля производится аналогично настройке политик для группы ДБ (см. «Политики для группы ДБ»). Для применения параметров на модулях необходима синхронизация.

10.4.6 Задания модуля СЗИ НСД Dallas Lock Linux

На уровне модуля СЗИ НСД Dallas Lock Linux в списке на вкладе «Задания» доступны для создания только задания, актуальные для СЗИ НСД Dallas Lock Linux (рис. 157):

- изменение параметров лицензии (изменяет номер лицензии и код технической поддержки);
- удаление модуля.

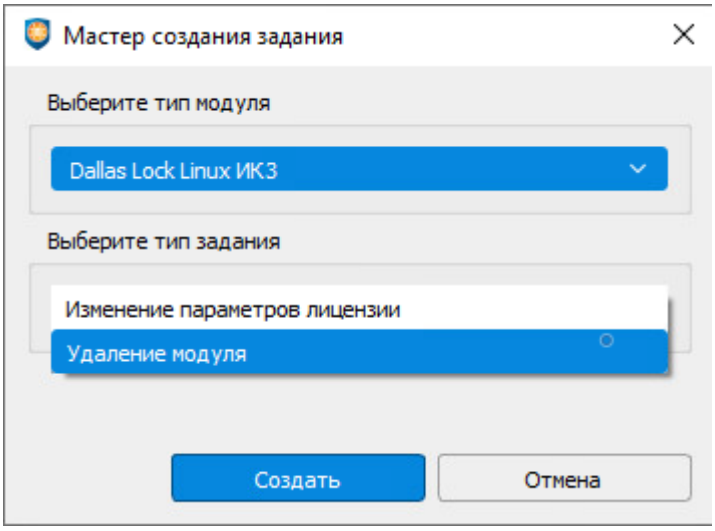

Рис. 157. Мастер создания задания для модуля СЗИ НСД Dallas Lock Linux

Работа с заданиями для модуля СЗИ НСД Dallas Lock Linux производится аналогично настройке заданий для ДБ (см. «Задания ДБ»). Для выполнения задания требуется синхронизация с модулем.

10.4.7 Журналы модуля СЗИ НСД Dallas Lock Linux

Вкладка «Журналы» для модуля СЗИ НСД Dallas Lock Linux позволяет просматривать журналы безопасности модуля (рис. 158).

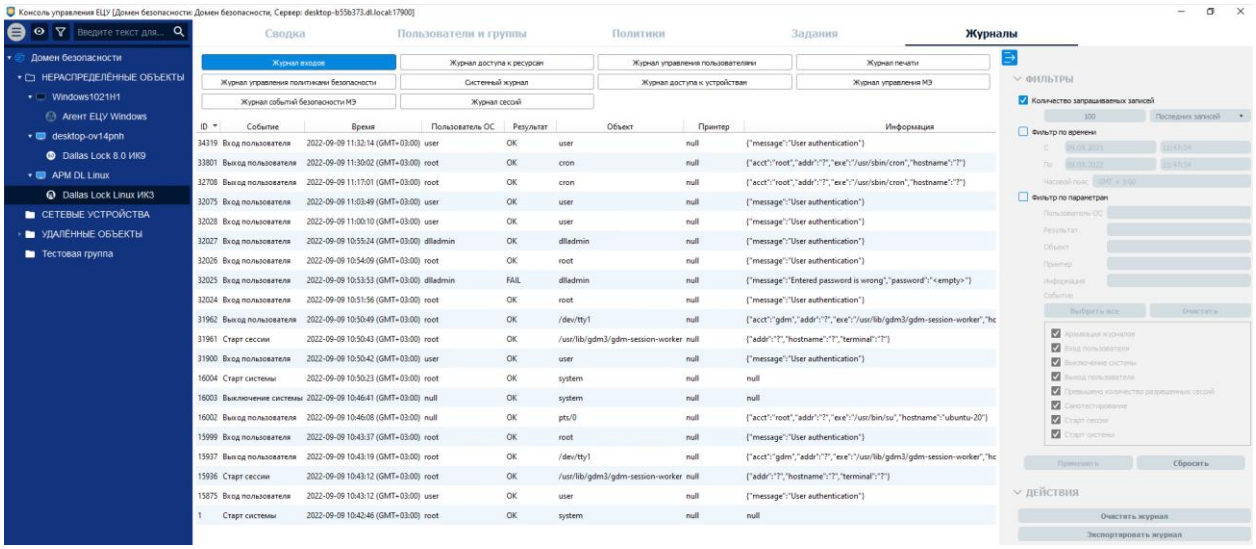

Рис. 158. Вкладка «Журналы»

Для модуля СЗИ НСД Dallas Lock Linux доступны:

- «Журнал сессий»;
- «Журнал доступа к устройствам»;
- «Журнал входов»;
- «Журнал печати»;
- «Журнал управления пользователями»;
- «Журнал управления политиками безопасности»;
- «Системный журнал»;
- «Журнал доступа к ресурсам»;
- «Журнал управления МЭ»;
- «Журнал событий безопасности МЭ».

Работа с журналами модулей описана в разделе «Журналы модуля».
Для получения записей журналов с модуля требуется выполнение сбора журналов.

11 МОДУЛЬ СЗИ ВИ DALLAS LOCK

11.1 Ввод модуля в ДБ

Ввести модуль СЗИ ВИ Dallas Lock в Домен безопасности можно через Консоль Центра управления СЗИ ВИ Dallas Lock.

Внимание! При вводе модуля СЗИ ВИ Dallas Lock в ДБ должен быть соблюден ряд условий:

- в ЛВС должен быть работающий сервер ЕЦУ;
- между модулем и сервером ЕЦУ должен быть свободный обмен пакетами по TCP/IP порту 17900.

Внимание! После ввода модуля СЗИ ВИ Dallas Lock под управление ЕЦУ Dallas Lock значения параметров безопасности подлежат синхронизации со значениями политик ЕЦУ Dallas Lock для базовой группы «Нераспределенные объекты».

Для ввода модуля в ДБ через Консоль Центра управления СЗИ ВИ Dallas Lock необходимо:

1. Убедиться, что сервер ЕЦУ доступен по сети.
2. Запустить консоль модуля.
3. Открыть главное меню → «Параметры ЕЦУ…».
4. Поставить флаг «под управлением ЕЦУ» (рис. 159), чтобы поле настроек стало активно, затем указать следующие данные:
   - DNS-имя или IP-адрес сервера ЕЦУ;
   - имя АРМ, в составе которого необходимо ввести модуль;
   - ключ доступа к ДБ.

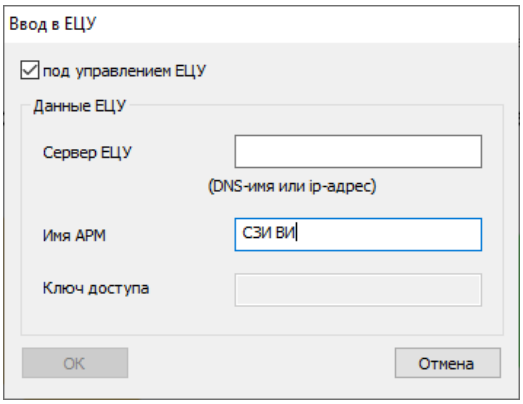

Рис. 159. Ввод в ЕЦУ

5. Нажать кнопку «ОК», и будет инициировано создание АРМ и регистрация модуля в его составе (рис. 160).

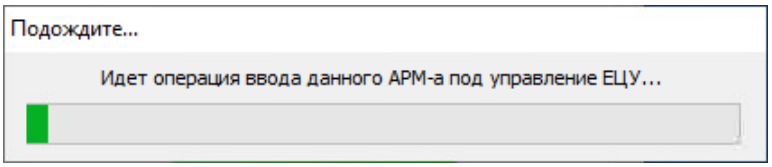

Рис. 160. Операция ввода АРМ под управление ЕЦУ Dallas Lock

Если процесс ввода модуля в ДБ прошел успешно, то через некоторое время появится соответствующее сообщение (рис. 161).

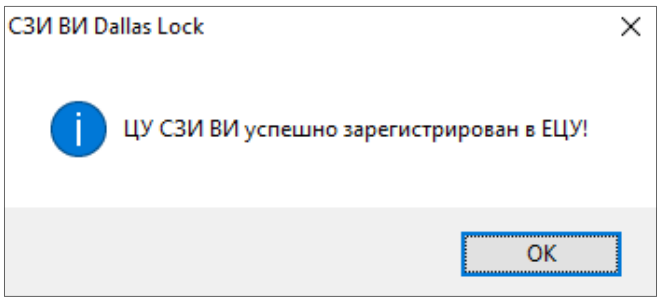

Рис. 161. Модуль зарегистрирован в ЕЦУ Dallas Lock

Примечание. Если во время процесса ввода модуля СЗИ ВИ Dallas Lock в ДБ возникает ошибка, содержащая текст «Ошибка регистрации в ЕЦУ! (Некорректные параметры вызова функции.)», то необходимо выполнить следующие действия:

- в настройках ЕЦУ Dallas Lock (см. «Общие параметры работы») в параметре «Способ подключения к серверу» установить значение «Оба способа» и выбрать приоритет подключения по IP-адресам;
- подождать 30 секунд для применения новых значений;
- повторить попытку ввода модуля СЗИ ВИ Dallas Lock в ДБ.

После, при необходимости, можно установить значение по умолчанию для параметра «Способ подключения к серверу» (оба способа с приоритетом подключения по полным доменным именам), на управление уже зарегистрированными в ДБ модулями СЗИ ВИ Dallas Lock это не повлияет.

11.2 Вывод модуля из ДБ

Вывести модуль СЗИ ВИ Dallas Lock из Домена безопасности можно следующими способами:

- с помощью Консоли ЕЦУ (см. «Настройка модуля»);
- через Консоль Центра управления СЗИ ВИ Dallas Lock.

Для вывода модуля через Консоль Центра управления СЗИ ВИ Dallas Lock необходимо:

1. Запустить консоль модуля, подключиться к Центру управления СЗИ ВИ.
2. Открыть главное меню → «Параметры ЕЦУ…».
3. Убрать флаг «под управлением ЕЦУ» (рис. 159), чтобы поле настроек стало активно.
4. Нажать кнопку «ОК».
5. В появившемся диалоговом окне нажать кнопку «Да» (рис. 162).

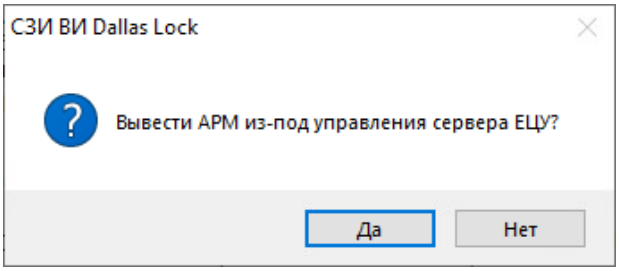

Рис. 162. Вывод АРМ из-под управления сервера ЕЦУ Dallas Lock

Если процесс вывода модуля из ДБ прошел успешно, то через некоторое время появится сообщение о том, что АРМ (модуль Dallas Lock СЗИ ВИ) выведен из ДБ (рис. 163).

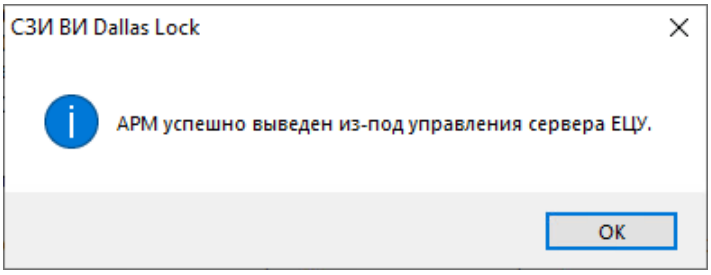

Рис. 163. Модули СЗИ ВИ выведены из ДБ ЕЦУ Dallas Lock

В Консоли ЕЦУ удаленный модуль переместится в базовую группу «Удаленные объекты» дерева ДБ.

Примечание. При отсутствии сетевого подключения к Службе ЕЦУ, модуль может быть выведен из Домена безопасности ЕЦУ принудительно. При этом, в Консоли ЕЦУ такой модуль продолжит отображаться, но его статус будет «Недоступен».

Поэтому, каждый модуль, выведенный из состава ДБ во время отсутствия связи со Службой ЕЦУ, необходимо дополнительно удалять вручную из Консоли ЕЦУ.

11.3 Настройка СЗИ ВИ Dallas Lock

В дереве Домена безопасности ЕЦУ присутствуют зарегистрированные в ДБ модули СЗИ ВИ Dallas Lock, которые отображаются в составе АРМ.
Значки объектов, обозначающих модули СЗИ ВИ Dallas Lock, зависят от состояния модуля и могут принимать следующий вид:

— модуль подключен;

— связь с модулем отсутствует.

Настройки на уровне модуля отображаются на нескольких основных вкладках.

11.3.1 Синхронизация

Для приведения в соответствие значениям параметров, выставленным на ЕЦУ Dallas Lock, на модуле СЗИ ВИ Dallas Lock необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между ЕЦУ Dallas Lock и модулем:

- при включении модуля;
- периодически (см. «Параметры работы модулей»);
- по команде пользователя:
  - из Консоли ЕЦУ;
  - из Консоли Центра управления СЗИ ВИ Dallas Lock.

Синхронизация по команде из Консоли ЕЦУ

Команда «Синхронизировать» в Консоли ЕЦУ для СЗИ ВИ Dallas Lock доступна на вкладке «Сводка» на уровне модуля Dallas Lock СЗИ ВИ в дереве ДБ на панели инструментов «Оперативное управление» (рис. 164).

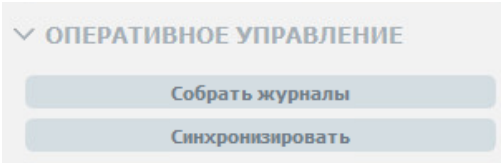

Рис. 164. Панель инструментов «Оперативное управление»

Синхронизация по команде из Консоли Центра управления СЗИ ВИ Dallas Lock

Для проведения синхронизации с Доменом безопасности ЕЦУ Dallas Lock по команде из Консоли Центра управления СЗИ ВИ Dallas Lock на клиентском ПК необходимо выполнить следующие шаги:

1. Запустить консоль модуля, подключиться к Центру управления СЗИ ВИ.
2. Выбрать в дереве объектов вкладку «Агенты ВИ».
3. Нажать кнопку «Синхронизировать» (рис. 165).

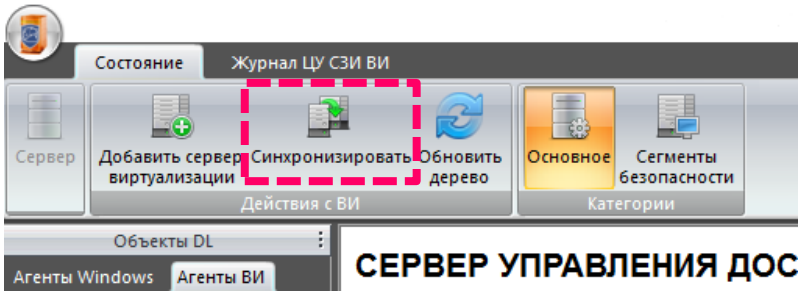

Рис. 165. Кнопка «Синхронизировать»

11.3.2 Сбор журналов

Для получения в ЕЦУ Dallas Lock записей журналов, ведущихся на модуле СЗИ ВИ Dallas Lock, необходимо проведение сбора журналов. Сбор журналов может быть проведен при условии наличия сетевого подключения между ЕЦУ и модулем:

- при включении модуля;
- периодически (см. «Параметры работы модулей»);
- по команде пользователя из Консоли ЕЦУ.

Сбор журналов по команде из Консоли ЕЦУ

Команда «Собрать журналы» в Консоли ЕЦУ для модулей Dallas Lock СЗИ ВИ доступна на вкладке «Сводка» на уровне модуля в дереве ДБ на панели инструментов «Оперативное управление» (рис. 164).

11.3.3 Сводка модуля Dallas Lock СЗИ ВИ

Вкладка «Сводка» на уровне модуля Dallas Lock СЗИ ВИ отображает общее состояние модуля (рис. 166).

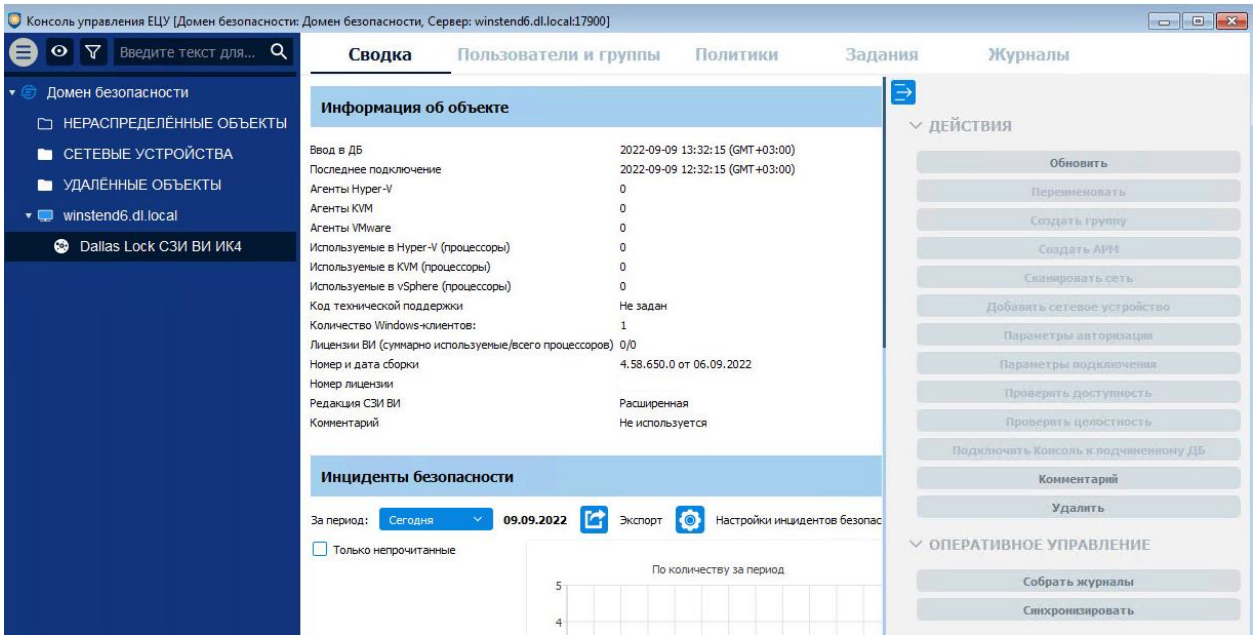

Рис. 166. Вкладка «Сводка»

Доступны следующие разделы информационной панели.

Информация об объекте

В верхней части информационной панели отображается следующая информация о текущем состоянии модуля:
• информация о дате и времени последнего подключения;
• информация о дате и времени ввода модуля в ДБ;
• номер и дата сборки;
• номер лицензии;
• количество Windows-клиентов;
• код технической поддержки;
• параметры лицензии:
  • общее количество лицензий ВИ;
  • количество используемых процессоров в vSphere;
  • количество используемых процессоров в Hyper-V;
  • количество используемых процессоров в KVM;
• количество агентов VMware;
• количество агентов Hyper-V;
• количество агентов KVM;
• редакция СЗИ ВИ;
• комментарий к модулю.

Инциденты безопасности
Отображается список инцидентов безопасности модуля с графической панелью. Доступна фильтрация отображаемых событий по периоду и настройка отображения диаграмм (см. «Настройка инцидентов безопасности»). Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное. Поле «Комментарий» доступно для редактирования.

Доступны следующие действия с модулем на панели инструментов:

1. Обновить.
2. Удалить модуль.
3. Комментарий.

Доступны следующие команды оперативного управления на панели инструментов:

1. Собрать журналы.
2. Синхронизировать.

11.3.4 Пользователи и группы модуля Dallas Lock СЗИ ВИ

Вкладка «Пользователи и группы» на уровне модуля Dallas Lock СЗИ ВИ содержит список глобальных и доменных пользователей и групп, наследуемых с уровней выше по иерархии и созданных на уровне данного модуля, а также модульных пользователей.
Управление пользователями и группами на уровне модуля Dallas Lock СЗИ ВИ производится аналогично описанному управлению пользователями и группами в разделе «Пользователи и группы модуля». Для применения изменений на модулях необходима синхронизация.

11.3.5 Политики модуля Dallas Lock СЗИ ВИ

На уровне модуля Dallas Lock СЗИ ВИ в списке на вкладе «Политики» (рис. 167) доступны только политики, актуальные для Dallas Lock СЗИ ВИ (см. «Политики ДБ»).

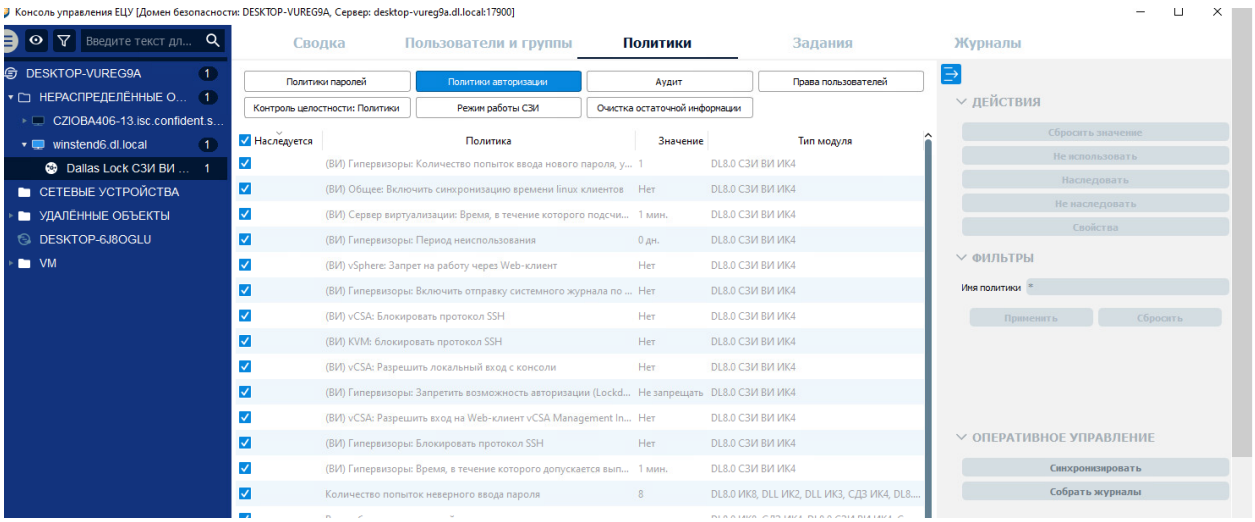

Рис. 167. Политики модуля Dallas Lock СЗИ ВИ

Настройка политик для модуля производится аналогично настройке политик для группы ДБ (см. «Политики для группы ДБ»). Для применения параметров на модулях необходима синхронизация.

11.3.6 Задания модуля Dallas Lock СЗИ ВИ

На уровне модуля Dallas Lock СЗИ ВИ в списке на вкладе «Задания» доступны для создания только задания, актуальные для Dallas Lock СЗИ ВИ (рис. 168):

- изменение параметров лицензии;
- получение конфигурации;
- получение отчета о конфигурации;
- применение конфигурации;
- проверка обновлений.

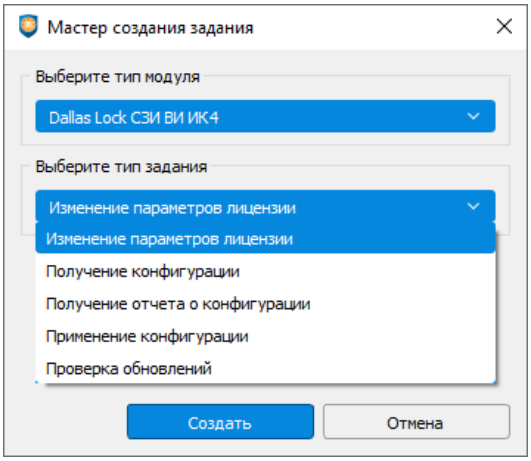

Рис. 168. Мастер создания задания для модуля Dallas Lock СЗИ ВИ

Работа с заданиями для модуля Dallas Lock СЗИ ВИ производится аналогично настройке заданий для ДБ (см. «Задания ДБ»). Для выполнения задания требуется синхронизация с модулем.

11.3.7 Журналы модуля Dallas Lock СЗИ ВИ

Вкладка «Журналы» для модуля Dallas Lock СЗИ ВИ позволяет просматривать журналы безопасности модуля (рис. 169).

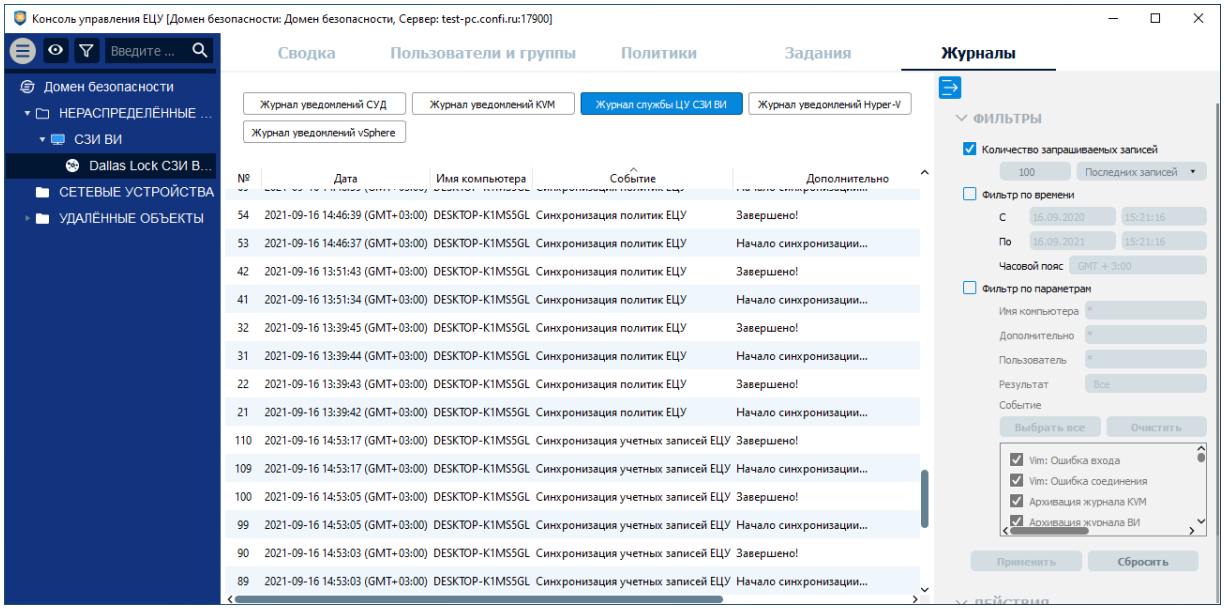

Рис. 169. Вкладка «Журналы»

Для модуля Dallas Lock СЗИ ВИ доступны:

- «Журнал уведомлений СУД»;
- «Журнал уведомлений KVM»;
- «Журнал службы ЦУ СЗИ ВИ»;
- «Журнал уведомлений Hyper-V»;
- «Журнал уведомлений vSphere».

Работа с журналами модулей описана в разделе «Журналы модуля».

Для получения записей журналов с модуля требуется выполнение сбора журналов.

12 МОДУЛЬ СДЗ DALLAS LOCK

12.1 Ввод модуля в ДБ

Ввести модуль СДЗ Dallas Lock в Домен безопасности можно через оболочку администратора СДЗ Dallas Lock.

Внимание! При вводе модуля СДЗ Dallas Lock в ДБ должен быть соблюден ряд условий:

- в ЛВС должен быть работающий сервер ЕЦУ;
- между модулем и сервером ЕЦУ должен быть свободный обмен пакетами по TCP/IP порту 17900.

Внимание! После ввода модуля СДЗ Dallas Lock под управление ЕЦУ Dallas Lock значения политик безопасности подлежат синхронизации со значениями политик ЕЦУ Dallas Lock для базовой группы «Нераспределенные объекты».

Для ввода модуля в ДБ через оболочку администратора необходимо:

1. Убедиться, что сервер ЕЦУ доступен по сети.
2. Запустить ТС с установленной платой СДЗ Dallas Lock, ввести авторизационные данные и выбрать сценарий сессии «Администрирование».
3. Дождаться запуска оболочки администратора модуля СДЗ Dallas Lock.
4. Перейти на вкладку «Параметры» → категория «Параметры сети» (рис. 170).

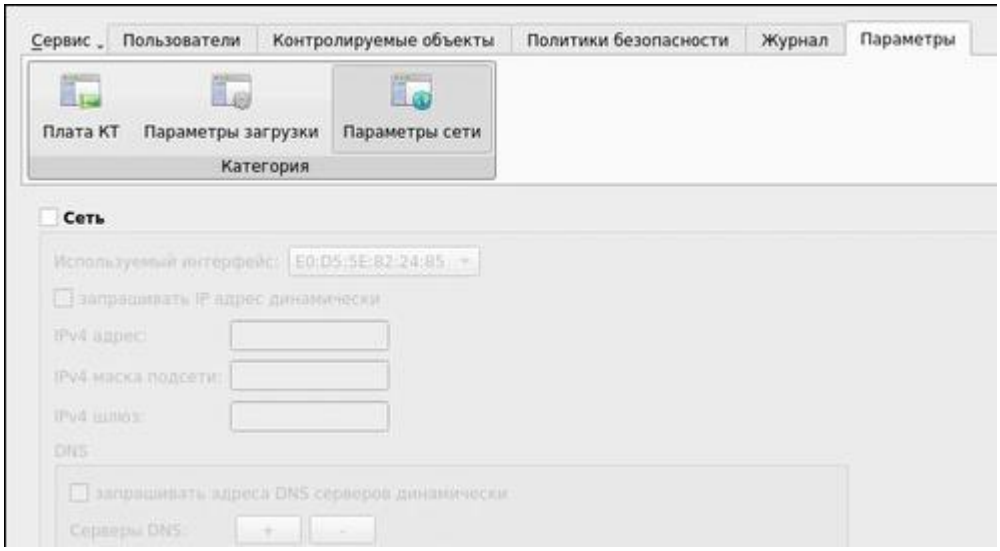

Рис. 170. Вкладка «Параметры сети» модуля СДЗ Dallas Lock

5. Поставить флаг в поле «Сеть», после чего станут доступны для редактирования другие поля страницы.
6. Заполнить вручную необходимые сетевые параметры или же поставить флаг в поле «запрашивать IP-адрес динамически» для автоматического назначения сетевых параметров DHCP-сервером (рис. 171). Нажать кнопку «Применить».

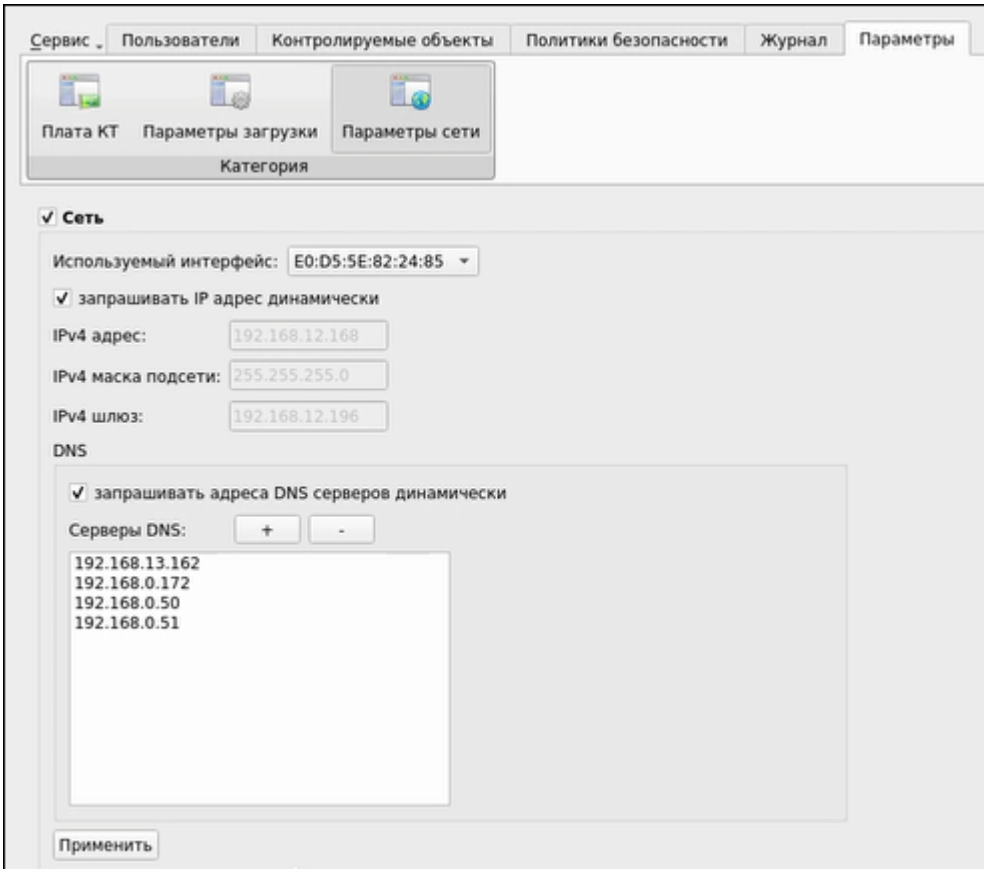

Рис. 171. Заполненные сетевые параметры

7. Заполнить параметры ввода в ДБ на панели «Централизованное управление» (рис. 172):
   - выбрать «Единый Центр Управления»;
   - указать имя АРМ, в составе которого необходимо ввести модуль;
   - указать сетевой адрес сервера ЕЦУ;
   - ввести ключ доступа к ДБ.

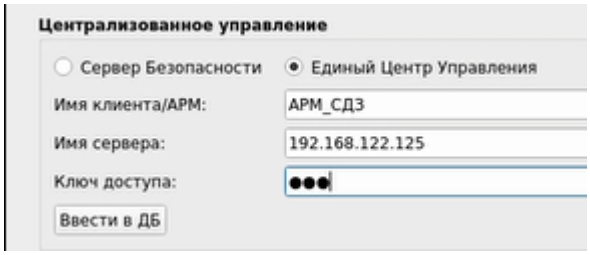

Рис. 172. Централизованное управление

8. После заполнения полей нажать кнопку «Вести в ДБ».
9. Если процесс ввода модуля в ДБ прошел успешно, то через некоторое время появится соответствующее сообщение (рис. 173).

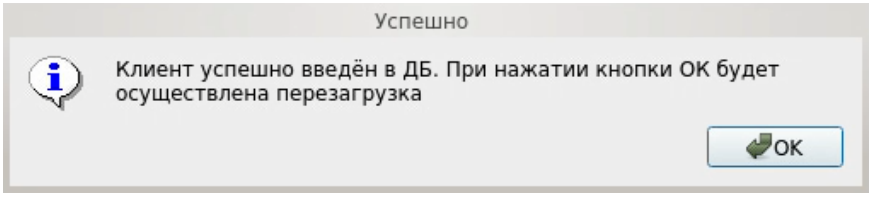

Рис. 173. Сообщение об успешном вводе модуля в ДБ

В Консоли ЕЦУ в группе дерева ДБ «Нераспределенные объекты» появится новый АРМ с указанным именем, в котором зарегистрирован модуль СДЗ Dallas Lock.

12.2 Вывод модуля из ДБ

Вывести модуль СДЗ Dallas Lock из Домена безопасности можно следующими способами:

- с помощью Консоли ЕЦУ (см. «Настройка модуля»);
- через оболочку администратора СДЗ Dallas Lock.

Для вывода модуля через оболочку администрирования необходимо:

1. Запустить ТС с установленной платой СДЗ Dallas Lock, ввести авторизационные данные и выбрать сценарий сессии «Администрирование».
2. Дождаться запуска оболочки администратора модуля СДЗ Dallas Lock.
3. Перейти на вкладку «Параметры» → категория «Параметры сети».
4. На панели «Централизованное управление» нажать кнопку «Вывести из ДБ» (рис. 174).

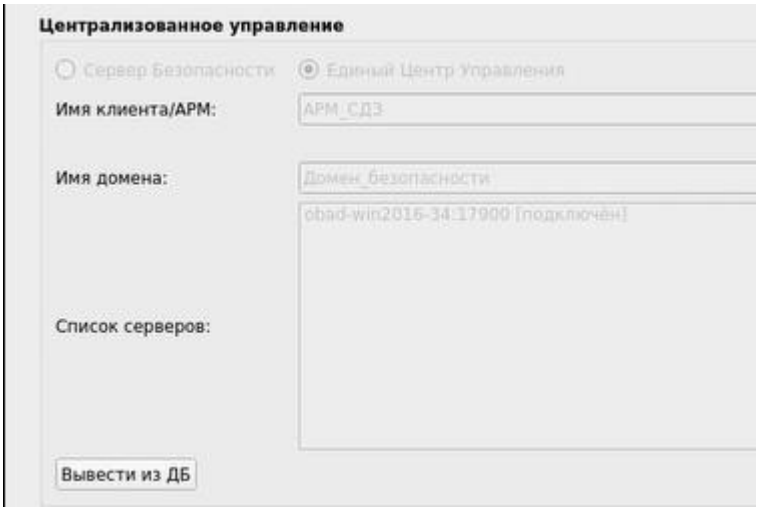

Рис. 174. Вывод модуля СДЗ посредством оболочки администратора

5. Если процесс вывода модуля из ДБ прошел успешно, то через некоторое время появится соответствующее сообщение (рис. 175).

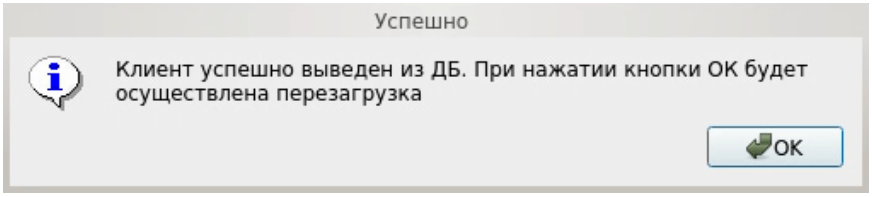

Рис. 175. Сообщение об успешном выводе модуля из ДБ

В Консоли ЕЦУ удаленный модуль переместится в базовую группу «Удаленные объекты» при условии наличия связи с ЕЦУ Dallas Lock.

Примечание. При отсутствии сетевого подключения к Службе ЕЦУ, модуль может быть выведен из Домена безопасности ЕЦУ принудительно. При этом, в Консоли ЕЦУ такой модуль продолжит отображаться, но его статус будет «Недоступен».

Поэтому, каждый модуль, выведенный из состава ДБ во время отсутствия связи со Службой ЕЦУ, необходимо дополнительно удалять вручную из Консоли ЕЦУ.

12.3 Настройка модуля СДЗ Dallas Lock

В дереве Домена безопасности ЕЦУ Dallas Lock присутствуют зарегистрированные в ДБ модули СДЗ Dallas Lock в составе АРМ.

Значки объектов, обозначающих модули СДЗ, зависят от состояния модуля и могут принимать следующий вид:

— модуль подключен, выполнен вход в оболочку администратора на АРМ;

— модуль находится на связи с ЕЦУ Dallas Lock посредством установленного на АРМ Агента ШОС;

— связь с модулем отсутствует;
— модуль находится в режиме работы ШОС и в ШОС не установлен Агент;
— нет соединения между Агентом ШОС и ЕЦУ Dallas Lock.

Настройки на уровне модуля отображаются на нескольких основных вкладках.

12.3.1 Синхронизация

Для приведения в соответствие значениям параметров, выставленным на ЕЦУ Dallas Lock, на модуле СДЗ Dallas Lock необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между ЕЦУ Dallas Lock и модулем при включении модуля.

12.3.2 Сбор журналов

Для получения в ЕЦУ Dallas Lock записей журналов, ведущихся на модуле СДЗ Dallas Lock, необходимо проведение сбора журналов. Сбор журналов может быть проведен при условии наличия сетевого подключения между ЕЦУ и модулем при включении модуля.

12.3.3 Сводка модуля СДЗ Dallas Lock

Вкладка «Сводка» на уровне модуля СДЗ Dallas Lock отображает общее состояние модуля (рис. 176).

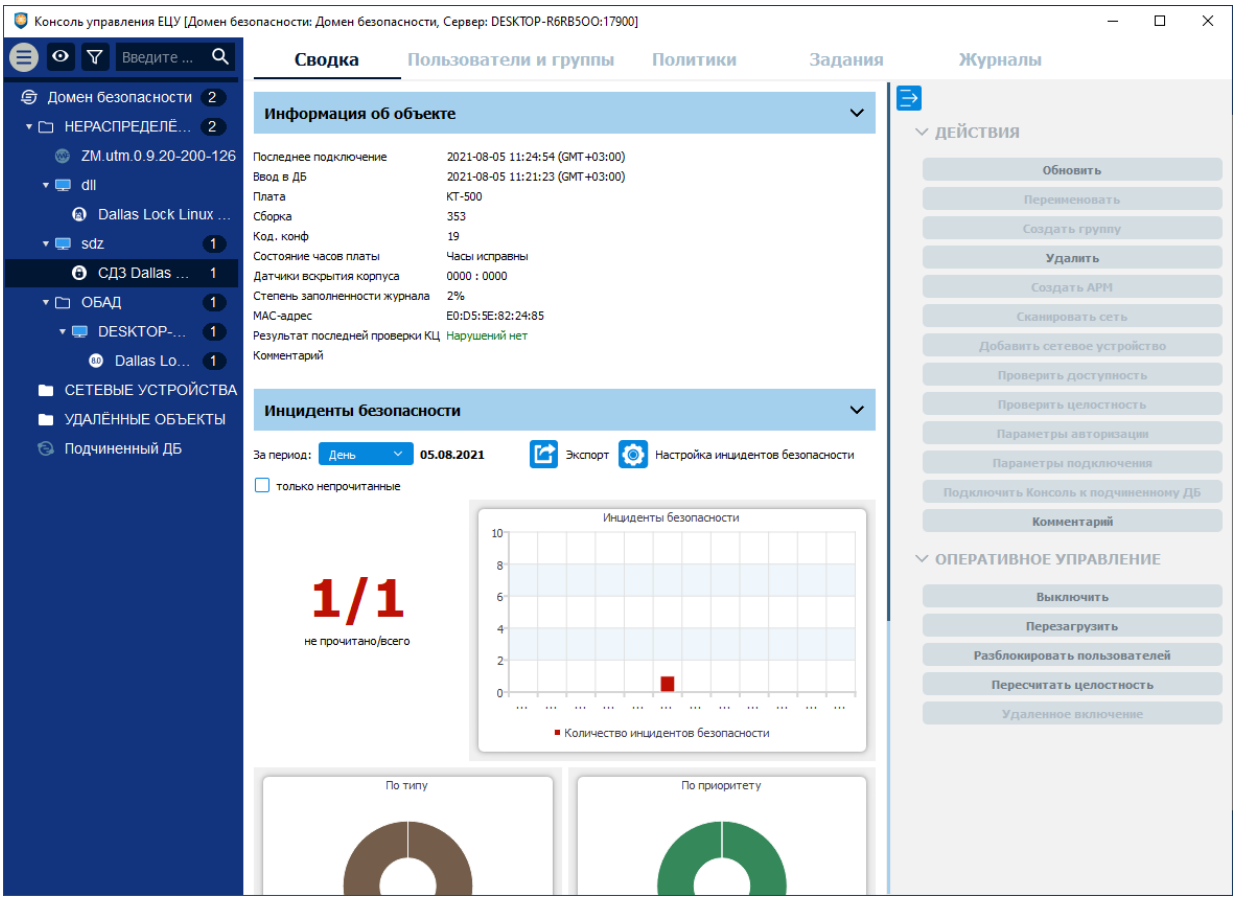

Рис. 176. Вкладка «Сводка»

Доступны следующие разделы информационной панели.

Информация об объекте
В верхней части информационной панели отображается следующая информация о текущем состоянии модуля: • информация о дате и времени последнего подключения; • информация о дате и времени ввода модуля в ДБ; • исполнение печатной платы; • версия прошивки; • код конфигурации; • состояние часов платы; • состояние датчиков вскрытия корпуса; • степень заполненности журналов; • MAC-адрес; • результат последней проверки КЦ; • комментарий к модулю.
Инциденты безопасности
Отображается список инцидентов безопасности модуля с графической панелью. Доступна фильтрация отображаемых событий по периоду и настройка отображения диаграмм (см. «Настройка инцидентов безопасности»). Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное. Поле «Комментарий» доступно для редактирования.

Доступны следующие действия с модулем на панели инструментов:

1. Обновить.
2. Удалить модуль.
3. Комментарий.

Доступны следующие команды оперативного управления на панели инструментов:

1. Выключить.
2. Перезагрузить.
3. Разблокировать пользователей.
4. Пересчитать целостность.

12.3.4 Пользователи и группы модуля СДЗ Dallas Lock

Вкладка «Пользователи и группы» на уровне модуля СДЗ Dallas Lock содержит список глобальных и доменных пользователей и групп, наследуемых с уровней выше по иерархии и созданных на уровне данного модуля, а также модульных пользователей.

Управление пользователями и группами на уровне модуля СДЗ Dallas Lock производится аналогично описанному управлению пользователями и группами в разделе «Пользователи и группы модуля». Для применения изменений на модулях необходима перезагрузка.

12.3.5 Политики модуля СДЗ Dallas Lock

На уровне модуля СДЗ Dallas Lock в списке на вкладе «Политики» доступны только политики, актуальные для СДЗ Dallas Lock (см. «Политики ДБ»).

Настройка политик для модуля производится аналогично настройке политик для группы ДБ (см. «Политики для группы ДБ»). Для применения параметров на модулях необходима перезагрузка.

12.3.6 Задания модуля СДЗ Dallas Lock

На уровне модуля СДЗ Dallas Lock в списке на вкладе «Задания» доступны для создания только задания, актуальные для СДЗ Dallas Lock (рис. 177):

- очистка журнала;
- получение конфигурации;
- получение отчета об аппаратном обеспечении;
- получение отчета по конфигурации;

- применение конфигурации.

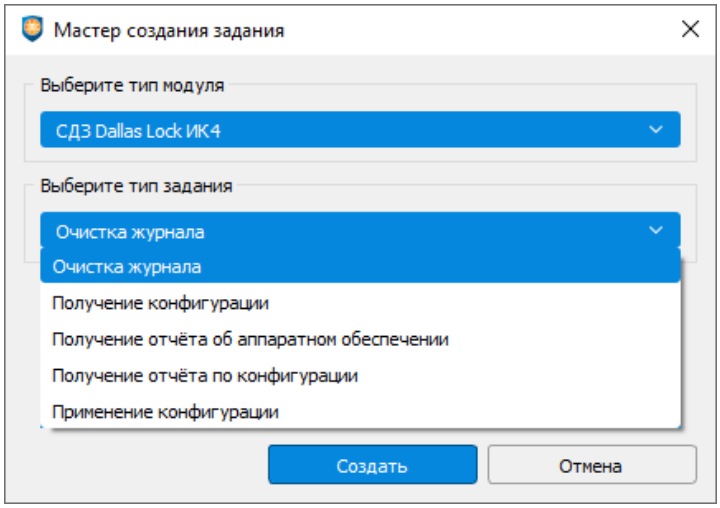

Рис. 177. Мастер создания задания для модуля СДЗ

Работа с заданиями для модуля СДЗ Dallas Lock производится аналогично настройке заданий для ДБ (см. «Задания ДБ»). Для выполнения задания требуется перезагрузка модуля СДЗ Dallas Lock.

12.3.7 Журналы модуля СДЗ Dallas Lock

Вкладка «Журналы» для модуля СДЗ Dallas Lock позволяет просматривать журналы безопасности модуля (рис. 178).

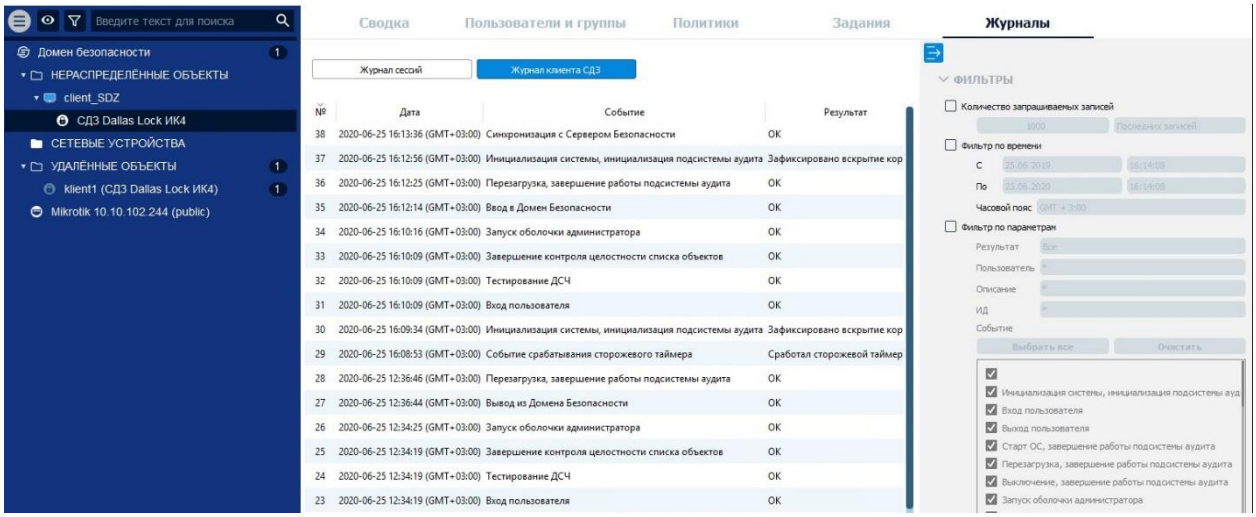

Рис. 178. Вкладка «Журналы»

Для модуля СДЗ Dallas Lock доступны:

- «Журнал сессий»;
- «Журнал клиента СДЗ».

Работа с журналами модулей описана в разделе «Журналы модуля».
Для получения записей журнала с модуля требуется перезагрузка модуля СДЗ Dallas Lock.

13 МОДУЛЬ WAF DALLAS LOCK

13.1 Ввод модуля в ДБ

Ввести модуль WAF Dallas Lock в Домен безопасности можно через веб-интерфейс модуля.

Внимание! При вводе модуля WAF Dallas Lock в ДБ должен быть соблюден ряд условий:

- в ЛВС должен быть работающий сервер ЕЦУ;
- между модулем и сервером ЕЦУ должен быть свободный обмен пакетами по TCP/IP порту 17900.

Для ввода модуля в ДБ через веб-интерфейс модуля необходимо:

1. Убедиться, что сервер ЕЦУ доступен по сети.
2. Запустить веб-интерфейс модуля и авторизоваться.
3. Перейти на вкладку «Настройки» → пункт «Настройки модуля ЕЦУ» (рис. 179).

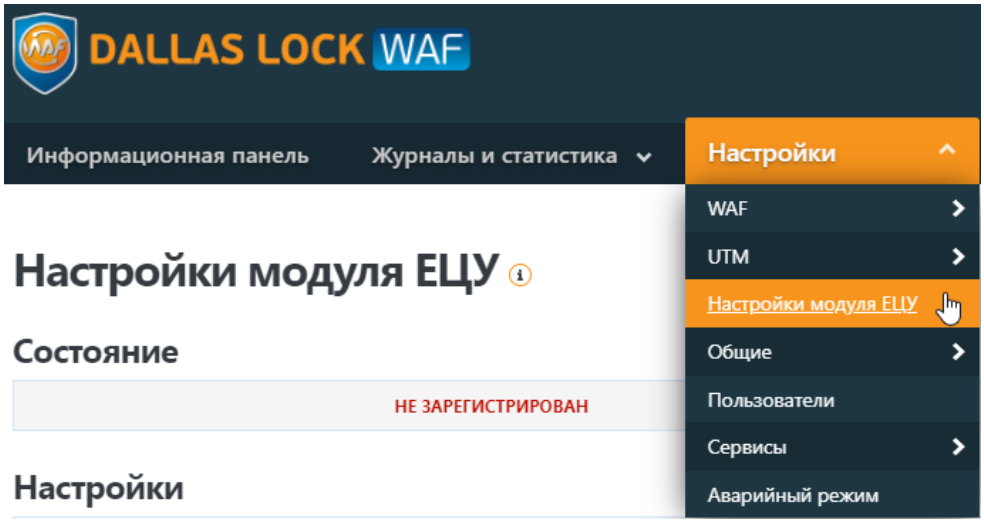

Рис. 179. Вкладка «Настройки»

4. В разделе «Настройки» заполнить параметры ввода в ДБ (рис. 180):
   - имя модуля;
   - сетевой адрес сервера ЕЦУ;
   - ключ доступа к ДБ.

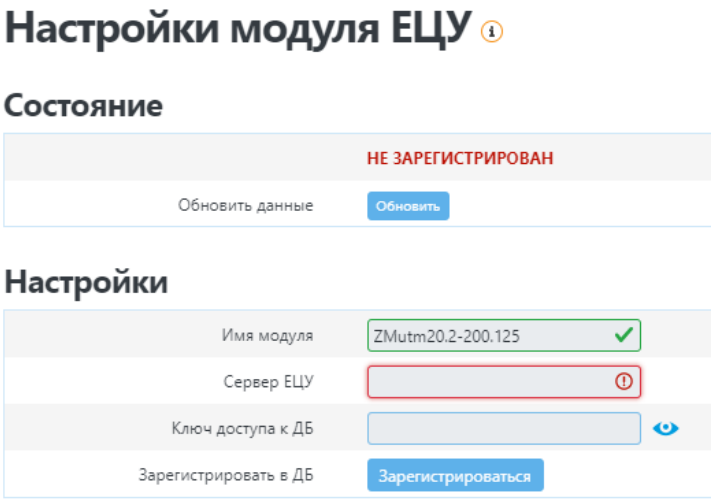

Рис. 180. Настройки модуля ЕЦУ

5. Далее необходимо нажать кнопку «Зарегистрироваться».

Если процесс ввода модуля в ДБ прошел успешно, то через некоторое время поля с настройками станут недоступными для редактирования, в разделе «Состояние» появится информация о Домене безопасности ЕЦУ Dallas Lock (рис. 181).

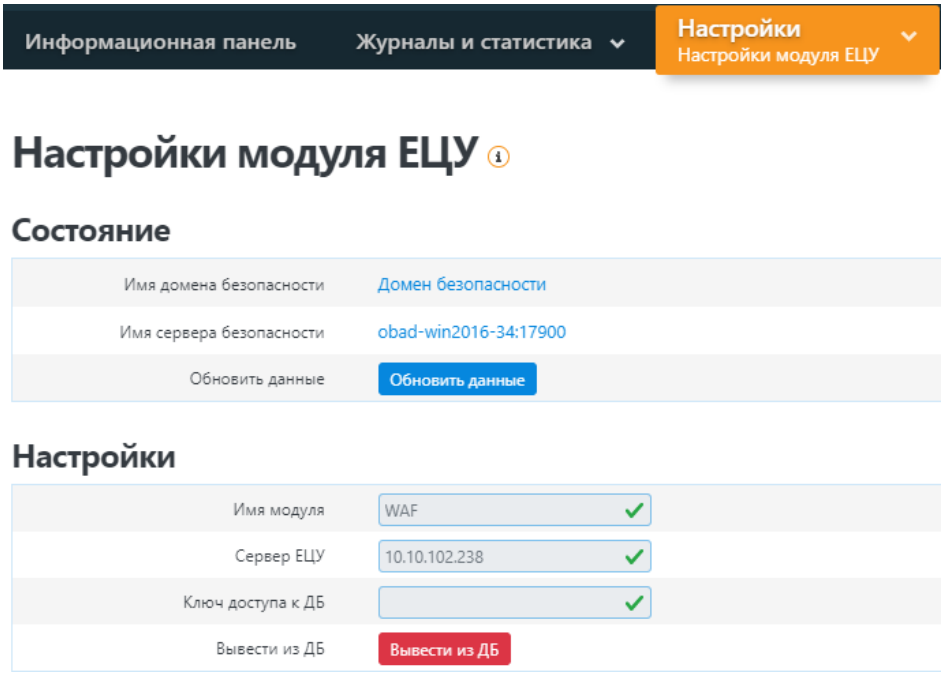

Рис. 181. Состояние

В Консоли ЕЦУ в дереве ДБ в группе «Нераспределенные объекты» появится модуль WAF (без АРМ) с соответствующим именем (рис. 182).

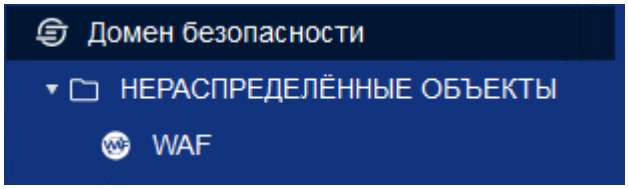

Рис. 182. Иконка модуля в дереве ДБ

После успешного ввода модуля в состав ДБ ЕЦУ Dallas Lock, на WAF автоматически настраивается синхронизация по времени с ЕЦУ Dallas Lock.

13.2 Вывод модуля из ДБ

Вывести модуль WAF Dallas Lock из Домена безопасности можно следующими способами:

- с помощью Консоли ЕЦУ (см. «Настройка модуля»);
- через веб-интерфейс модуля WAF Dallas Lock.

Для вывода модуля через веб-интерфейс необходимо:

1. Запустить веб-интерфейс WAF Dallas Lock и авторизоваться.
2. Перейти на вкладку «Настройки» → пункт «Настройки модуля ЕЦУ».
3. В разделе «Настройки» нажать кнопку «Вывести из ДБ» (рис. 183).

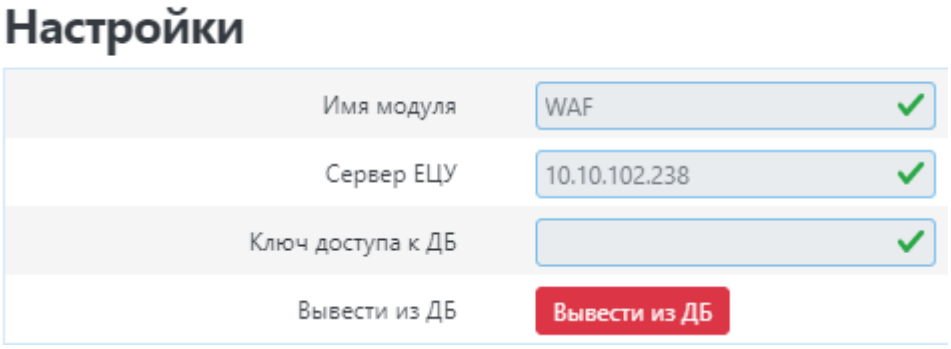

Рис. 183. Вывод из ДБ

Если процесс вывода модуля из ДБ прошел успешно, то через некоторое время поля с настройками модуля ЕЦУ Dallas Lock станут доступными для редактирования, в разделе «Состояние» отобразится статус «НЕ ЗАРЕГИСТРИРОВАН».
В Консоли ЕЦУ удаленный модуль переместится в базовую группу «Удаленные объекты» дерева ДБ.

Примечание. При отсутствии сетевого подключения к Службе ЕЦУ, модуль может быть выведен из Домена безопасности ЕЦУ принудительно. При этом, в Консоли ЕЦУ такой модуль продолжит отображаться, но его статус будет «Недоступен».
Поэтому, каждый модуль, выведенный из состава ДБ во время отсутствия связи со Службой ЕЦУ, необходимо дополнительно удалять вручную из Консоли ЕЦУ.

13.3 Настройка модуля WAF Dallas Lock

В дереве Домена безопасности ЕЦУ Dallas Lock присутствуют зарегистрированные в ДБ модули WAF Dallas Lock.
Значки объектов, обозначающих модули WAF Dallas Lock, зависят от состояния модуля и могут принимать следующий вид:

— модуль подключен;

— связь с модулем отсутствует.

Настройки на уровне модуля отображаются на нескольких основных вкладках.

Примечание. В случае если два или более модулей WAF подключены к ЕЦУ Dallas Lock, и на одном из них происходит блокировка каких-либо атакующих узлов — данные блокировки передаются через ЕЦУ Dallas Lock на все подключенные к ЕЦУ Dallas Lock модули WAF Dallas Lock. После этого, все подключенные к ЕЦУ Dallas Lock модули WAF Dallas Lock — блокируют атакующий хост до истечения времени блокировки.

13.3.1 Синхронизация

Для отправки на ЕЦУ Dallas Lock сведений о модуле WAF Dallas Lock и приведения в соответствие системного времени необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между ЕЦУ Dallas Lock и модулем:

- при включении модуля;
- периодически (см. «Параметры работы модулей»);
- по команде пользователя:
  - из Консоли ЕЦУ;
  - посредством веб-интерфейса модуля WAF Dallas Lock.

Синхронизация по команде из Консоли ЕЦУ

Команда «Синхронизировать» в Консоли ЕЦУ для WAF Dallas Lock доступна на вкладке «Сводка» на уровне модуля WAF Dallas Lock в дереве Домена безопасности на панели инструментов «Оперативное управление» (рис. 184).

Рис. 184. Панель инструментов «Оперативное управление»

Синхронизация по команде из веб-интерфейса модуля WAF Dallas Lock

Для проведения синхронизации с Доменом безопасности ЕЦУ Dallas Lock по команде из веб-интерфейса модуля WAF Dallas Lock необходимо выполнить следующие шаги:

1. Запустить веб-интерфейс модуля и авторизоваться.
2. Перейти на вкладку «Настройки» → пункт «Настройки модуля ЕЦУ».
3. В разделе «Состояние» нажать кнопку «Обновить» (рис. 185).

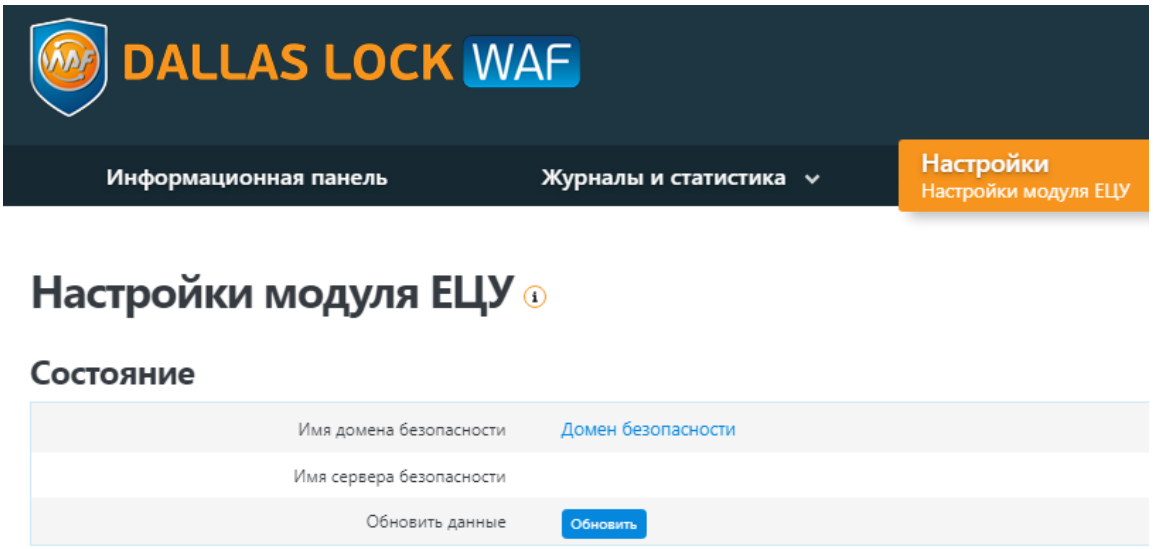

Рис. 185. Кнопка «Обновить»

13.3.2 Сбор журналов

Для получения в ЕЦУ Dallas Lock записей журналов, ведущихся на модуле, необходимо проведение сбора журналов. Сбор журналов может быть проведен при условии наличия сетевого подключения между ЕЦУ Dallas Lock и модулем:

- при включении модуля;
- периодически (см. «Параметры работы модулей»);
- по команде пользователя из Консоли ЕЦУ.

Сбор журналов по команде из Консоли ЕЦУ

Команда «Собрать журналы» в Консоли ЕЦУ для модуля WAF Dallas Lock доступна на вкладке «Сводка» на уровне модуля в дереве Домена безопасности на панели инструментов «Оперативное управление» (рис. 184).

13.3.3 Сводка модуля WAF Dallas Lock

Вкладка «Сводка» на уровне модуля WAF Dallas Lock отображает общее состояние модуля (рис. 186).

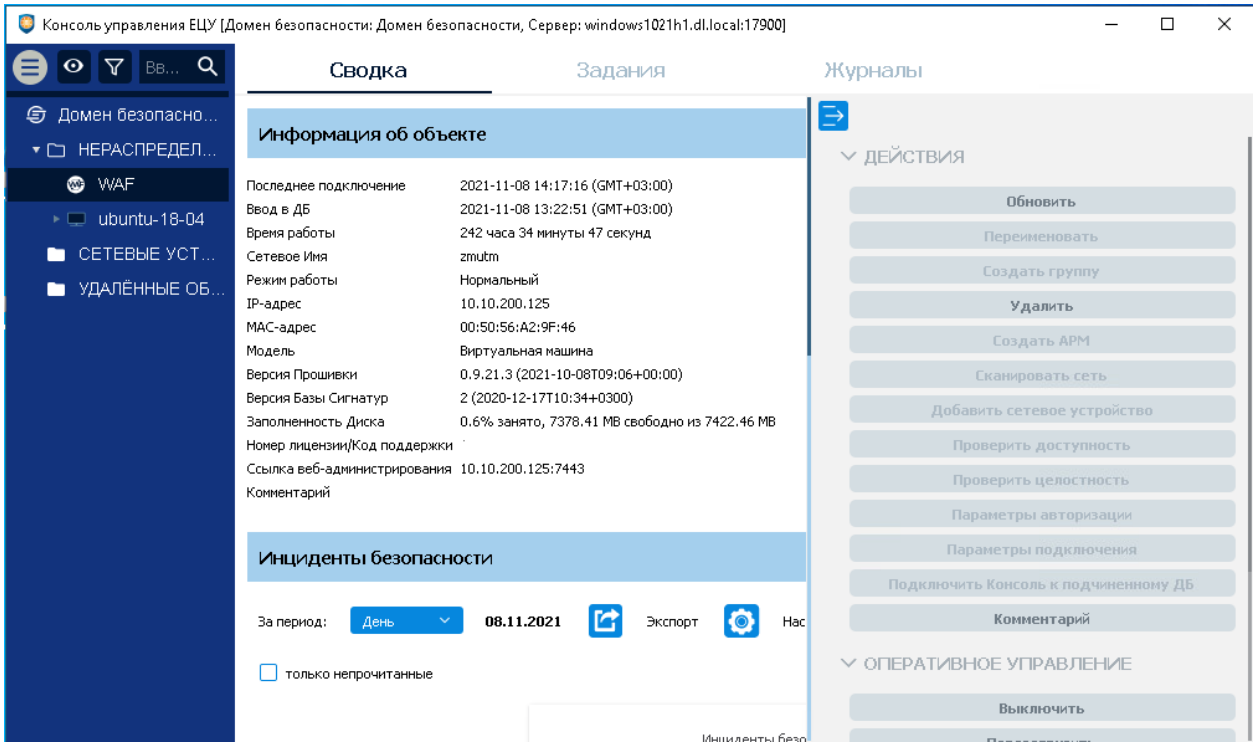

Рис. 186. Вкладка «Сводка»

Доступны следующие разделы информационной панели.

Информация об объекте
В верхней части информационной панели отображается следующая информация о текущем состоянии модуля: • информация о дате и времени последнего подключения модуля; • информация о дате и времени ввода модуля в ДБ; • время работы; • сетевое имя; • режим работы (нормальный/аварийный); • IP-адрес; • MAC-адрес; • модель; • версия пошивки; • версия базы сигнатур; • информация о заполненности диска; • номер лицензии и код технической поддержки; • ссылка для веб-администрирования; • комментарий к модулю.

Инциденты безопасности
Отображается список инцидентов безопасности модуля с графической панелью. Доступна фильтрация отображаемых событий по периоду и настройка отображения диаграмм (см. «Настройка инцидентов безопасности»). Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное. Поле «Комментарий» доступно для редактирования.

Доступны следующие действия с модулем на панели инструментов:

1. Обновить.
2. Удалить.
3. Комментарий.

Доступны следующие команды оперативного управления на панели инструментов:

1. Выключить.
2. Перезагрузить.
3. Собрать журналы.
4. Синхронизировать.
5. Включить аварийный режим.
6. Отключить аварийный режим.
7. Сбросить блокировки.
8. Открыть web-администрирование.

13.3.4 Задания модуля WAF Dallas Lock

На уровне модуля WAF Dallas Lock в списке на вкладе «Задания» доступны для создания только задания, актуальные для WAF Dallas Lock (рис. 187):

- восстановить резервную копию;
- обновление базы разрешающих правил;
- сбор журналов;
- сброс к заводским настройкам;
- создать резервную копию.

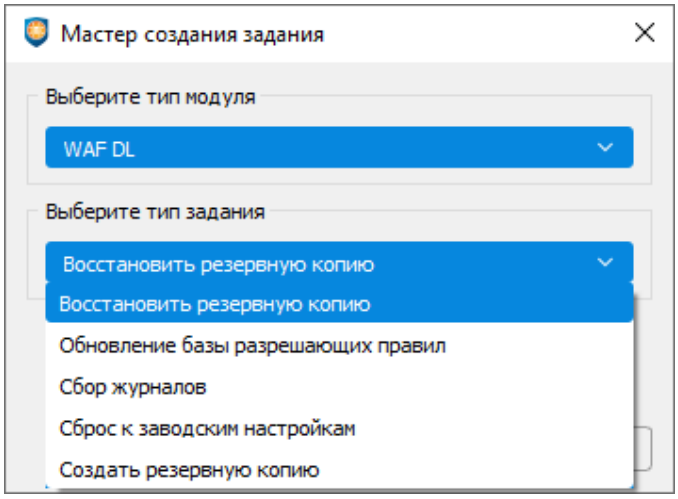

Рис. 187. Мастер создания задания для модуля WAF Dallas Lock

Работа с заданиями для модуля WAF Dallas Lock производится аналогично настройке заданий для ДБ (см. «Задания ДБ»). Для выполнения задания требуется синхронизация с модулем.

13.3.5 Журналы модуля WAF Dallas Lock

Вкладка «Журналы» для модуля WAF Dallas Lock позволяет просматривать журналы безопасности модуля (рис. 188).

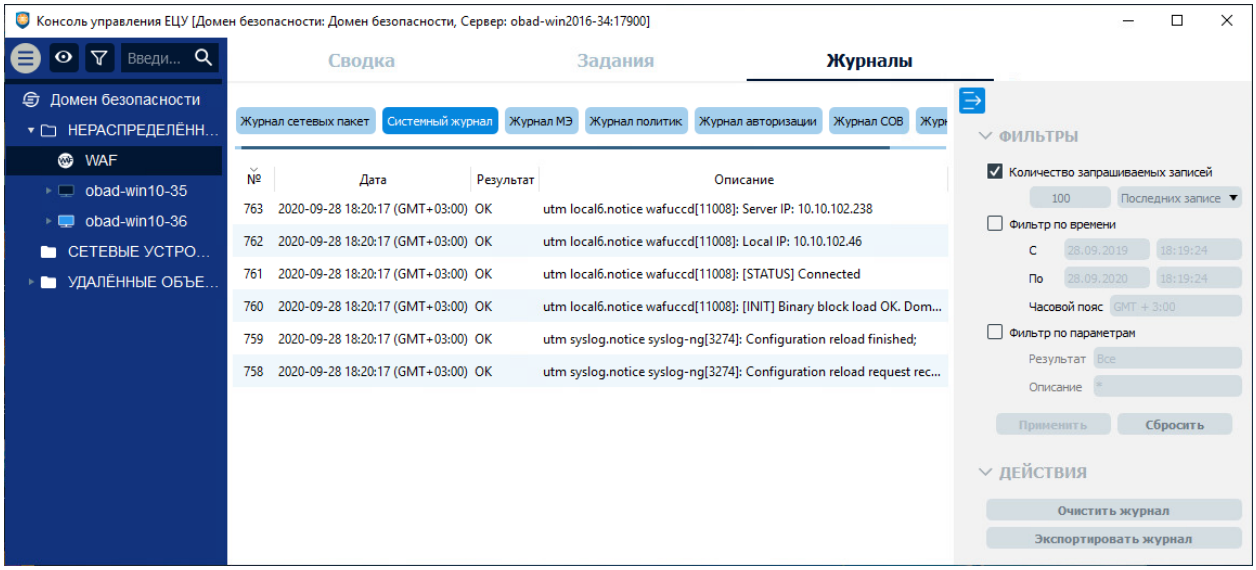

Рис. 188. Вкладка «Журналы»

Для модуля WAF Dallas Lock доступны:

- «Журнал сетевых пакетов»;
- «Системный журнал»;
- «Журнал МЭ»;
- «Журнал политик»;
- «Журнал авторизации»;
- «Журнал СОВ»;
- «Журнал WAF».

Работа с журналами модулей описана в разделе «Журналы модуля».

Для получения записей журналов с модуля требуется выполнение сбора журналов.

14 АГЕНТ ЕЦУ

Независимый агент для ПК (далее — Агент ЕЦУ) предназначен для передачи базовой информации об устройстве (системные журналы, версия ОС, IP- и MAC-адреса) на которое он установлен.

14.1 Требования к аппаратному и программному обеспечению

Агент ЕЦУ представляет собой службу, работающую в фоновом режиме, устанавливаемую на ПК, для последующего ввода в ДБ ЕЦУ Dallas Lock. Агентом ЕЦУ поддерживаются следующие типы операционных систем семейства Windows:

- Windows 7 x32, x64 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
- Windows Server 2012 x64 (Foundation, Essentials, Standard, Datacenter);
- Windows 8.1 x32, x64 (Core, Pro, Enterprise);
- Windows Server 2012 R2 x64 (Foundation, Essentials, Standard, Datacenter);
- Windows 10 x32, x64 (Enterprise, Education, Pro, Home);
- Windows Server 2016 x64 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server);
- Windows Server 2019 x64 (Standard, Datacenter, Essentials);
- Windows Server 2022 x64 (Standard, Datacenter);
- Windows 11 x64 (Home, Pro, Enterprise, Education);

и семейства Linux (x64):

- Debian 10;
- Debian 11;
- CentOS 7;
- CentOS 8;
- Red Hat Enterprise Linux 8;
- Ubuntu 18.04 LTS;
- Ubuntu 20.04 LTS;
- Astra Linux Common Edition (Орел) 2.12;
- Astra Linux Special Edition (Смоленск) 1.6;
- Astra Linux Special Edition (Смоленск) 1.7;
- Альт Рабочая Станция 9.0;
- Альт Рабочая Станция 9.1;
- Альт Рабочая Станция 9.2;
- Альт Рабочая Станция 10.0;
- Альт Рабочая Станция 10.1;
- Альт Рабочая Станция К 10.0;
- Альт Рабочая Станция К 10.1;
- Альт Сервер 9;
- Альт Сервер 10;
- Альт Сервер 10.1;
- РЕД ОС 7.3 Муром.

14.2 Установка и удаление Агента ЕЦУ

14.2.1 Локальная установка Агента ЕЦУ

До установки Агента ЕЦУ на ОС Linux, необходимо произвести дополнительные действия в терминале:

- для Debian, Ubuntu, Astra Linux, Альт Рабочая Станция выполнить команду:
  apt-get update
- для CentOS, Red Hat Enterprise Linux, РЕД ОС выполнить команду:
  yum repolist ; yum makecache

Для установки Агента ЕЦУ необходимо запустить установочный файл uccAgentInst, который

находится в корневой директории дистрибутива (или выбрать данное действие в меню окна autorun).

Примечание. При установке Агента ЕЦУ на ПК с ОС Linux, перед запуском установочного файла, необходимо проверить, является ли файл «uccAgentInst» исполняемым. Для этого можно воспользоваться следующей командой:
chmod a+x <путь к файлу>.run

Примечание. Для подключения к Агенту ЕЦУ по VNC требуется дополнительно открыть TCP-порт 17902, исходящее подключение.

Если Агент ЕЦУ устанавливается на ПК, не оснащенный приводом компакт-дисков, а дистрибутив поставляется именно на CD-диске, то можно скопировать с диска необходимый установочный файл на данный ПК любым удобным способом: через ЛВС, USB-Flash накопитель и др.

После запуска программы установки необходимо выполнять действия по подсказкам программы. Выполнение следующего шага установки осуществляется с помощью кнопки «Далее». На каждом шаге установки предоставляется возможность отмены установки с возвратом произведенных изменений. Для этого служит кнопка «Отмена».

1. После запуска приложения на экране будет выведено окно для подтверждения операции. После подтверждения запустится мастер установки Агента ЕЦУ Dallas Lock (рис. 189).

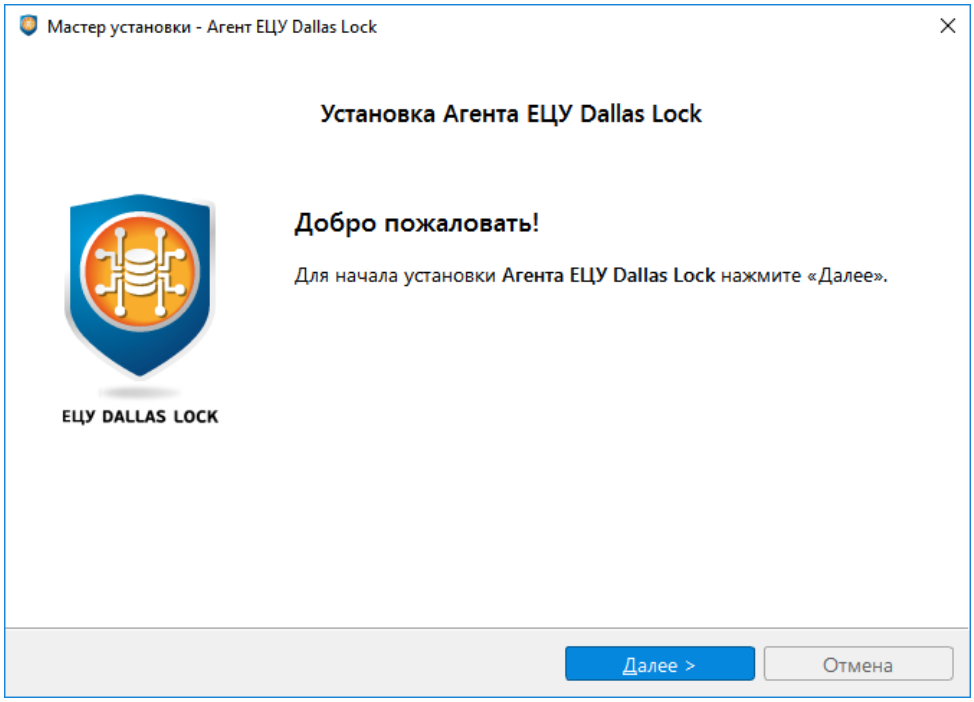

Рис. 189. Окно начала установки Агента ЕЦУ

Для продолжения установки нажать кнопку «Далее».

2. На следующем шаге можно сразу ввести компьютер в ДБ, установив флаг напротив «Ввести компьютер в Домен Безопасности». После установки флага, станут доступны для изменения параметры регистрации Агента ЕЦУ в ДБ (рис. 190).

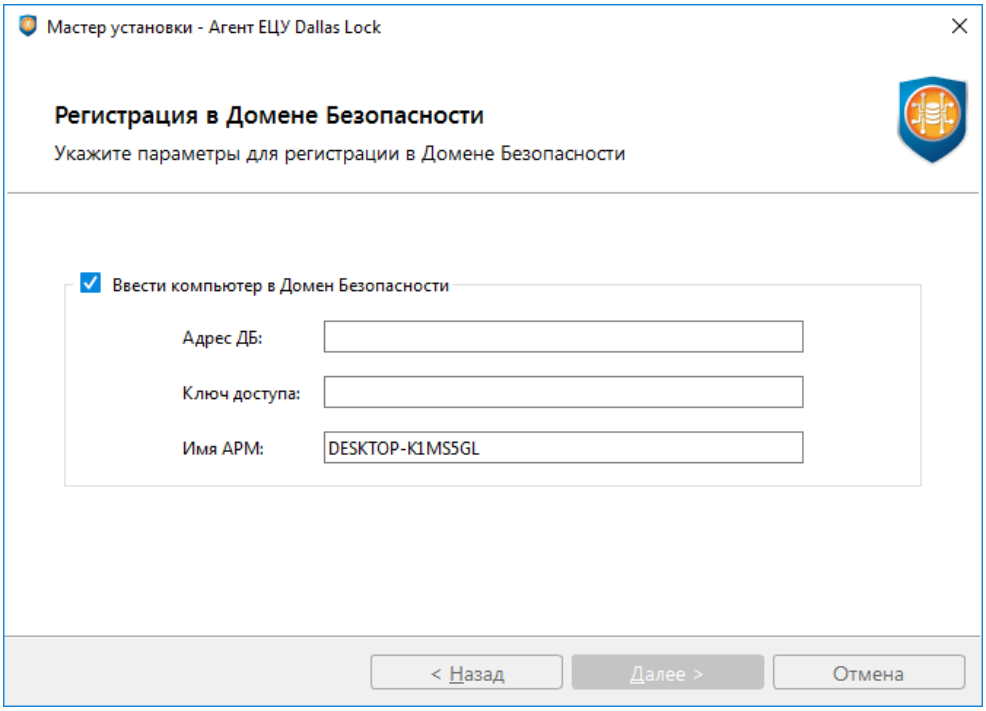

Рис. 190. Регистрация Агента ЕЦУ в ДБ

После нажатия на кнопку «Далее» выполняется проверка введенных для регистрации данных. В случае успешной проверки данных, произойдет переход к следующему шагу.
Чтобы пропустить ввод Агента ЕЦУ в ДБ во время установки, нужно нажать на кнопку «Далее».

3. Затем необходимо выбрать режим работы Агента ЕЦУ (рис. 191):
   - стандартный режим;
   - скрытый режим (позволяет скрыть присутствие Агента на ПК от пользователя).

Внимание! Сменить режим работы Агента ЕЦУ после установки невозможно.

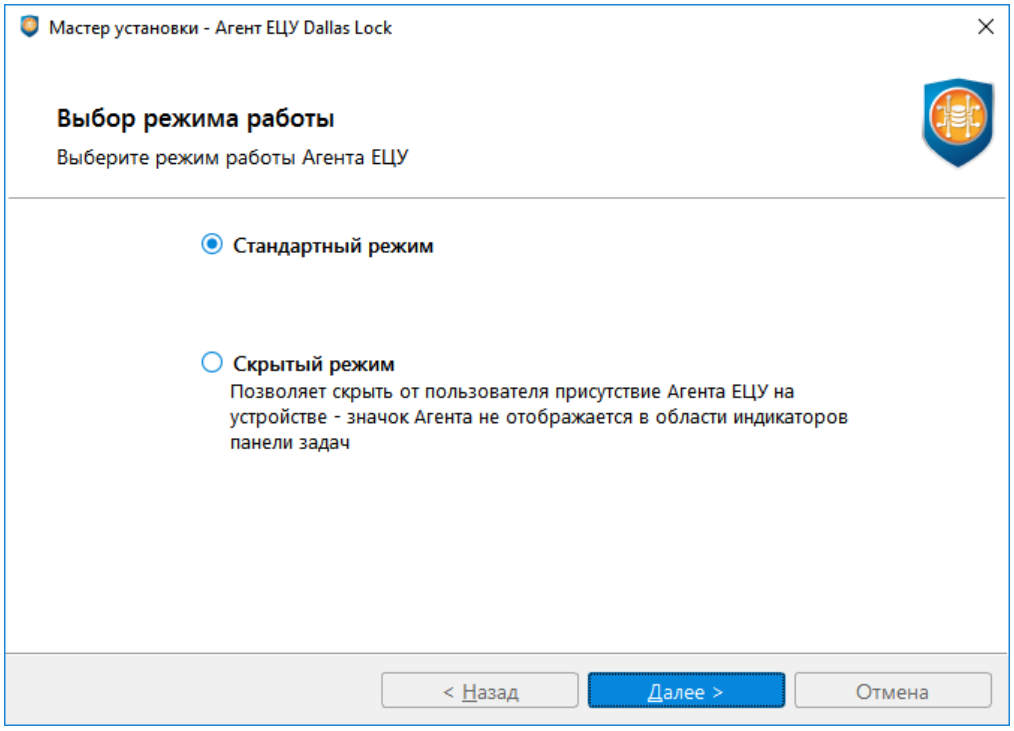

Рис. 191. Выбор режима работы Агента ЕЦУ

Для продолжения установки нажать кнопку «Далее».

4. Следующим шагом нужно проверить параметры установки (рис. 192) и нажать кнопку «Установить».

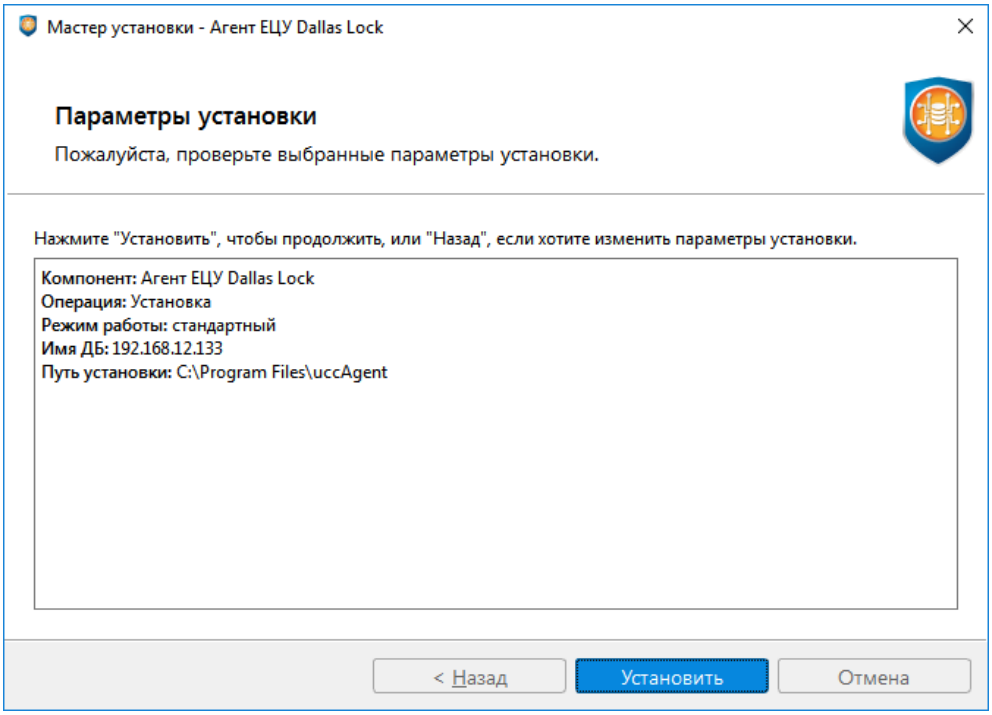

Рис. 192. Проверка параметров установки Агента ЕЦУ

5. Далее возможно наблюдать за процессом установки (рис. 193). Если процесс прошел без ошибок, необходимо нажать кнопку «Завершить».

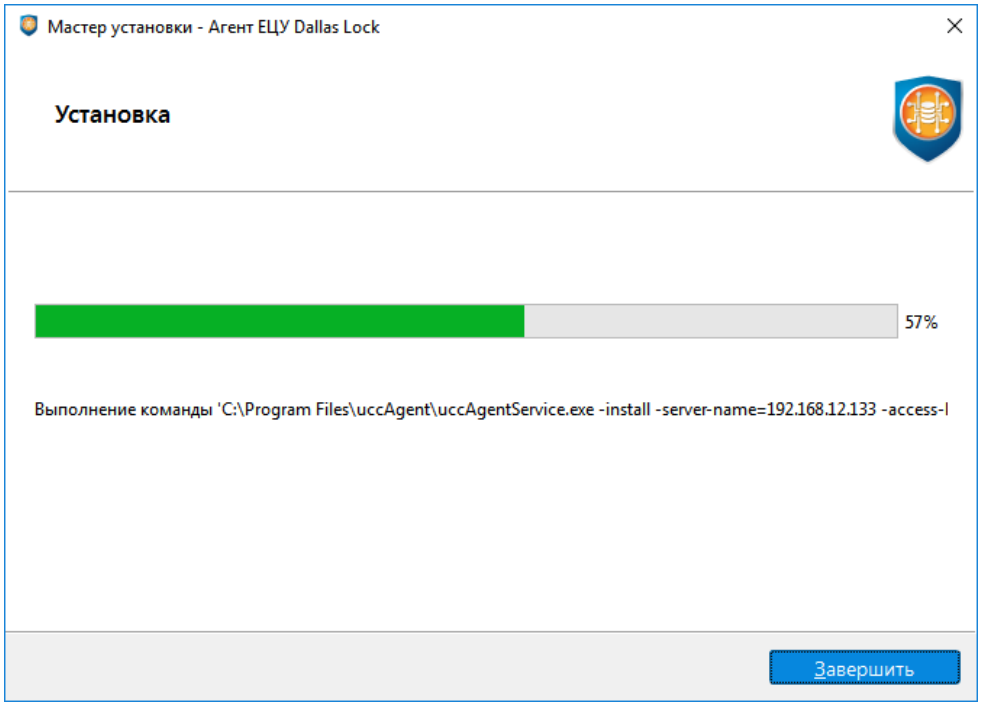

Рис. 193. Процесс установки Агента ЕЦУ

Примечание. 1) Если на АРМе с Linux уже установлены сторонние СЗИ или драйверы на другие аппаратные идентификаторы, и при этом в процессе установки Агента ЕЦУ произошла ошибка установки, которая связана с пакетным менеджером, то может помочь команда *sudo apt --fix-broken install*.
2) Если в процессе установки Агента ЕЦУ на Linux возникает ошибка вида: "...error whiel loading shared libaries: libxcb-xkb.so.1: cannot open shared object file: No such file or directory", то необходимо перед установкой вручную установить пакет "libxcb-xkb1.

После успешного завершения установки Агента ЕЦУ на ПК, в дереве ДБ Консоли ЕЦУ в группе «Нераспределенные объекты» будет создан новый АРМ, в состав которого включен зарегистрированный модуль «Агент ЕЦУ Dallas Lock» (рис. 194).

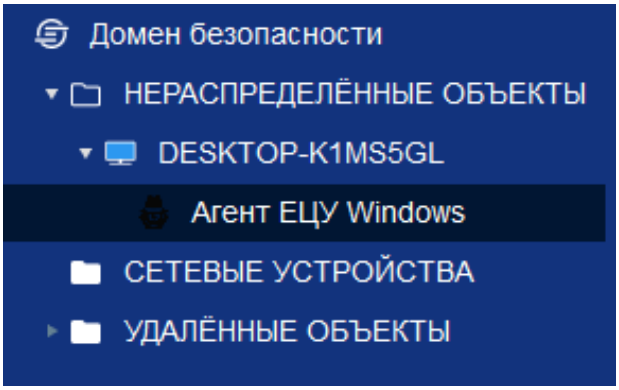

Рис. 194. Отображение Агента ЕЦУ В ДБ

В случае, если введенное имя АРМ уже было в дереве объектов ДБ, и в его составе нет другого модуля Агент ЕЦУ, то в данный АРМ Агент ЕЦУ будет добавлен как модуль «Агент ЕЦУ Windows» или «Агент ЕЦУ Linux».

Примечание. Зарегистрированный в ДБ Агент ЕЦУ должен поддерживать связь с сервером ЕЦУ. В случае, когда серверов ЕЦУ несколько (кластер репликации), Агент ЕЦУ должен иметь сетевой доступ хотя бы к одному серверу из списка кластера серверов ЕЦУ, который есть в списке серверов репликации у данного модуля.

14.2.2 Удаленная установка Агента ЕЦУ Windows

Удаленная установка возможна в следующих вариантах:

- для группы компьютеров, имеющих одинаковые имена и пароли администратора ОС;
- для компьютеров, имеющих индивидуальные имя и пароль администратора ОС, удаленную установку следует выполнять отдельно от других.

Примечание. По умолчанию в операционных системах начиная с Windows 7 доступ к удаленному компьютеру под локальной учетной записью запрещен. Подробную информацию об этом ограничении можно найти на официальном сайте Справки и поддержки компании Microsoft по адресу https://support.microsoft.com/kb/951016 (на английском языке).

Если ранее на данный ПК не выполнялось удаленное развертывание Агента ЕЦУ или модуля СЗИ НСД Dallas Lock, то для разрешения удаленного подключения под локальной учетной записью необходимо в редакторе реестра по пути HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System создать ключ типа dword с именем LocalAccountTokenFilterPolicy со значением «1» («LocalAccountTokenFilterPolicy»=dword:00000001) и перезагрузить компьютер. В крупных сетях с AD данное значение можно распространить через политики.

Примечание. По умолчанию удаленная установка выполняется через порт 445. Если ранее на данный ПК не выполнялось удаленное развертывание Агента ЕЦУ или модуля СЗИ НСД Dallas Lock, то в Брандмауэре Windows данного ПК необходимо открыть порт 445 (создать правило для входящих подключений).

Внимание! Для нескольких целевых ТС централизованную удаленную установку можно осуществить только при выполнении следующих условий:

- целевые ТС входят в тот же домен AD или LDAP, что и АРМ с ЕЦУ Dallas Lock;
- известны имя пользователя и пароль доменной учетной записи с правами администратора домена.

Для удаленной установки Агента ЕЦУ, необходимо выполнить следующие шаги:

1. На удаленном АРМе, на который будет устанавливаться Агент ЕЦУ из Консоли управления ЕЦУ, должен быть доступен для входящих соединений TCP-порт 135 (epmap).
2. Перед централизованной установкой необходимо разместить на компьютере, на котором запущена Консоль ЕЦУ, дистрибутив Агента ЕЦУ Windows.
3. Далее необходимо открыть главное меню Консоли ЕЦУ → «Утилиты» → «Удаленное развертывание Агента ЕЦУ Windows».

   В открывшемся окне необходимо добавить целевые ТС для удаленного развертывания. ТС можно добавить одним из следующих способов, через:

   - ручной ввод адреса — для этого нужно заполнить поля «Порт» и «Введите IP-адрес или сетевое имя компьютера», затем нажать кнопку «Добавить компьютер» (рис. 195);
   - импорт из файла — нажать «Импорт из файла» и прикрепить текстовый файл со списком IP-адресов целевых ТС.

     Примечание. Для файла с IP-адресами возможен только следующий формат списка: в каждой строке файла может быть указан только один IP-адрес без дополнительных символов.
     Пример:
     192.168.0.1
     192.168.0.35
     10.10.112.55

   Затем нажать кнопку «Далее».

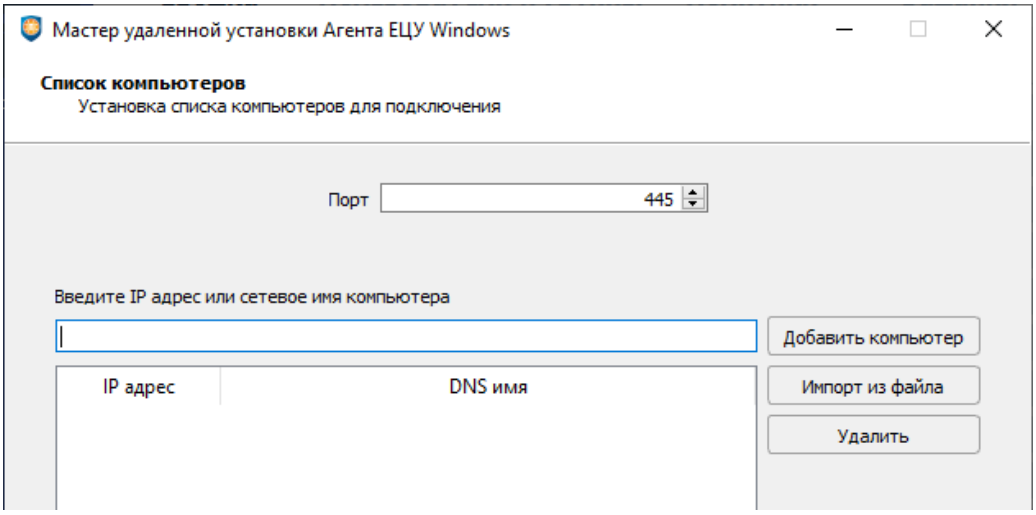

Рис. 195. Начало удаленной установки Агента ЕЦУ Windows

4. В следующем окне (рис. 196) необходимо ввести авторизационные данные:

- логин и пароль администратора ОС на целевых ТС;
- логин и пароль суперпользователя (опционально).

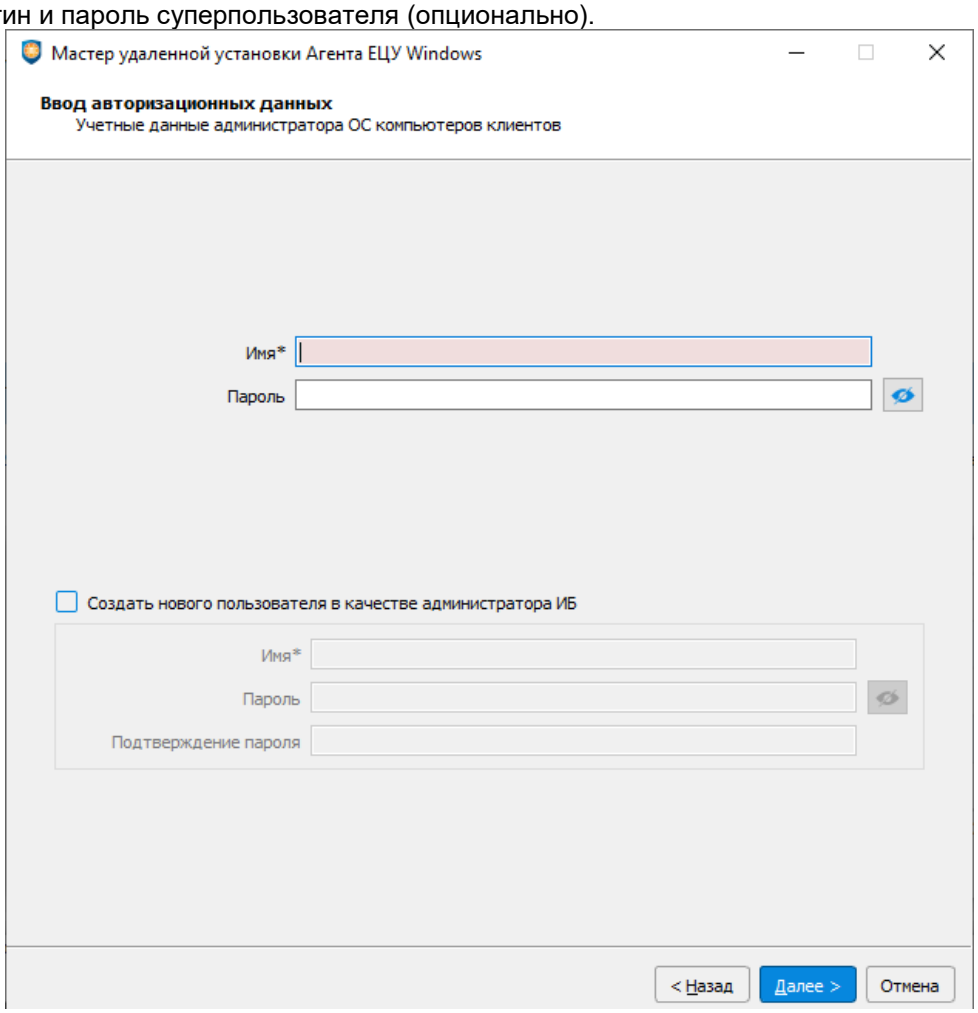

Рис. 196. Ввод авторизационных данных

5. Далее (рис. 197) необходимо указать путь к исходному дистрибутиву Агента ЕЦУ.

Для того, чтобы скрыть от пользователя присутствие Агента ЕЦУ, можно выбрать скрытый режим установив соответствующий флаг.

Для ввода модулей в Домен безопасности ЕЦУ Dallas Lock сразу после установки, можно поставить флаг «Ввод в домен безопасности ЕЦУ», указать имя сервера ЕЦУ и ключ доступа к ДБ ЕЦУ. Затем нажать кнопку «Установить».

Примечание. Если указан неверный ключ доступа к ДБ ЕЦУ, то дальнейшая установка Агента ЕЦУ не будет выполняться.

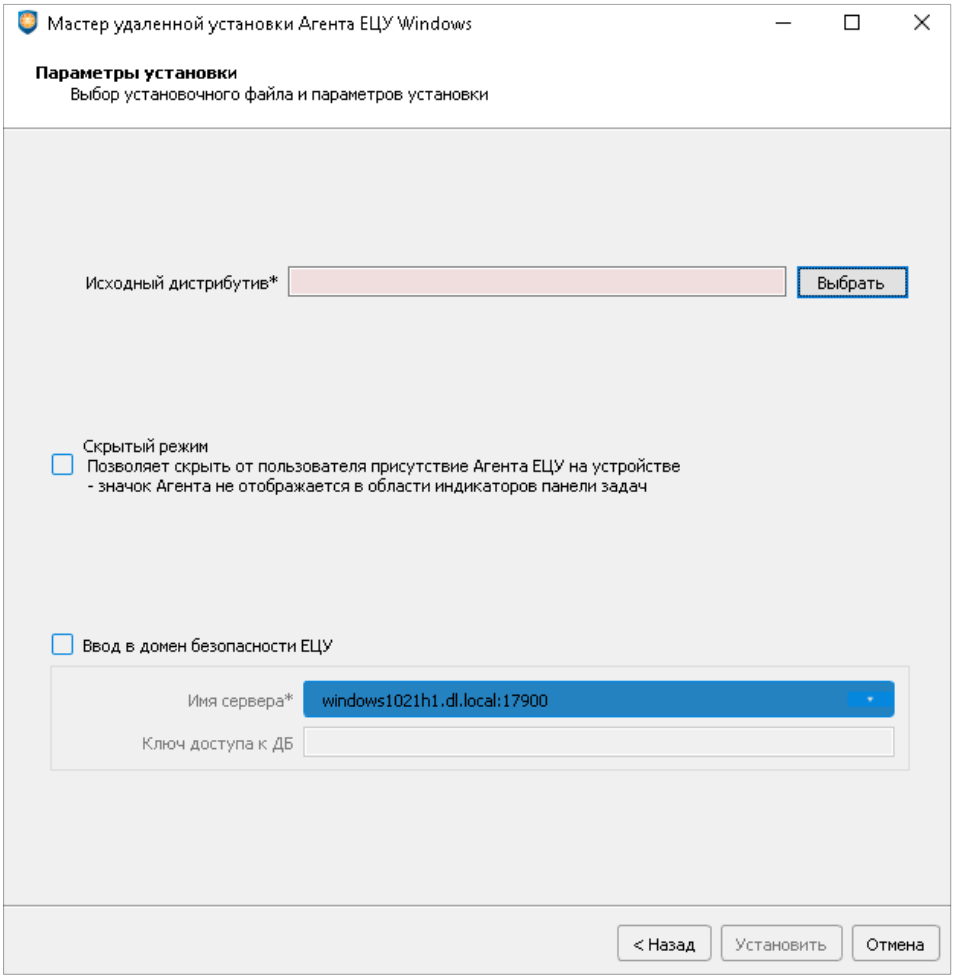

Рис. 197. Параметры установки Агента ЕЦУ

6. В новом окне (рис. 198) можно наблюдать за процессом установки Агента ЕЦУ. По окончанию процесса будет выведено сообщение о результате завершения операции.

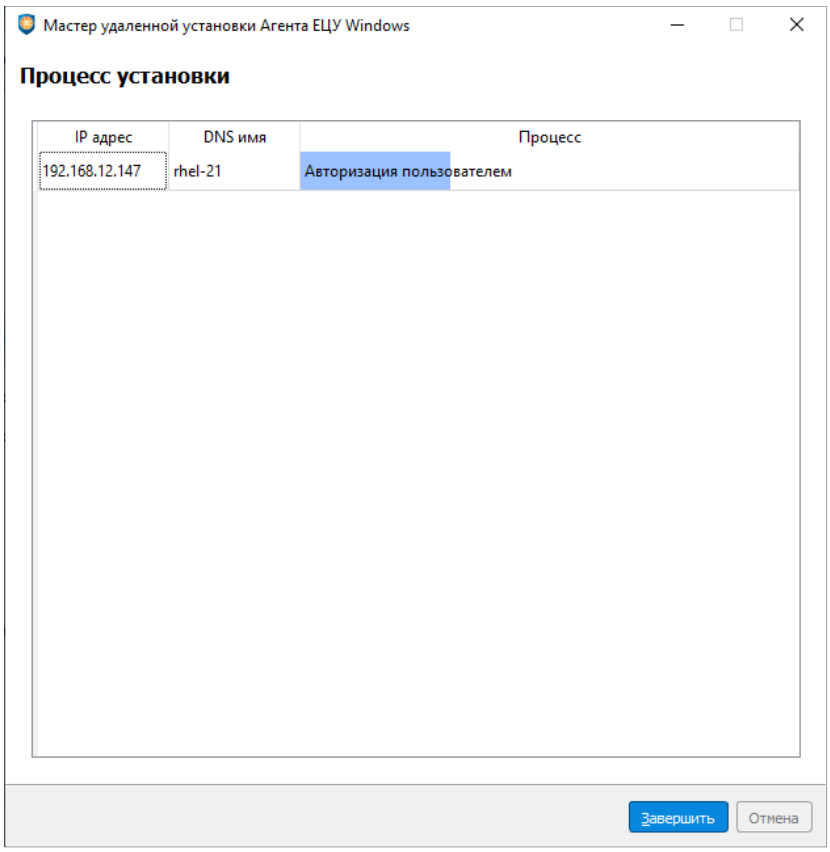

Рис. 198. Процесс установки Агента ЕЦУ

14.2.3 Удаленная установка Агента ЕЦУ Linux

На удаленном АРМе, на который будет устанавливаться Агент ЕЦУ Linux из Консоли управления ЕЦУ, должен быть доступен для входящих соединений TCP-порт 135 (epmap).

Перед централизованной установкой необходимо разместить на компьютере, на котором запущена Консоль ЕЦУ, дистрибутив Агента ЕЦУ Linux.

Для перехода к процессу установки Агента ЕЦУ Linux, необходимо открыть главное меню консоли ЕЦУ → «Утилиты» → «Удаленное развертывание Агента ЕЦУ Linux».

Следующая последовательность действий для удаленной установки Агента ЕЦУ Linux аналогична удаленной установке Агента ЕЦУ Windows (см. «Удаленная установка Агента ЕЦУ Windows»).

Примечание. Если в процессе установки Агента ЕЦУ на Linux возникает ошибка вида: "...error whiel loading shared libaries: libxcb-xkb.so.1: cannot open shared object file: No such file or directory", то необходимо перед установкой вручную установить пакет "libxcb-xkb1.

14.2.4 Удаление Агента ЕЦУ Windows

В ОС Windows необходимо открыть «Пуск» → «Панель управления» → «Программы и компоненты». В появившемся окне из списка выбрать программу «Агент ЕЦУ Dallas Lock», нажать «Удалить» и подтвердить удаление (рис. 199).

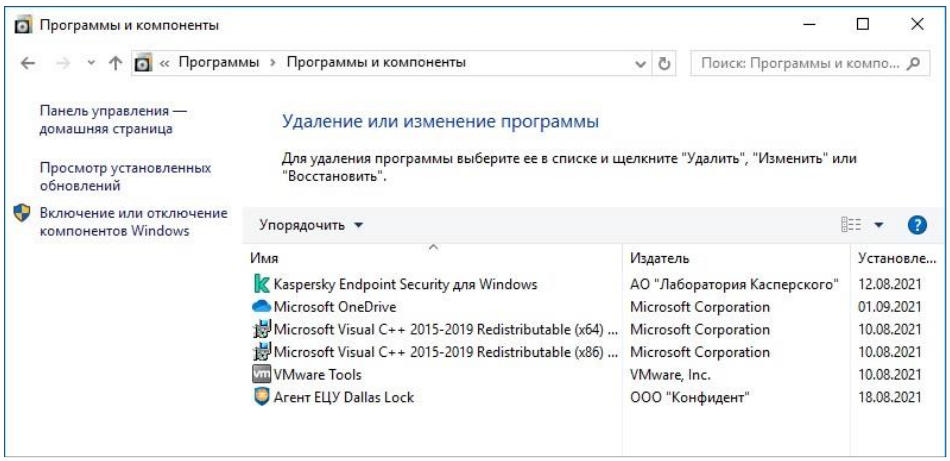

Рис. 199. Удаление Агента ЕЦУ Dallas Lock

Примечание. Мастер удаления Агента ЕЦУ также можно вызвать с помощью запуска установочного дистрибутива.

После подтверждения запустится мастер удаления Агента ЕЦУ Dallas Lock (рис. 200). Для продолжения удаления нажать кнопку «Далее».

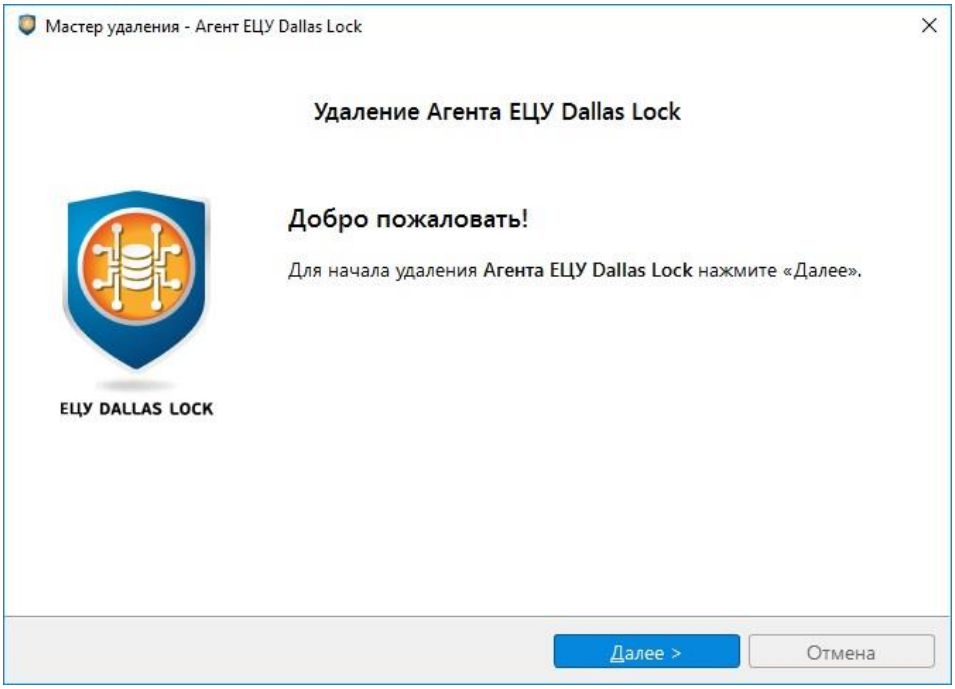

Рис. 200. Окно начала удаления Агента ЕЦУ Dallas Lock

Проверить и подтвердить удаление Агента ЕЦУ (рис. 197).

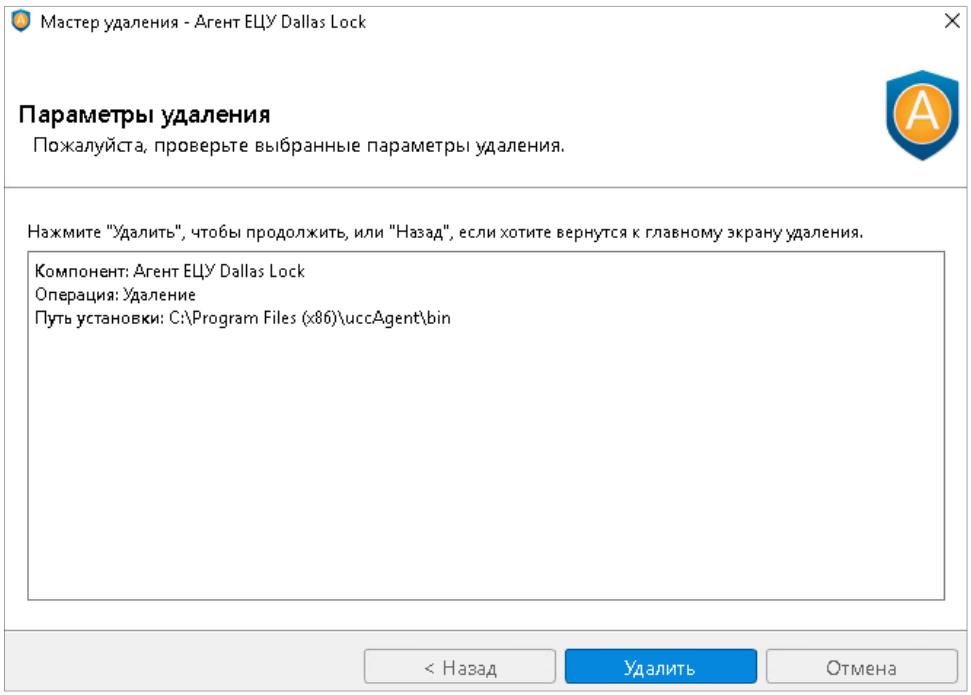

Рис. 201. Параметры удаления

Далее возможно наблюдать за процессом удаления (рис. 202). Если процесс прошел без ошибок, необходимо нажать кнопку «Завершить».

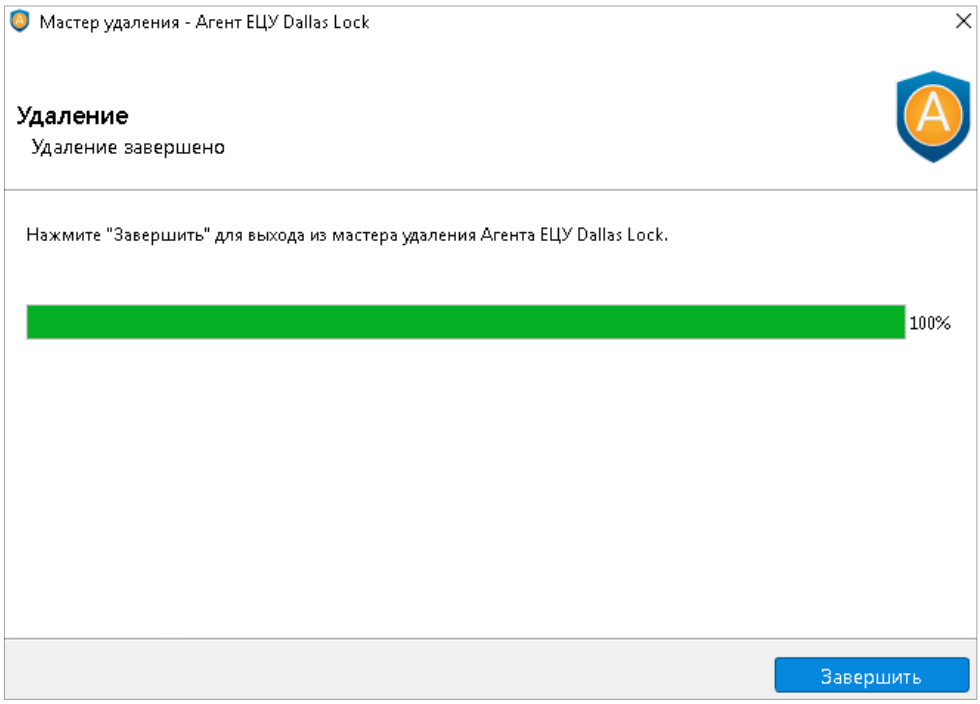

Рис. 202. Процесс удаления Агента ЕЦУ Dallas Lock

14.2.5 Удаление Агента ЕЦУ Linux

Для удаления Агента ЕЦУ необходимо обладать правами администратора ОС (root) на данном ПК. Далее необходимо запустить исполняемый файл uccAgentUninst (путь расположения: /opt/uccAgent/bin/uccAgentUninst) в терминале. Для этого необходимо выполнить в терминале команду:

sudo /opt/uccAgent/bin/uccAgentUninst

После выполнения команды запустится окно мастера удаления Агента ЕЦУ Dallas Lock (рис. 200).

Далее порядок удаления Агента ЕЦУ Dallas Lock аналогичен порядку удаления данной программы в ОС семейства Windows (см. «Удаление Агента ЕЦУ Windows»).

14.3 Регистрация Агента ЕЦУ в ДБ

Зарегистрировать модуль Агент ЕЦУ в Домене безопасности можно следующими способами:

- во время локальной или удаленной установки Агента ЕЦУ (см. «Локальная установка Агента ЕЦУ»);
- путем сканирования сети (см. «Настройка модуля»).

14.4 Настройка модуля Агент ЕЦУ

В Консоли ЕЦУ в дереве ДБ Агенты ЕЦУ отображаются как отдельные модули «Агент ЕЦУ Dallas Lock Windows» или «Агент ЕЦУ Dallas Lock Linux» в составе АРМ. Значки Агента ЕЦУ зависят от состояния модуля и могут принимать следующий вид:

— модуль подключен;

— модуль не подключен.

Примечание. Для корректной работы функции удалённого управления с помощью Агента ЕЦУ необходимо на АРМ с Linux отключить протокол *Wayland*.

14.4.1 Сводка модуля Агент ЕЦУ

Вкладка «Сводка» (рис. 203) отображает общее состояние рабочей станции, на которую установлен Агент ЕЦУ.

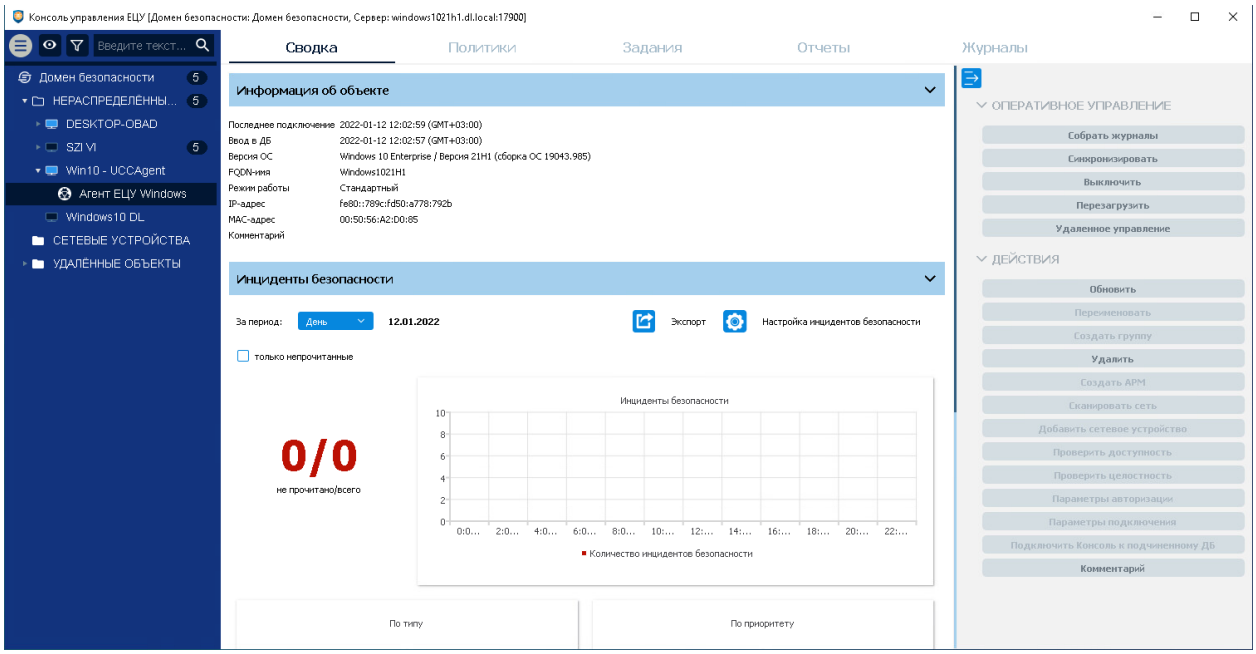

Рис. 203. Вкладка «Сводка» модуля Агент ЕЦУ

Доступны следующие разделы информационной панели.

Информация об объекте
В верхней части информационной панели отображается следующая информация о текущем состоянии модуля: • информация о дате и времени последнего подключения; • информация о дате и времени ввода в ДБ; • версия ОС; • FQDN-имя; • режим работы; • IP-адрес; • MAC-адрес; • комментарий.
Инциденты безопасности
Отображается список инцидентов безопасности с графической панелью. Доступна фильтрация отображаемых событий по периоду и настройка отображения диаграмм (см. «Настройка инцидентов безопасности»). Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное. Поле «Комментарий» доступно для редактирования.

На панели инструментов вкладки «Сводка» (рис. 203) доступны следующие действия:

- «Обновить» — позволяет обновить информацию на вкладке «Сводка»;
- «Удалить» — перемещает в базовую группу «Удаленные объекты» с сохранением журналов;
- «Комментарий» — добавленный комментарий отобразится в разделе «Информация об объекте» вкладки «Сводка».

Для модуля Агент ЕЦУ доступны следующие команды оперативного управления (рис. 204) на панели инструментов:

- «Выключить»;
- «Перезагрузить»;
- «Собрать журналы»;
- «Синхронизировать»;
- «Удаленное управление».

Рис. 204. Оперативное управление

Примечание. Результат выполнения команд оперативного управления не отражается в Журналах ЕЦУ. Также не предусмотрены всплывающие и прочие уведомления о результатах выполнения команд оперативного управления.

14.4.2 Сбор журналов Агента ЕЦУ

Для получения в ЕЦУ Dallas Lock записей журналов, ведущихся на ТС, где установлен Агент ЕЦУ, необходимо проведение сбора журналов. Сбор журналов может быть проведен при условии наличия сетевого подключения между ЕЦУ и ТС с установленным Агентом:

- периодически (см. «Параметры работы модулей»);
- по команде пользователя из Консоли ЕЦУ.

Команда «Собрать журналы» в Консоли ЕЦУ для модуля Агент ЕЦУ доступна на вкладке «Сводка» на панели инструментов «Оперативное управление» (рис. 204).

14.4.3 Подключение к удаленному рабочему столу

Для подключения к удаленному рабочему столу ТС, необходимо:

1. Выбрать нужный модуль Агент ЕЦУ в дереве ДБ;
2. На панели инструментов в разделе «Оперативное управление» выбрать пункт «Удаленное управление» (рис. 204).
3. На АРМ, где установлен Агент ЕЦУ появится окно (Рис. 205), в котором пользователю необходимо выбрать действие с помощью кнопок.

Кнопка «Подключить сейчас» позволяет начать сеанс удаленного подключения.
Кнопка «Отклонить» позволяет отклонить запрос на сеанс удаленного подключения.
Кнопка «Закрыть» позволяет закрыть окно. По истечении времени, установленного политикой «Время ожидания подключения по VNC(секунд)», запрос на удаленное подключение будет прерван.
Если подключение возможно, то на экране отобразится запущенная сессия на выбранном ТС. В ином случае появится сообщение об ошибке (Рис. 206).
Для того чтобы снять блокировку экрана при подключении по VNC, необходимо нажать сочетание клавиш *Win+Del*.

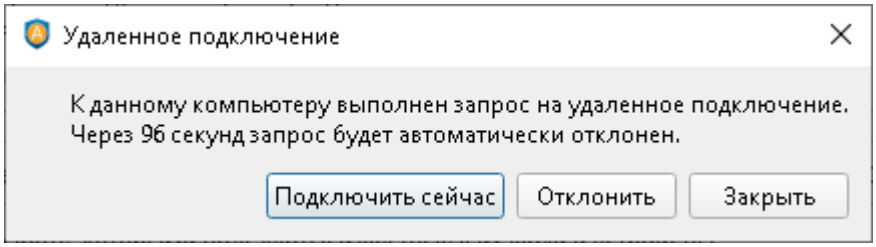

Рис. 205. Окно удаленного подключения на стороне АРМ с Агентом ЕЦУ

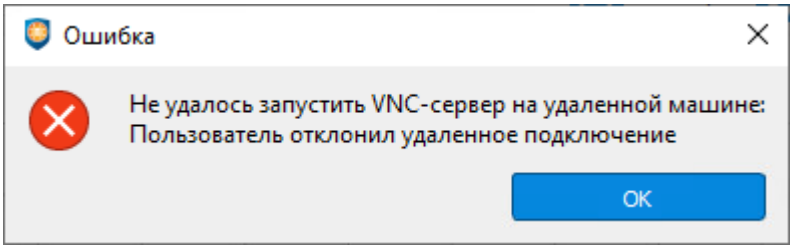

Рис. 206. Ошибка удаленного подключения

Примечание. События, связанные с удаленным подключением к ТС, фиксируются в журнале «Журнал ЕЦУ» (ошибки подключения, начало и завершение удаленного подключения).

Примечание. Одновременное подключение к ТС с установленным Агентом ЕЦУ возможно только с одной Консоли ЕЦУ.

Примечание. При инициировании подключения по VNC консоль ЕЦУ блокируется до момента подключения/отказа в подключении.

Внимание! Подключение к ТС (с установленным Агентом ЕЦУ), расположенным за NAT, по протоколу VNC не поддерживается.

14.4.4 Политики модуля Агент ЕЦУ

На уровне модуля Агент ЕЦУ в списке на вкладе «Политики» (рис. 207) доступны только политики, актуальные для модуля Агент ЕЦУ (см. «Политики ДБ»).

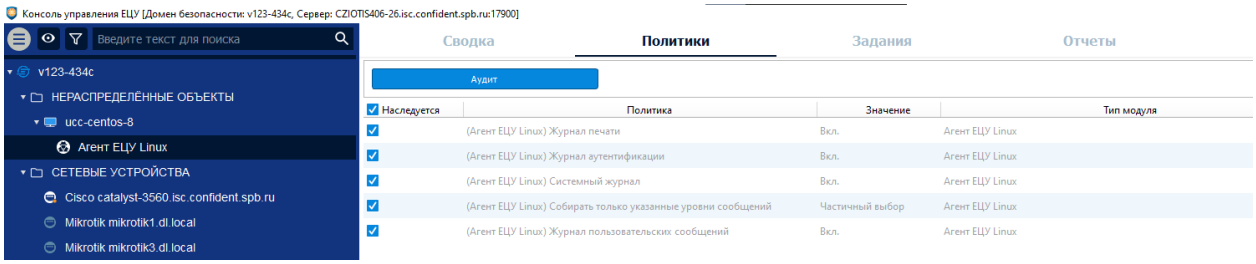

Рис. 207. Вкладка «Политики» модуля Агент ЕЦУ

Настройка политик для модуля производится аналогично настройке политик для группы ДБ (см. «Политики для группы ДБ»). Для применения параметров на модулях необходима синхронизация.

14.4.5 Задания модуля Агент ЕЦУ

На уровне модуля Агент ЕЦУ в списке на вкладе «Задания» доступны для создания только задания, актуальные для Агента ЕЦУ (рис. 208):

- отчет об аппаратном обеспечении;
- удаление Агента ЕЦУ;
- отчет о программном обеспечении.

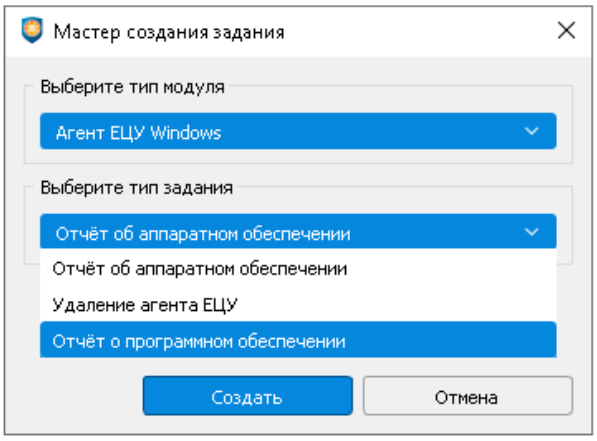

Рис. 208. Мастер создания задания для модуля Агент ЕЦУ Windows

Примечание. Типы заданий одинаковые для модулей Агент ЕЦУ Linux и Агент ЕЦУ Windows.

Работа с заданиями для модуля Агент ЕЦУ производится аналогично настройке заданий для ДБ (см. «Задания ДБ»). Для выполнения задания требуется синхронизация с модулем.

14.4.6 Отчеты модуля Агент ЕЦУ

На уровне модуля Агент ЕЦУ на вкладе «Отчеты» (рис. 209) доступны следующие отчеты модуля:

- отчет об аппаратном обеспечении (содержит информацию о материнской плате, BIOS, процессорах, оперативной памяти, PCI-устройствах и о накопителях);
- отчет о программном обеспечении (содержит информацию обо всех установленных программах (для модулей Агент ЕЦУ Windows) или пакетах (для модулей Агент ЕЦУ Linux)).

Первые полученные для Агента ЕЦУ (отчеты об аппаратном обеспечении и ПО) становятся *эталонными*. Следующие получаемые отчеты сравниваются с эталонным. Первый отчет будет получен ЕЦУ Dallas Lock сразу после процесса регистрации модуля Агент ЕЦУ в ДБ.

На панели инструментов «Действия» вкладки «Отчеты» доступны следующие команды по работе с отчетами модуля Агент ЕЦУ:

- «Обновить» (получить текущий отчет с модуля и сравнить с эталоном);
- «Применить изменения» (сделать текущий отчет эталонным);
- «Сохранить в файл» (позволяет сохранить текущий отчет в текстовом формате).

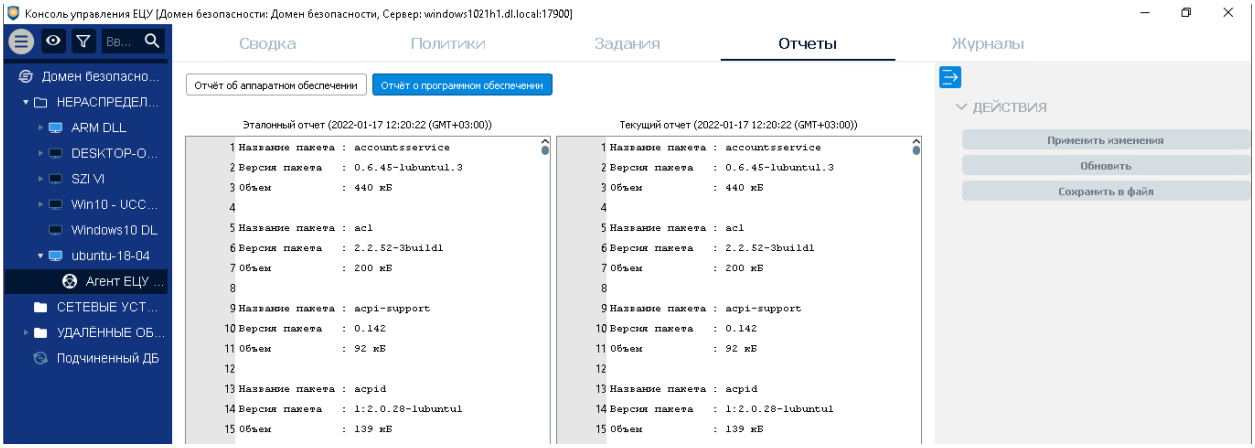

Рис. 209. Отчеты модуля Агент ЕЦУ

Примечание. Периодическое сравнение отчетов можно настроить в разделе «Параметры работы модулей».

Полученный текущий отчет от Агента ЕЦУ сравнивается с эталонным. Результат сравнения отображается в рабочей области вкладки «Отчеты».

Если полученный отчет отличается от эталонного, то происходит нарушение целостности. В таком случае появляется уведомление об инциденте безопасности, а отличия в отчете будут выделены цветом.

При выборе на панели инструментов «Действия» команды «Сохранить в файл», открывается окно «Сохранить отчет об аппаратном обеспечении» или «Сохранить отчет о программном обеспечении», соответственно.

В окне необходимо указать путь для сохранения, и задать имя файла (по необходимости, заполнить информацию о подразделениях и автоматизированной системе).

В шапке отчета дополнительно будет зафиксирована информация о пользователе, инициировавшем составление отчета, дата составления отчета и имя компьютера.

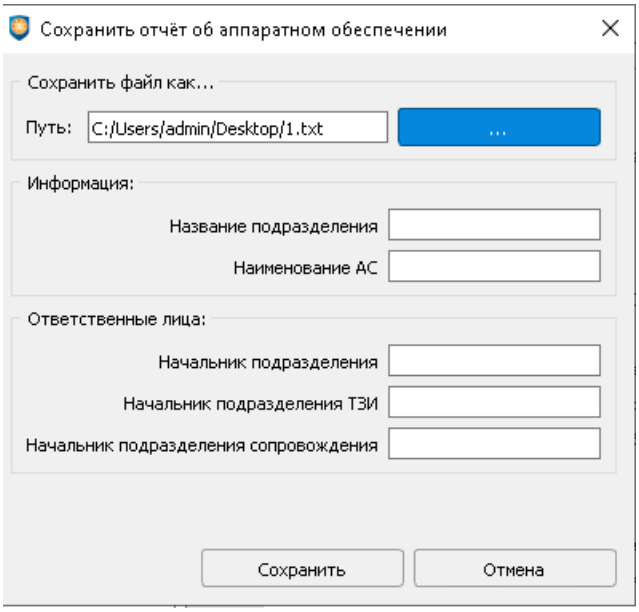

Рис. 210. Команда «Сохранить в файл»

14.4.7 Журналы Агента ЕЦУ

Вкладка «Журналы» для Агента ЕЦУ позволяет просматривать журналы безопасности модуля. Для модуля Агент ЕЦУ Windows (рис. 211) доступны:

- «Журнал безопасности»;
- «Системный журнал»;
- «Журнал приложений»;
- «Журнал установок».

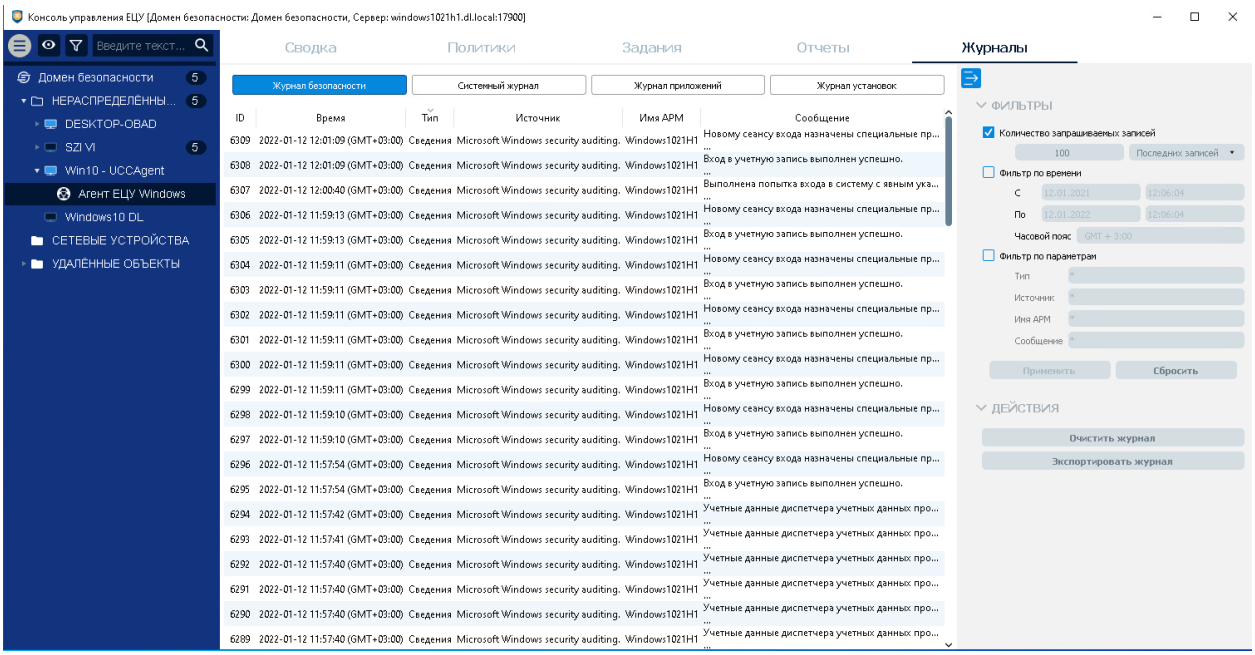

Рис. 211. Журналы Агента ЕЦУ Windows

Для модуля Агент ЕЦУ Linux (рис. 212) доступны:

- «Системный журнал»;
- «Журнал управления пользователями»;
- «Журнал печати»;
- «Журнал входов».

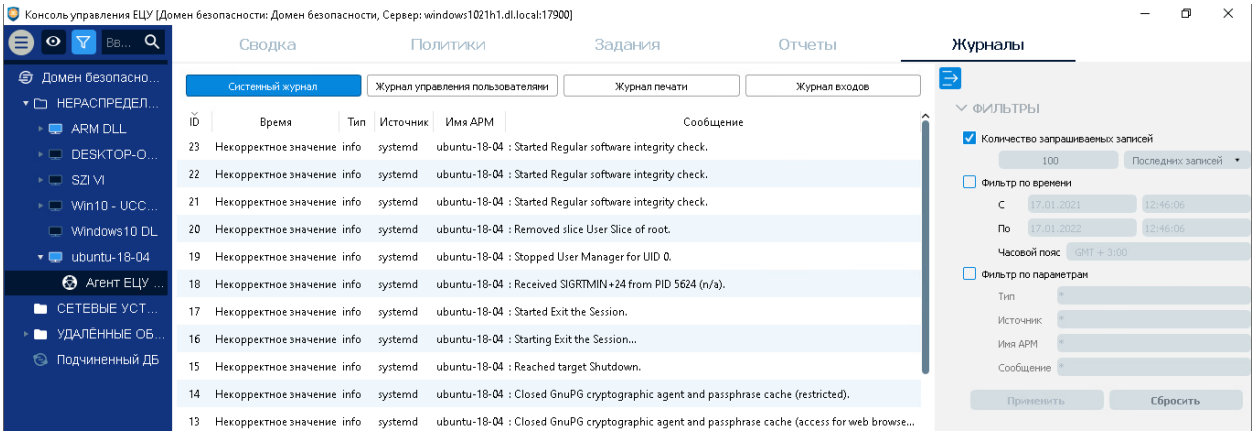

Рис. 212. Журналы Агента ЕЦУ Linux

Работа с журналами модулей описана в разделе «Журналы модуля».
Для получения записей журналов с модуля требуется выполнение сбора журналов.

15 KASPERSKY SECURITY CENTER

15.1 Подключение к Kaspersky Security Center

Для подключения к KSC необходимо открыть главное меню Консоли ЕЦУ и выбрать пункт → «Подключение к Kaspersky Security Center».

В окне «Подключение к Kaspersky Security Center» (рис. 213) указать:

- сервер KSC (формат ввода *<адрес>*:*<порт>*. В качестве адреса можно указать DNS-имя, NetBIOS-имя, либо IP-адрес);
- имя администратора KSC;
- пароль.

Нажать кнопку «Далее» для подтверждения подключения к KSC. Для отмены подключения нажать «Отмена».

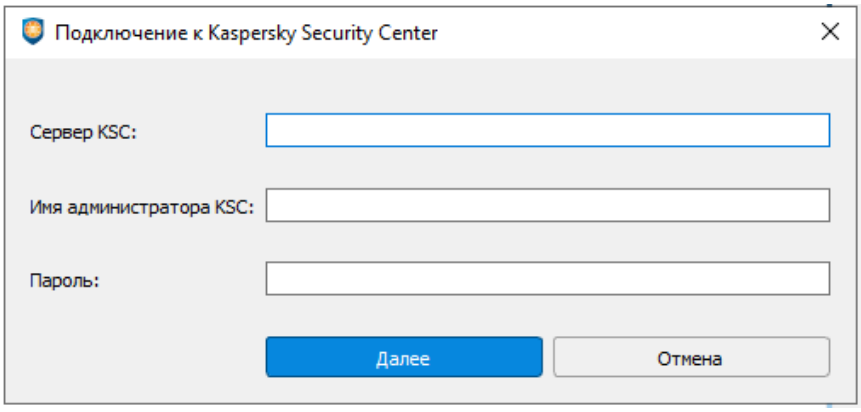

Рис. 213. Подключение к Kaspersky Security Center

Если подключение прошло успешно — в следующем окне (рис. 214) отобразится базовая информация о сервере KSC.

Установка флага «Автоматический ввод в ДБ новых клиентов KES» — позволяет зарегистрировать всех клиентов KES, входящих в состав подключаемого сервера KSC, в Домене ЕЦУ Dallas Lock. После редактирования параметров нажать кнопку «Ввести в ДБ».

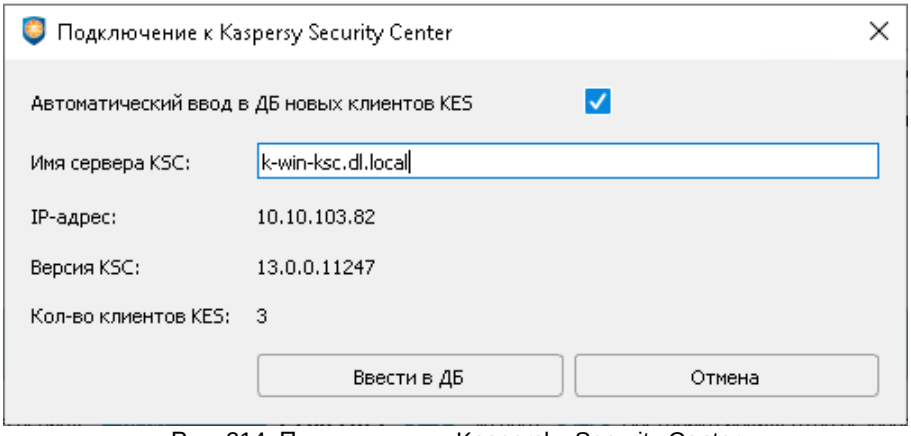

Рис. 214. Подключение к Kaspersky Security Center

В Консоли ЕЦУ в корне дерева Домена безопасности появится запись с соответствующим именем сервера KSC (рис. 215).

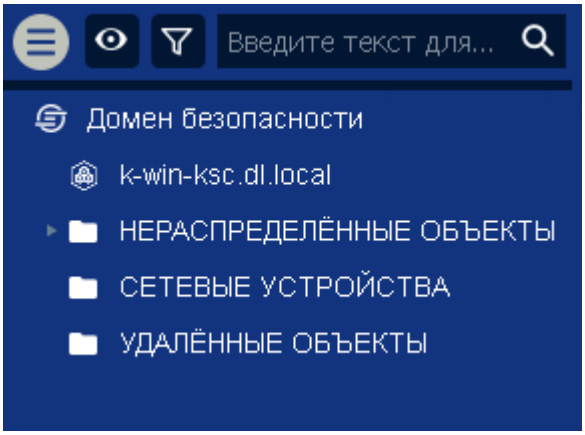

Рис. 215. KSC в дереве Домена безопасности

Клиенты KES в дереве Домена безопасности отображаются как отдельные модули в составе АРМ (рис. 216). Для регистрации в ДБ ЕЦУ незарегистрированных клиентов KES или удаления зарегистрированных модулей KES, необходимо установить/снять флаг в столбце «Состояние» (см. «Клиенты Kaspersky Security Center»). Все изменения отображаются в дереве Домена безопасности.

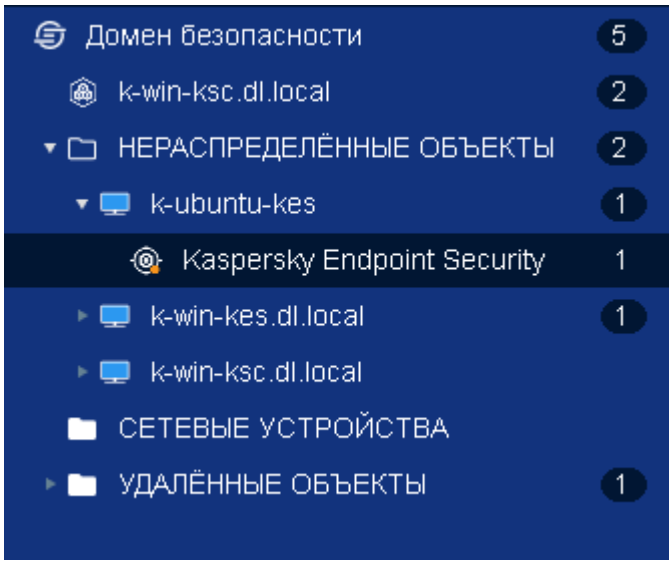

Рис. 216. KES в дереве Домена безопасности

Примечание. Для регистрации в ДБ ЕЦУ клиентов KES, входящих в состав подключаемого сервера KSC, необходимо наличие установленного на регистрируемых АРМ ПО «Агент администрирования KSC».

15.2 Отключение Kaspersky Security Center

Вывести сервер KSC и входящие в него модули KES из Домена безопасности ЕЦУ Dallas Lock можно следующими способами:

- на вкладке «Сводка» выбрать действие «Удалить»;
- открыть контекстное меню в дереве объектов для данного узла, выбрать «Удалить».

При выборе действия «Удалить» появится окно с предупреждением (рис. 217). Если подтвердить удаление — сервер KSC и модули KES будут перемещены в базовую группу Домена безопасности «Удаленные объекты».

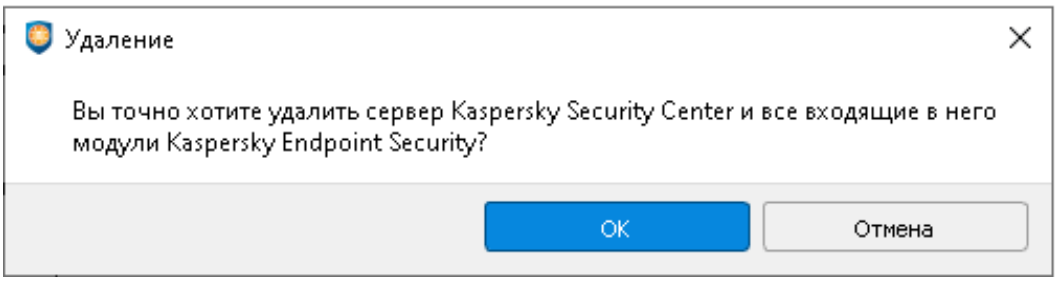

Рис. 217. Отключение Kaspersky Security Center

15.3 Настройка Kaspersky Security Center

В корне дерева Домена безопасности ЕЦУ Dallas Lock отображается подключение к серверу KSC. Значки подключенного сервера KSC, зависят от состояния и могут принимать следующий вид:

— сервер подключен;

— сервер не подключен.

15.3.1 Синхронизация

Для отправки на ЕЦУ Dallas Lock сведений о сервере KSC и приведения в соответствие системного времени необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между ЕЦУ Dallas Lock и сервером KSC:

- периодически (см. «Параметры Kaspersky»);
- по команде пользователя из Консоли ЕЦУ.

Команда «Синхронизировать» в Консоли ЕЦУ для сервера KSC доступна на вкладке «Сводка» на панели инструментов «Оперативное управление» (рис. 218).

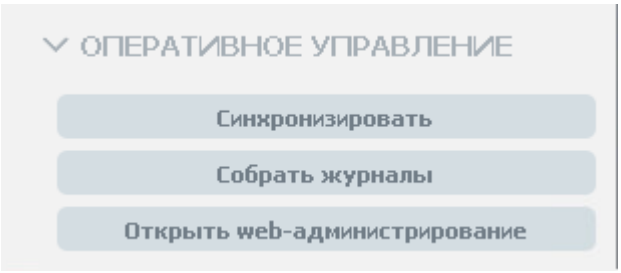

Рис. 218. Оперативное управление

15.3.2 Сбор журналов

Для получения в ЕЦУ Dallas Lock записей журналов, ведущихся на сервере KSC, необходимо проведение сбора журналов. Сбор журналов может быть проведен при условии наличия сетевого подключения между ЕЦУ Dallas Lock и сервера KSC:

- периодически (см. «Параметры Kaspersky»);
- по команде пользователя из Консоли ЕЦУ.

Команда «Собрать журналы» в Консоли ЕЦУ для KSC доступна на вкладке «Сводка» на панели инструментов «Оперативное управление» (рис. 218).

15.3.3 Открыть web-администрирование

Для перехода в веб-интерфейс Kaspersky Security Center, необходимо выбрать команду «Открыть web-администрирование» на панели инструментов «Оперативное управление» (рис. 218).

При нажатии на кнопку «Открыть web-администрирование», в браузере откроется окно ввода, где необходимо заполнить следующие поля:

- имя пользователя;
- пароль;
- имя Сервера администрирования, к которому нужно подключиться.

Затем нажать кнопку «Войти».

15.3.4 Сводка Kaspersky Security Center

Вкладка «Сводка» (рис. 219) отображает общее состояние сервера KSC.

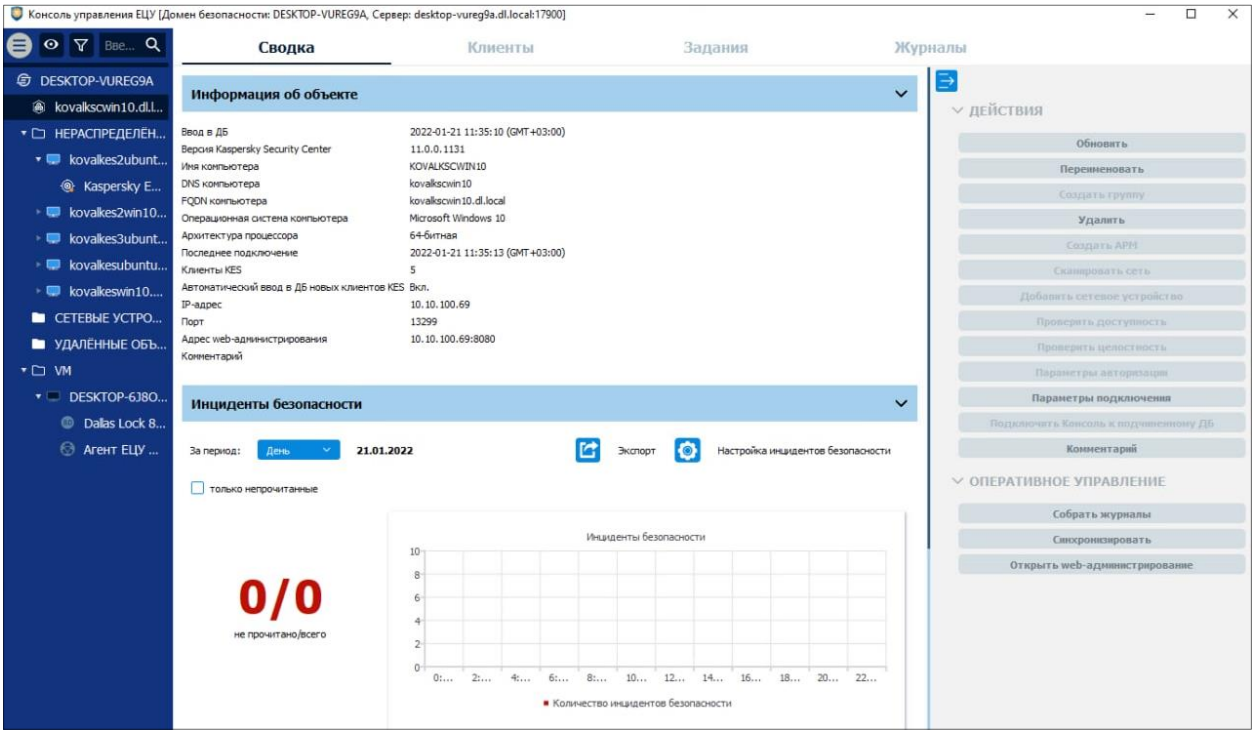

Рис. 219. Вкладка «Сводка» Kaspersky Security Center

Доступны следующие разделы информационной панели.

Информация об объекте
В верхней части информационной панели отображается следующая информация о текущем состоянии модуля: • информация о дате и времени ввода в ДБ; • версия Kaspersky Security Center; • имя компьютера KSC; • DNS компьютера KSC; • FQDN компьютера KSC; • ОС компьютера KSC; • архитектура процессора; • информация о дате и времени последнего подключения; • информация о количестве клиентов KES; • статус параметра «Автоматический ввод в ДБ новых клиентов KES»; • IP-адрес; • порт; • адрес web-администрирования; • комментарий.
Инциденты безопасности
Отображается список инцидентов безопасности с графической панелью. Доступна фильтрация отображаемых событий по периоду и настройка отображения диаграмм (см. «Настройка инцидентов безопасности»).

Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное. Поле комментарий доступно для редактирования.

На панели инструментов вкладки «Сводка» (рис. 219) доступны следующие действия:

- «Обновить» (обновить информацию на вкладке «Сводка»);
- «Переименовать» (переименовать имя сервера);
- «Удалить» (вывести сервер KSC и все входящие в него модули KES из ДБ ЕЦУ Dallas Lock);
- «Параметры подключения» (рис. 220) (редактировать адрес сервера, логин и пароль администратора, включать/отключать чекбоксом автоматический ввод в ДБ новых клиентов KES, которые появились в составе сервера KSC);
- «Комментарий» (добавленный комментарий отобразится в разделе «Информация об объекте» вкладки «Сводка»).

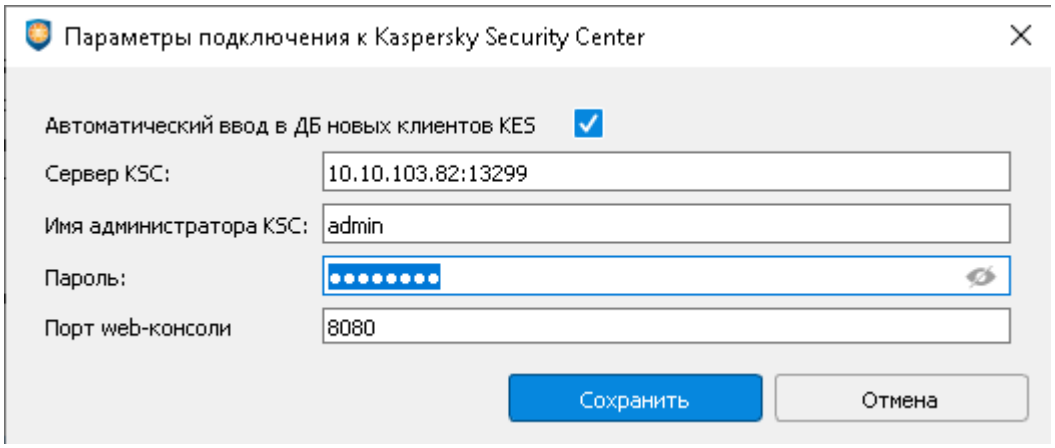

Рис. 220. Параметры подключения

Для сервера KSC доступны следующие команды оперативного управления (рис. 218) на панели инструментов:

- «Синхронизировать»;
- «Собрать журналы»;
- «Открыть web-администрирование».

Примечание. Результат выполнения команд оперативного управления не отражается в Журналах ЕЦУ. Также не предусмотрены всплывающие и прочие уведомления о результатах выполнения команд оперативного управления.

15.3.5 Клиенты Kaspersky Security Center

Вкладка «Клиенты» содержит список клиентов KES, полученных от сервера KSC (рис. 221). Поле «Состояние» отражает состояние регистрации клиентов KES в ДБ:

☑ — отмеченное флагом поле означает, что данная учетная запись пользователя имеет доступ на уровне группы ДБ, при этом «Состояние» задано (переопределено) на данном уровне дерева;

☐ — пустое поле означает, что клиент KES не зарегистрирован в ДБ.

Для регистрации в ДБ ЕЦУ Dallas Lock незарегистрированных клиентов KES или удаления зарегистрированных модулей KES, необходимо установить/снять флаг в столбце «Состояние», соответственно. При регистрации и удалении модулей KES изменения отображаются в дереве Домена безопасности.

Рис. 221. Клиенты Kaspersky Security Center

15.3.6 Журналы Kaspersky Security Center

На вкладке «Журналы» для KSC доступен «Журнал Kaspersky» (рис. 222). В журнале отображаются все события, которые приходят с определенного сервера KSC на ЕЦУ Dallas Lock. Справа на панели инструментов можно задать параметры фильтрации. В разделе «Действия» можно сохранить отфильтрованные записи журнала с помощью команды «Экспортировать журнал». Для очистки выбранного журнала модуля используется команда «Очистить журнал».

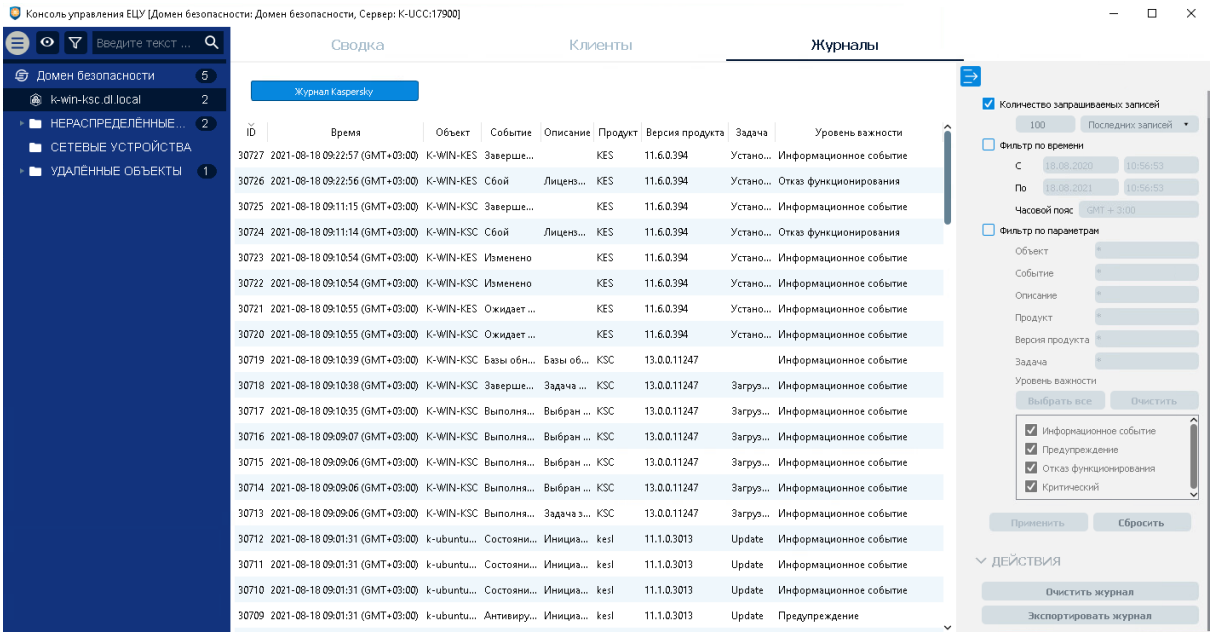

Рис. 222. Журналы Kaspersky Security Center

15.4 Настройка модуля Kaspersky Endpoint Security

KES отображаются как отдельные модули в составе АРМ, и могут принимать следующий вид:

— модуль подключен, защита включена;

— модуль подключен, защита выключена;

— модуль не подключен.

15.4.1 Сводка модуля Kaspersky Endpoint Security

Вкладка «Сводка» отображает общее состояние модуля KES (рис. 223).

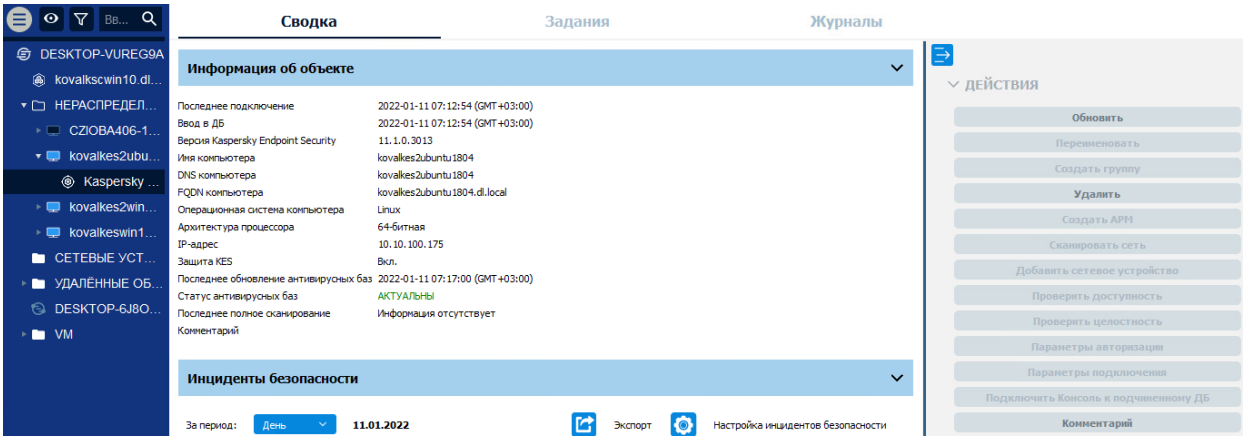

Рис. 223. Сводка модуля Kaspersky Endpoint Security

Доступны следующие разделы информационной панели.

Информация об объекте

В верхней части информационной панели отображается следующая информация о текущем состоянии модуля:

- информация о дате и времени последнего подключения модуля;
- информация о дате и времени ввода модуля в ДБ;
- версия Kaspersky Security Center;
- имя компьютера KSC;
- DNS компьютера KSC;
- FQDN компьютера KSC;
- ОС компьютера;
- Архитектура процессора;
- IP-адрес;
- статус защиты KES;
- информация о дате и времени последнего обновления антивирусных баз;
- статус антивирусных баз;
- информация о дате и времени последнего полного сканирования;
- комментарий к модулю.

Инциденты безопасности

Отображается список инцидентов безопасности модуля с графической панелью. Доступна фильтрация отображаемых событий по периоду и настройка отображения диаграмм (см. «Настройка инцидентов безопасности»).

Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное. Поле «Комментарий» доступно для редактирования.

Доступны следующие действия с модулем на панели инструментов:

4. Обновить.
5. Удалить.
6. Комментарий.

15.4.2 Задания модуля Kaspersky Endpoint Security

На уровне модуля Kaspersky Endpoint Security в списке на вкладе «Задания» доступны для создания только задания, актуальные для KES (рис. 224):

- обновление антивирусных баз;
- сканирование клиентских АРМ.

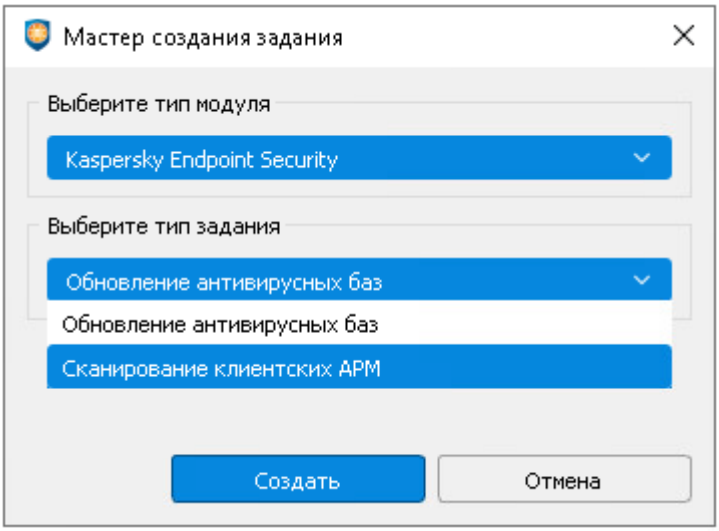

Рис. 224. Мастер создания задания

Работа с заданиями для модуля KES производится аналогично настройке заданий для ДБ (см. «Задания ДБ»).

15.4.3 Журналы модуля Kaspersky Endpoint Security

На вкладке «Журналы» для KES доступен «Журнал Kaspersky» (рис. 225). В журнале отображаются только те события, которые приходят с выбранного модуля KES.

На панели инструментов можно задать параметры фильтрации. В разделе Действия можно сохранить отфильтрованные записи журнала с помощью команды «Экспортировать журнал». Для очистки выбранного журнала модуля используется команда «Очистить журнал».

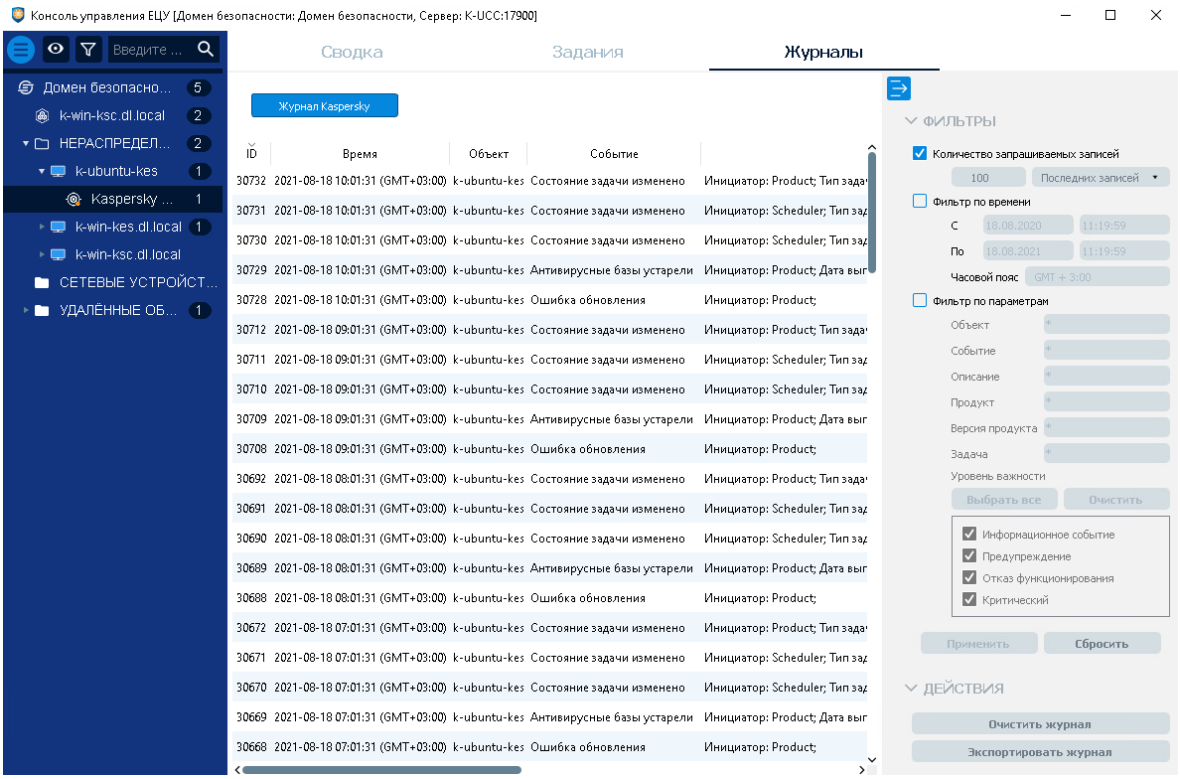

Рис. 225. Журналы модуля Kaspersky Endpoint Security

16 СЕТЕВОЕ ОБОРУДОВАНИЕ

16.1 Регистрация сетевого устройства в ДБ

Зарегистрировать сетевое устройство в Домене безопасности можно следующими способами:

- путем добавления по IP-адресу;
- путем сканирования сети.

Оба способа позволяют зарегистрировать сетевое устройство в домене безопасности ЕЦУ Dallas Lock по следующим протоколам: SNMP и SSH.

Примечание. Для корректного взаимодействия ЕЦУ Dallas Lock с сетевыми устройствами требуется дополнительно открыть следующие порты:

- SNMP: порт 161/UDP, исходящее подключение;
- SSH: порт 22/TCP, исходящее подключение;
- Syslog:
  - порт 514/ UDP, входящее подключение;
  - порт 1468/TCP, входящее подключение (при необходимости).

Примечание. В рамках контроля СУ по протоколу SSH обеспечена поддержка СУ Cisco IOS, Cisco ASA, D-Link DGS и ZyXel ZyNOS.

16.1.1 Добавление сетевого устройства по IP

Для регистрации сетевого устройства в Домене безопасности ЕЦУ Dallas Lock по IP-адресу необходимо выполнить следующие шаги:

1. Убедиться, что сетевое устройство поддерживает один из протоколов (SNMP/SSH), и доступно по сети для всех серверов кластера ДБ.
2. Запустить Консоль ЕЦУ и авторизоваться.
3. На уровне Домена безопасности или группы (подгруппы) на вкладке «Сводка» на панели инструментов «Действия» выбрать команду «Добавить сетевое устройство» (рис. 226).

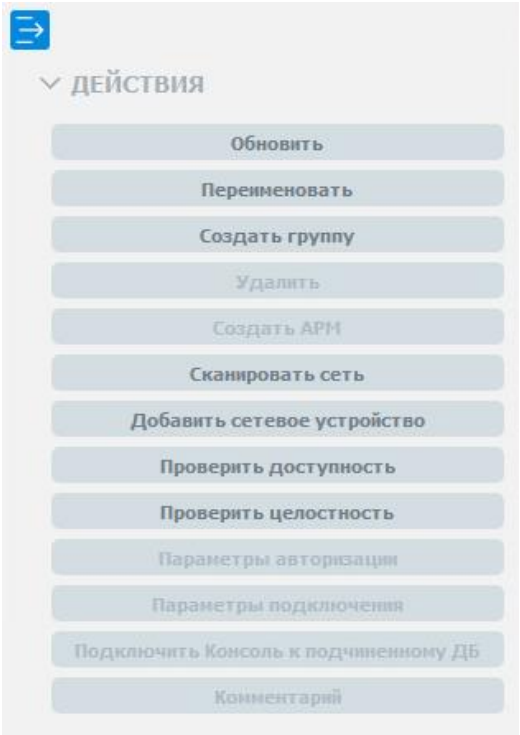

Рис. 226. Добавить сетевое устройство

4. Появится окно «Добавление сетевого устройства» (рис. 227) в котором необходимо указать IPv4-адрес и выбрать тип протокола сетевого устройства. Для выбора типа протокола, необходимо установить флаг напротив нужного (SNMP или SSH). По умолчанию включен флаг «Использовать SNMP».
   Далее необходимо заполнить параметры подключения выбранного протокола:

   SNMP
   - версия протокола SNMP
   - порт
   - таймаут (мс)
   - сообщество (пароль)

   SSH
   - порт
   - таймаут подключения (мс)
   - таймаут ответа (мс)
   - имя пользователя
   - пароль
   - привилегированный пароль

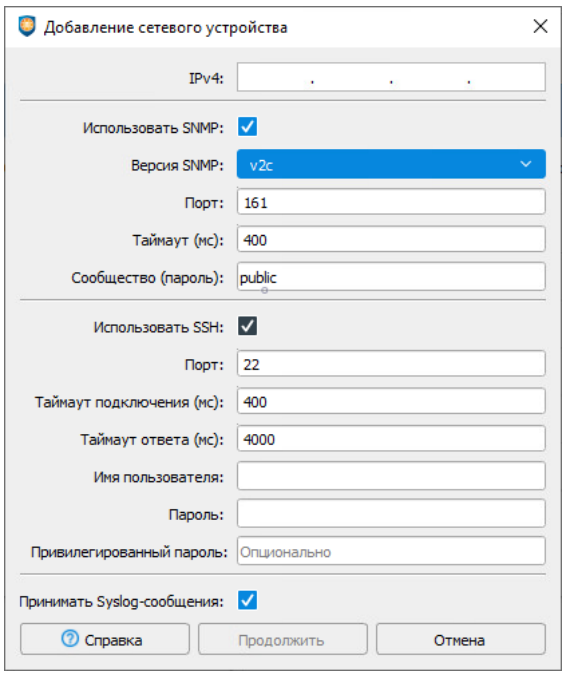

Рис. 227. Окно параметров подключения

5. После заполнения всех полей нажать кнопку «Продолжить». При регистрации устройства по протоколу SNMP появится окно «Предупреждение» (рис. 228). Для продолжения процесса регистрации необходимо нажать кнопку «Ок», при нажатии кнопки «Отмена» будет произведен возврат на шаг назад, где можно будет внести изменения в параметры подключения.

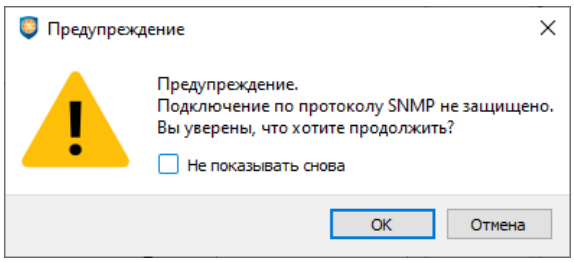

Рис. 228. Предупреждение о подключении по протоколу SNMP

Примечание. При установке флага «Не показывать снова», следующие предупреждения будут скрыты. Восстановить предупреждения можно нажав на кнопку «Восстановить предупреждения» в главном меню консоли ЕЦУ → «Параметры…» → «Общие» (см. «Параметры работы»).

Если процесс регистрации сетевого устройства в ДБ прошел успешно, то через некоторое время в дереве Домена на уровне, на котором была вызвана команда «Добавить сетевое устройство», появится иконка зарегистрированного сетевого устройства (рис. 229).

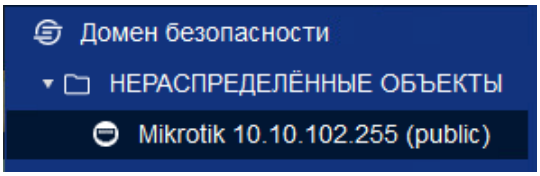

Рис. 229. Иконка зарегистрированного сетевого устройства в дереве ДБ

16.1.2 Сканирование диапазона сетевых адресов

Для регистрации сетевого устройства в Домене безопасности ЕЦУ Dallas Lock путем сканирования диапазона сетевых адресов необходимо выполнить следующие шаги:

1. Убедиться, что сетевое устройство поддерживает один из протоколов (SNMP/SSH), и доступно по сети для всех серверов кластера ДБ.
2. Запустить Консоль ЕЦУ и авторизоваться.
3. На уровне Домена безопасности или группы (подгруппы) на вкладке «Сводка» на панели инструментов «Действия» выбрать команду «Сканировать сеть» (рис. 230).

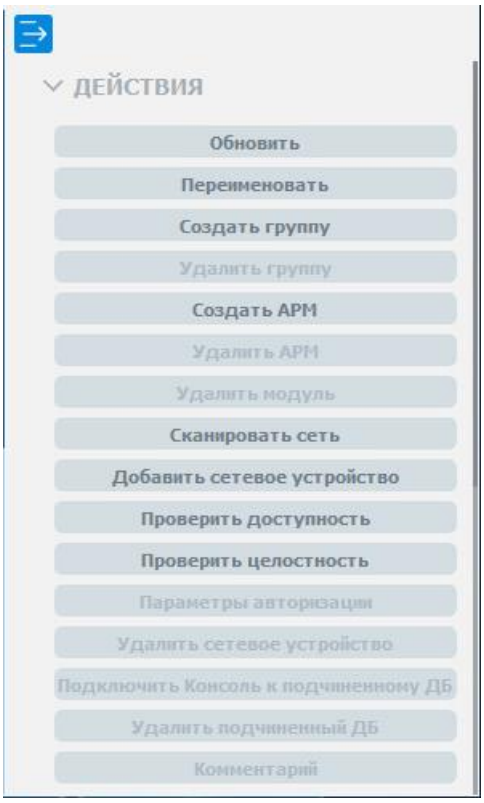

Рис. 230. Сканировать сеть

4. Появится окно «Сканирование сети», в котором нужно перейти на вкладку «Сетевое устройство» и указать диапазон IPv4-адресов для сканирования (рис. 231). Затем выбрать один из протоколов (SNMP/SSH) и заполнить требуемые для него поля:

SNMP
- версия протокола SNMP
- порт
- таймаут (мс)
- сообщество (пароль)

SSH
- порт
- таймаут подключения (мс)
- таймаут ответа (мс)
- имя пользователя
- пароль

- привилегированный пароль

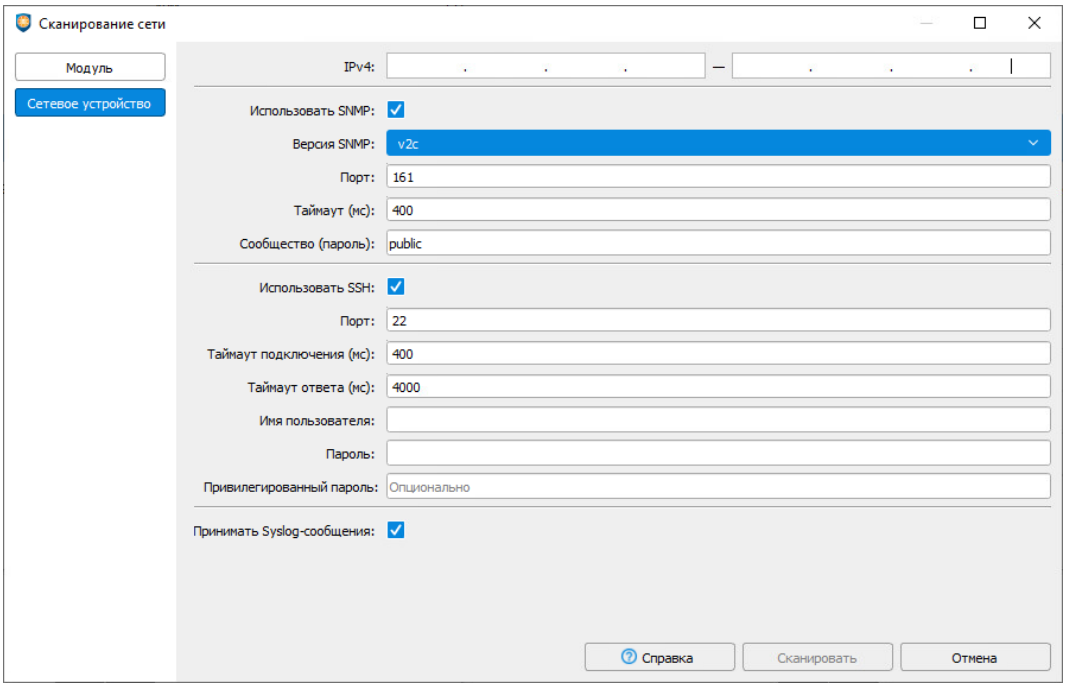

Рис. 231. Окно сканирование сети

В этом же окне с помощью постановки флага можно настроить прием Syslog-сообщений.

5. После заполнения всех полей нажать кнопку «Сканировать» и далее можно просматривать состояние процесса сканирования для каждого диапазона сетевых адресов.

Примечание. При сканировании сети по протоколу SNMP появится окно «Предупреждение» (рис. 228). Для продолжения процесса сканирования необходимо нажать кнопку «Ок», при нажатии кнопки «Отмена» будет произведен возврат на шаг назад, где можно внести изменения в параметры сканирования.

6. По завершении процесса сканирования из списка обнаруженных объектов можно выбрать те объекты, которые необходимо зарегистрировать в ДБ (рис. 232).

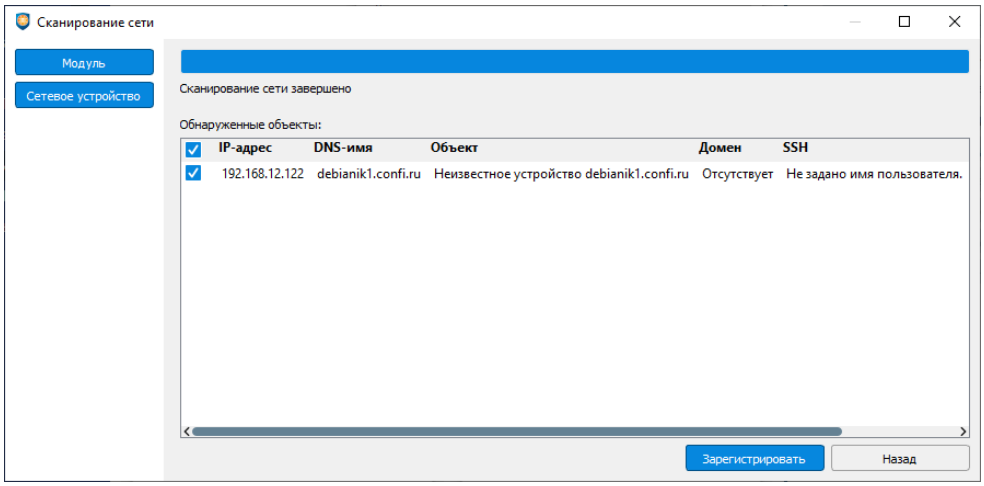

Рис. 232. Выбор объектов для регистрации в ДБ

7. После выбора всех регистрируемых устройств нужно нажать в окне кнопку «Зарегистрировать».

Если процесс регистрации сетевых устройств в ДБ прошел успешно, то выбранные сетевые устройства зарегистрируются в дереве Домена безопасности в базовой группе «Сетевые устройства» (рис. 233).

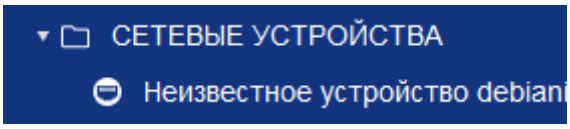

Рис. 233. Иконка зарегистрированного сетевого устройства в дереве ДБ

16.2 Удаление сетевого устройства из ДБ

Для удаления сетевого устройства из Домена безопасности ЕЦУ Dallas Lock необходимо:

1. Выбрать пункт «Удалить» из контекстного меню, нажав правой кнопкой мыши на нужное устройство в дереве ДБ (рис. 234), или воспользоваться командой «Удалить» на панели инструментов «Действия» вкладки «Сводка» на уровне устройства в дереве ДБ (рис. 235).

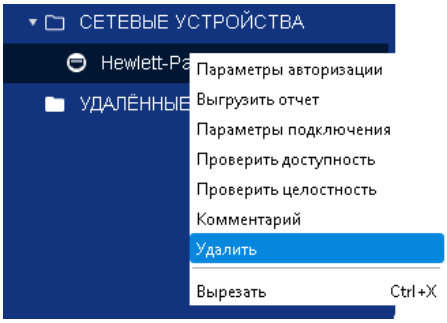

Рис. 234. Удаление устройства посредством контекстного меню

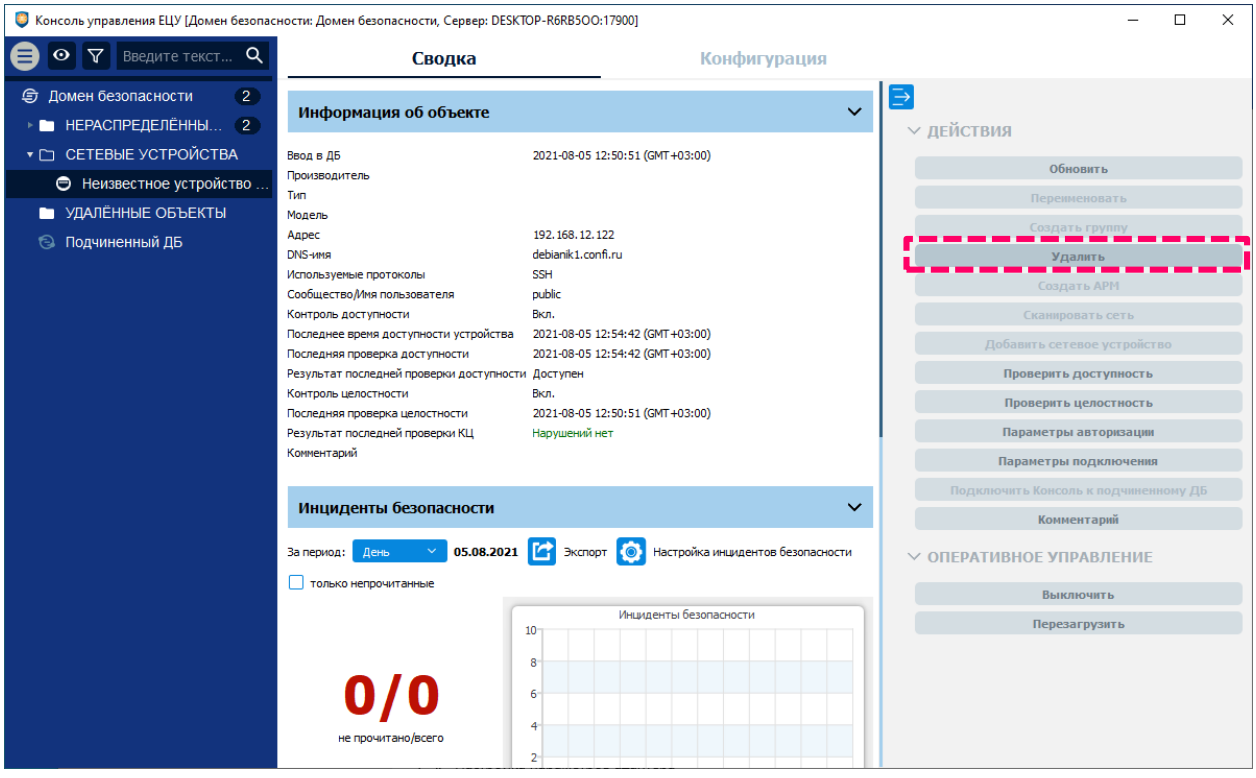

Рис. 235. Удаление посредством панели «Действия»

2. Удаленное сетевое устройство переместится в базовую группу «Удаленные объекты» дерева ДБ.

16.3 Настройка сетевого устройства

В дереве Домена безопасности ЕЦУ Dallas Lock присутствуют зарегистрированные сетевые устройства.
Значки объектов, обозначающих сетевые устройства, зависят от состояния сетевого устройства и могут принимать следующий вид:

— сетевое устройство доступно;

— сетевое устройство недоступно;

— на сетевом устройстве зафиксировано нарушение целостности конфигурации, при этом сетевое устройство доступно;

— на сетевом устройстве зафиксировано нарушение целостности конфигурации, при этом сетевое устройство недоступно;

— связь с сетевым устройством отсутствует свыше заданного на ЕЦУ Dallas Lock времени, которое определяется параметром «Оповещения при отсутствии связи с объектом (в днях)» (при условии, что настроено оповещение об отсутствии связи с объектом).

Настройки на уровне сетевого устройства отображаются на нескольких основных вкладках.

16.3.1 Сводка сетевого устройства

Вкладка «Сводка» на уровне сетевого устройства отображает общее состояние сетевого устройства (Рис. 236).

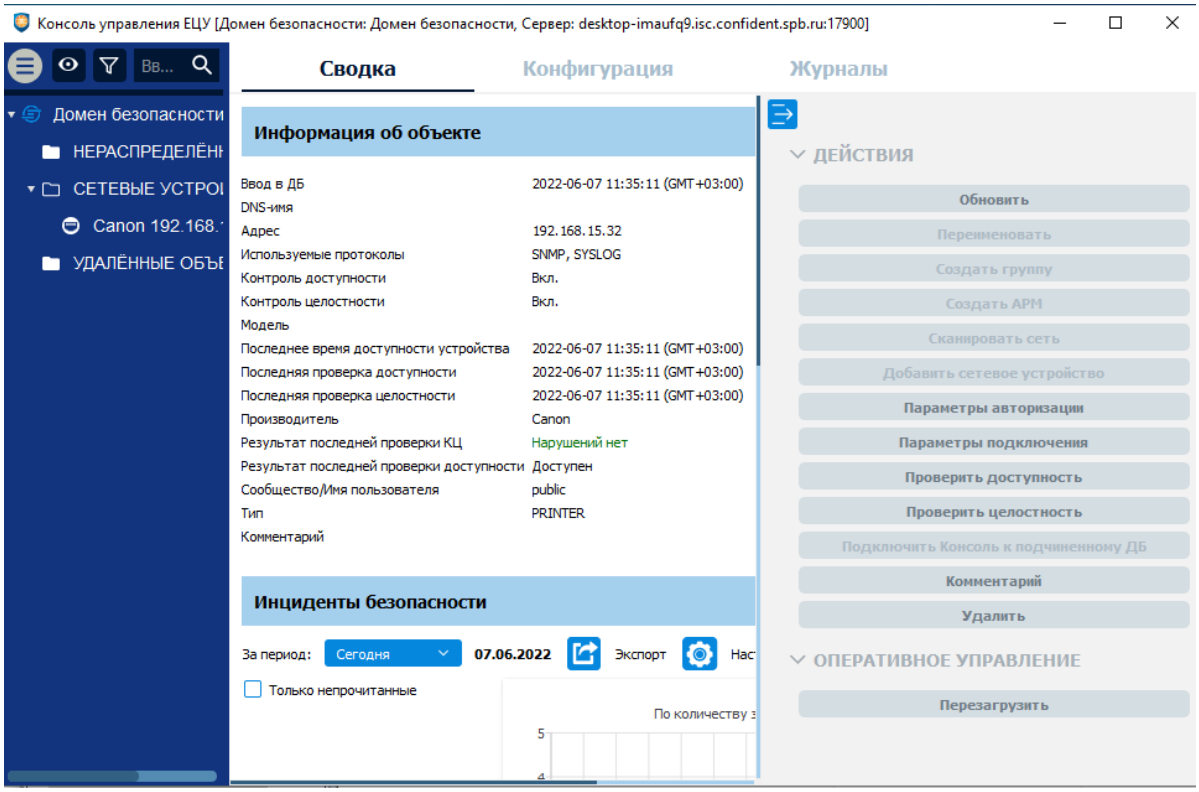

Рис. 236. Сводка сетевого устройства

Доступны следующие разделы информационной панели.

Информация об объекте
В верхней части информационной панели отображается следующая информация о текущем состоянии сетевого устройства: • дата и время регистрации сетевого устройства в ДБ; • DNS-имя устройства; • сетевой адрес устройства; • используемые протоколы; • состояние контроля доступности; • состояние контроля целостности; • информация о производителе, типе и модели сетевого устройства; • дата и время последней доступности устройства; • дата и время последней проверки доступности; • дата и время последней проверки целостности; • информация о результатах проверки целостности; • информация о результатах проверки доступности устройства; • сообщество/имя пользователя, под которым зарегистрировано устройство; • комментарий к устройству.
Инциденты безопасности
Отображается список инцидентов безопасности сетевого устройства с графической панелью. Доступна фильтрация отображаемых событий по периоду и настройка отображения диаграмм (см. «Настройка инцидентов безопасности»). Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное. Поле «Комментарий» доступно для редактирования.

Доступны следующие действия с сетевым устройством на панели инструментов:

1. Обновить.
2. Параметры авторизации.
3. Параметры подключения.
4. Проверить доступность.
5. Проверить целостность.
6. Комментарий.
7. Удалить.

На панели инструментов доступна команда оперативного управления «Перезагрузить».

Примечание. Не все сетевые устройства поддерживают управление питанием по SNMP, но даже такие устройства будут добавлены в группу сетевых устройств ДБ. Для корректной возможности перезагрузки сетевого устройства по SNMP требуется настроить параметры авторизации. В поле «Управление питанием» должно быть прописано *public (*Рис. 237*)*.

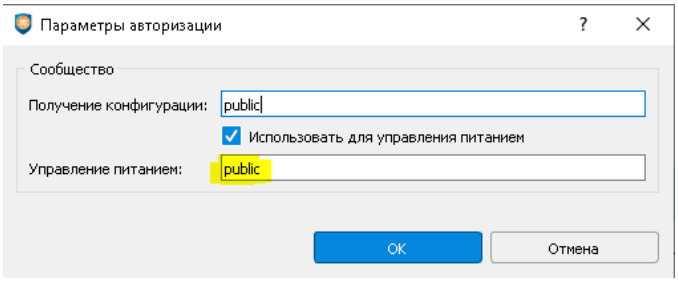

Рис. 237. Настройки параметров авторизации

Примечание. Результат выполнения команд оперативного управления не отражается в Журналах ЕЦУ. Также не предусмотрены всплывающие и прочие уведомления о результатах выполнения команд оперативного управления.

16.3.2 Конфигурация сетевого устройства

Вкладка «Конфигурация» на уровне сетевого устройства отображает параметры сетевого устройства (рис. 238).

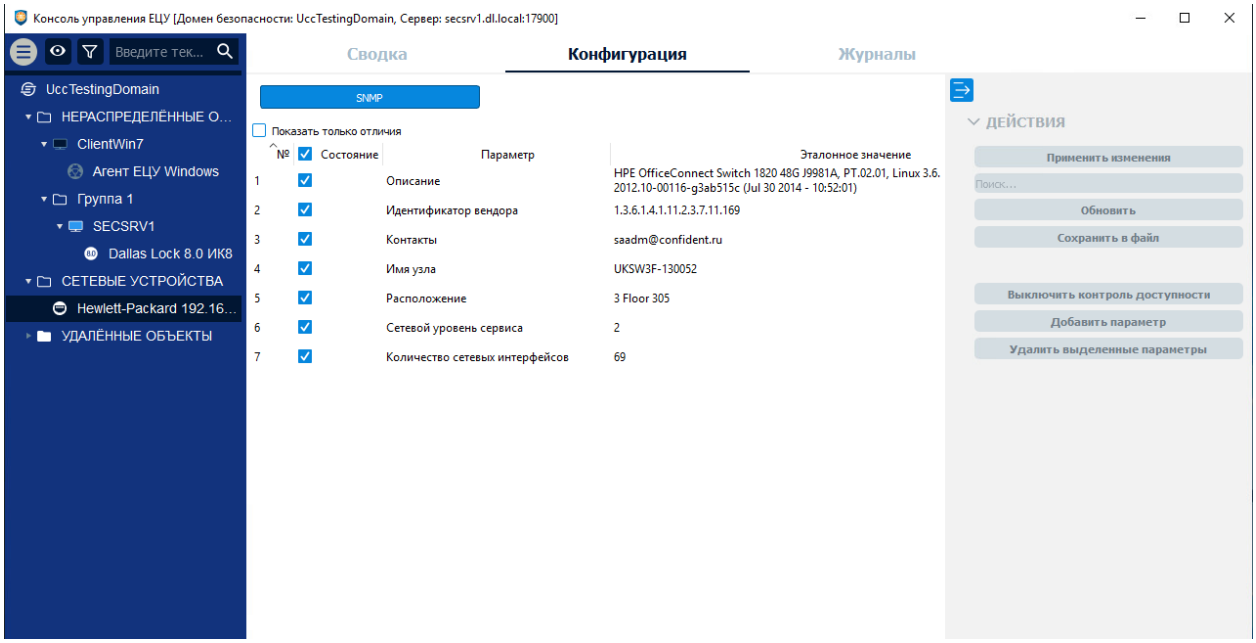

Рис. 238. Конфигурация сетевого устройства

В таблице на вкладке «Конфигурация» содержатся параметры и их значения, полученные от сетевого устройства по протоколу SNMP или SSH.
Список параметров сетевого устройства представляется собой таблицу с полями:

SNMP
- номер
- состояние
- параметр
- эталонное значение
- последнее значение

SSH
- номер
- состояние
- имя
- команда
- эталонное значение
- последнее значение

Над таблицей есть поле «Показать только отличия», установка флага напротив этого поля приводит к переходу в режим отображения параметров конфигурации, целостность которых нарушена. Снятие флага возвращает к просмотру всех параметров.

Примечание. MIB — база управляющей информации. OID — это уникальный идентификатор объекта в SNMP (объектом может быть модель устройства или конкретный параметр). OID записывается как последовательность чисел, разделенных точкой. Например, «1.3.6.3.2.1». MIB-файлы позволяют использовать текстовое представление OID. Например, для OIDa «1.3.6.1.2.1.31.1.1.1.10» текстовое представление — «ifHCOutOctets».

При регистрации сетевого устройства в Домене безопасности в Базе конфигураций ЕЦУ Dallas Lock осуществляется поиск конфигурации для данного устройства. Если в базе не обнаружена конфигурация для производителя, используется конфигурация по умолчанию (о том как пополнить Базу конфигураций ЕЦУ Dallas Lock см. «Параметры сетевого оборудования»).

Найденная в базе конфигурация представляет собой список OID. Устройство опрашивается по списку OID из конфигурации, далее полученные при первом опросе значения используются в качестве эталонных.
Если в ответ на запрос значения параметра у сетевого устройства ЕЦУ Dallas Lock получает пустое значение, в таблице напротив названия такого параметра будет содержаться символ «Ø». Если

устройство не ответило на запрос значения параметра — в таблице будет содержатся запись «(нет ответа)».
Если в процессе функционирования устройства значение параметра становится отличным от эталонного, в ДБ фиксируется инцидент безопасности «Нарушение целостности конфигурации сетевого оборудования» (рис. 239).

Примечание. События нарушения целостности сетевого оборудования могут возникать, если ЕЦУ Dallas Lock при работе не успевает получить значения параметров OID с устройств. Для решения данной проблемы сетевое устройство необходимо вывести из-под контроля ЕЦУ Dallas Lock и зарегистрировать заново, увеличив при добавлении время тайм-аута.

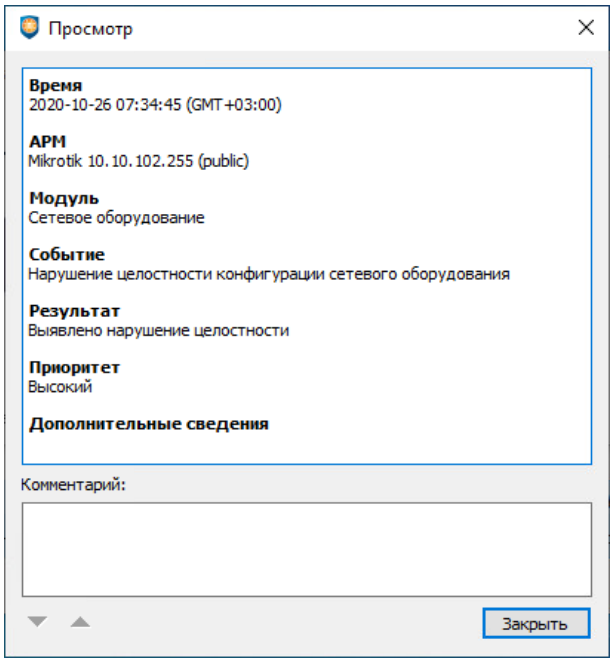

Рис. 239. Просмотр сведений об инциденте безопасности

На вкладке «Конфигурация» соответствующий параметр, отличный от эталонного, будет выделен цветом:

- эталонное значение соответствующего параметра – красным;
- последнее значение соответствующего параметра – зеленым.

Рис. 240. Отображение значений параметров сетевого оборудования на вкладке «Конфигурация»

На вкладке «Конфигурация» на панели инструментов «Действия» доступны следующие команды (Рис. 240):

1. «Применить изменения», предназначена для принятия последних полученных значений конфигурации за эталонные.
2. «Поиск…», позволяет искать параметры конфигурации.
3. «Обновить», предназначена для получения актуальных значений конфигурации от устройства.

4. «Сохранить в файл», предназначена для сохранения отчета о текущей конфигурации сетевого устройства в формате «.txt».
5. «Включить/Выключить контроль доступности», предназначена для изменения состояния контроля доступности сетевого устройства.
6. «Добавить параметр», для нового контролируемого параметра позволяет установить флаг «Контролировать параметр», а также задать имя и OID.
7. «Удалить выделенные параметры».

Для отображения только отличий между эталонным значением и последним значением доступен фильтр «Показать только отличия».

За эталонное значение будет принято значение, полученное от сетевого устройства при следующей проверке.

16.3.3 Журналы сетевого устройства

На вкладке «Журналы» для сетевого устройства доступен «Журнал Syslog». В журнале отображаются только Syslog-сообщения, полученные от сетевого устройства.
На панели инструментов можно задать параметры фильтрации. На панели инструментов в разделе «Действия» можно сохранить отфильтрованные записи журнала с помощью команды «Экспортировать журнал».
Для очистки журнала используется команда «Очистить журнал».

17 ПОДЧИНЕННЫЙ ДОМЕН БЕЗОПАСНОСТИ

Внимание! При вводе одного домена безопасности в подчинение другому должно быть соблюдено следующее условие: между доменами безопасности должен быть свободный обмен пакетами по TCP/IP порту 17900.

Внимание! В ЕЦУ Dallas Lock должно выполняться правило создания связей между главным и подчиненным доменом, которое заключается в запрете организации «циклов администрирования доменов», когда главный домен является подчиненным доменом для одного и того же домена.

Примечание. Подчиненный домен безопасности может иметь только один главный ДБ на один уровень выше по иерархии ЕЦУ Dallas Lock (существует возможность создавать несколько уровней подчинения). Ограничения по количеству подчиненных у главного домена безопасности устанавливаются лицензией.

17.1 Ввод ДБ в подчинение

17.1.1 Ввод ДБ в подчинение в процессе установки

Для ввода в подчинение Домена безопасности в процессе установки ЕЦУ Dallas Lock необходимо:

1. Убедиться, что Домен безопасности, в подчинение которому осуществляется ввод, доступен по сети.
2. Запустить процесс установки ЕЦУ Dallas Lock.
3. На шаге «Выбор типа домена» выбрать пункт «Подчиненный домен безопасности» (рис. 241).

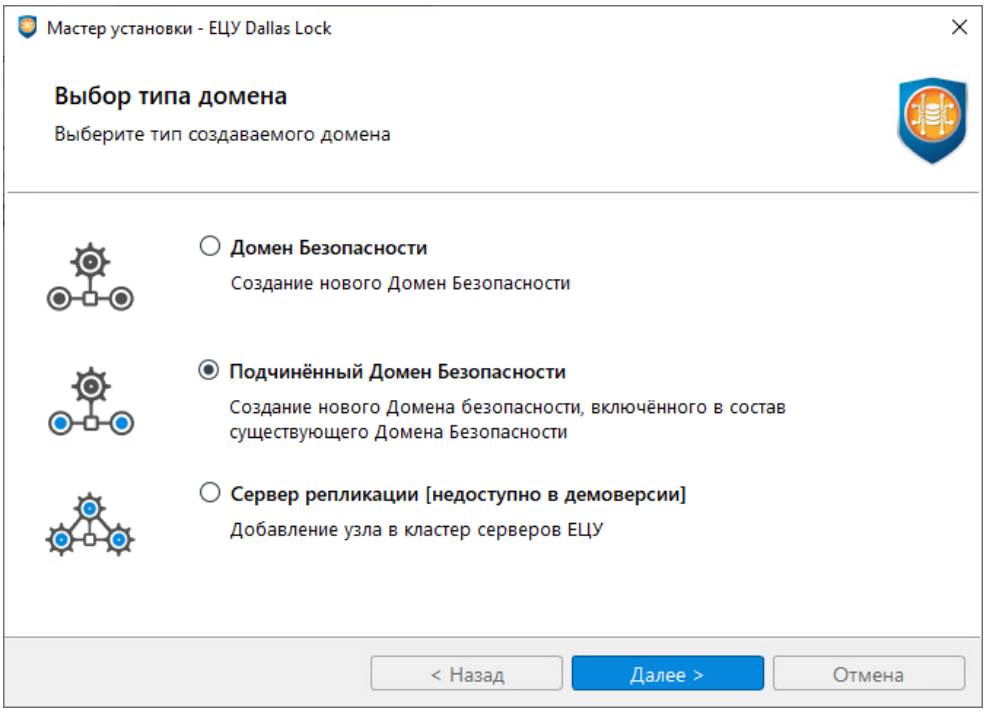

Рис. 241. Шаг «Выбор типа домена» в мастере установки ЕЦУ Dallas Lock

4. Задать параметры главного ДБ (рис. 242):
   - адрес главного ДБ;
   - ключ доступа к ДБ.

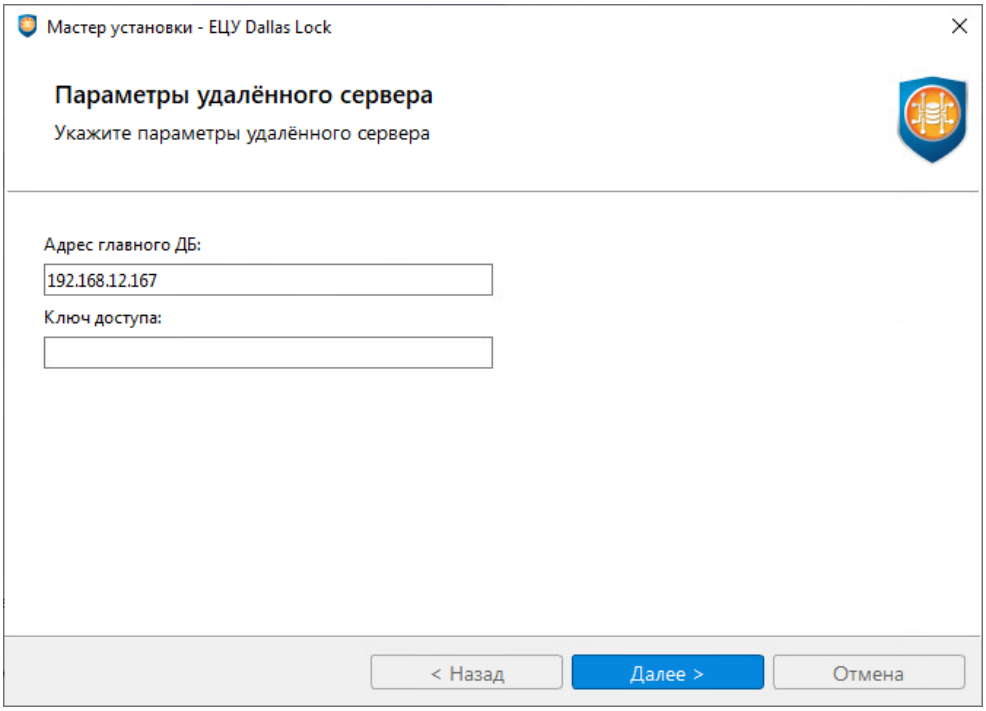

Рис. 242. Параметры удаленного сервера

5. Далее продолжить и завершить установку ЕЦУ Dallas Lock.
6. После завершения установки подчиненного ДБ в дереве главного ДБ появится введенный в подчинение ДБ (рис. 243).

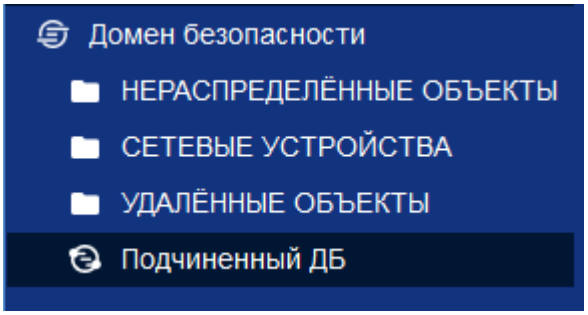

Рис. 243. Подчиненный ДБ в дереве родительского

17.1.2 Ввод ДБ в подчинение после установки

Для ввода в подчинение Домена безопасности после установки необходимо:

1. Убедиться, что Домен безопасности, в подчинение которому осуществляется ввод, доступен по сети.
2. Запустить Консоль ЕЦУ к ДБ, вводимого в подчинение.
3. Открыть главное меню Консоли ЕЦУ → «Ввод/вывод в подчинение».
4. В появившемся окне указать сетевое имя сервера из главного домена и ключ доступа к главному домену безопасности (рис. 244).

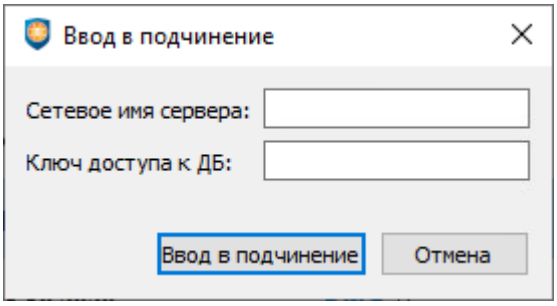

Рис. 244. Ввод в подчинение

5. Нажать кнопку «Ввод в подчинение».

Если процесс ввода в подчинение прошел успешно, то через некоторое время появится соответствующее сообщение (рис. 245).

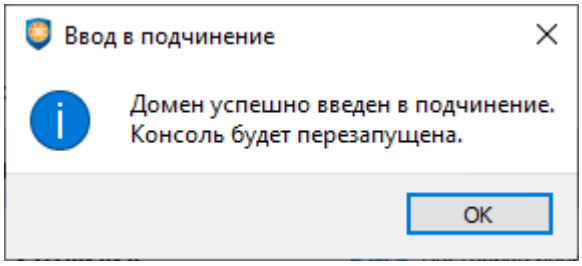

Рис. 245. ДБ успешно введен в подчинение

После перезапуска Консоли на уровне ДБ на вкладке «Сводка» → «Информация об объекте» отобразится информация о родительском домене (рис. 246).

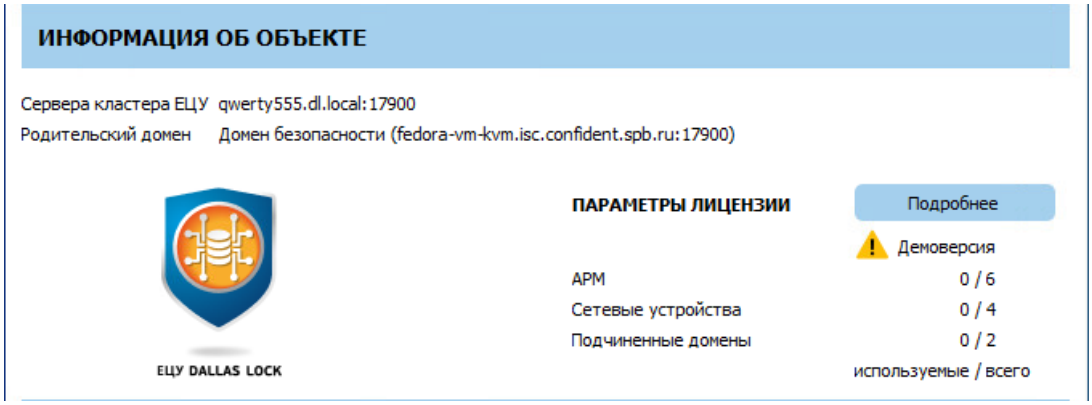

Рис. 246. Информация о родительском домене

Также в дереве главного ДБ появится введенный в подчинение ДБ (рис. 243).

17.2 Вывод ДБ из подчинения

17.2.1 Вывод ДБ из подчинения из собственной консоли

Для вывода из подчинения Домена безопасности посредством собственной консоли необходимо:

1. Подключить Консоль ЕЦУ к ДБ, находящемуся в подчинении.

2. Открыть главное меню Консоли ЕЦУ → «Ввод/вывод в подчинение».

3. В появившемся окне «Вывод из подчинения» (рис. 247) нажать кнопку «Вывод из подчинения».

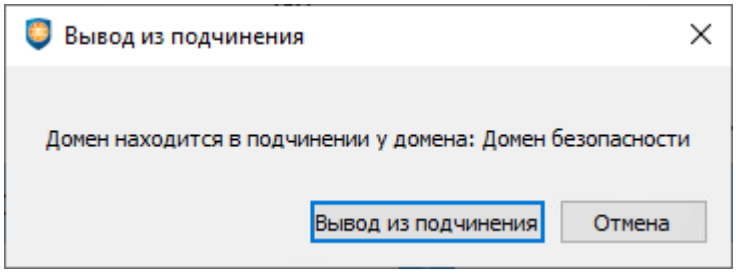

Рис. 247. Вывод из подчинения

Если процесс вывода домена из подчинения прошел успешно, то через некоторое время появится соответствующее сообщение (рис. 248).

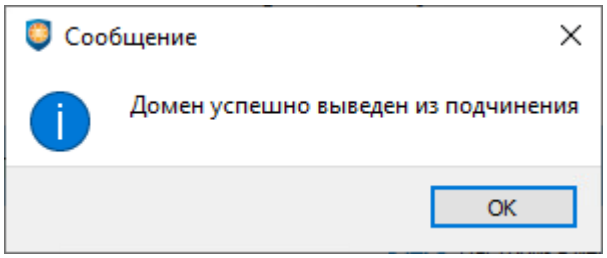

Рис. 248. ДБ успешно выведен из подчинения

17.2.2 Вывод ДБ из подчинения через консоль главного ДБ

Для вывода из подчинения ДБ через Консоль ЕЦУ главного ДБ необходимо:

1. Подключить Консоль ЕЦУ к главному ДБ.
2. Выбрать подчиненный ДБ в дереве и на вкладке «Сводка» нажать на панели инструментов «Действия» кнопку «Удалить» (рис. 250) или выбрать соответствующую команду из контекстного меню, нажав правой кнопкой мыши на подчиненный ДБ в дереве (рис. 249).

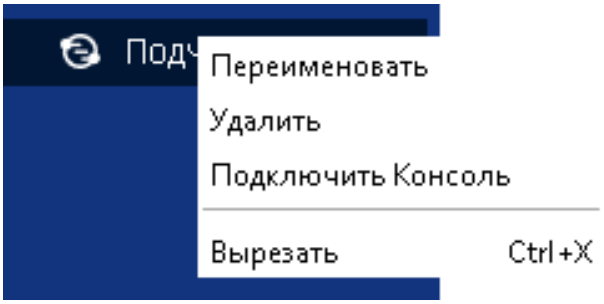

Рис. 249. Контекстное меню подчиненного ДБ

Рис. 250 Команды панели инструментов для подчиненного ДБ

Выведенный из подчинения ДБ переместится в базовую группу «Удаленные объекты».

17.3 Настройка подчиненного домена безопасности

В дереве главного Домена безопасности ЕЦУ Dallas Lock присутствуют подчиненные ДБ.

Значки объектов, обозначающих подчиненные ДБ, зависят от состояния ДБ и могут принимать следующий вид:

— подчиненный ДБ подключен;

— связь с подчиненным ДБ отсутствует;

— связь с подчиненным ДБ отсутствует свыше заданного в главном ДБ времени, которое определяется параметром «Оповещения при отсутствии связи с объектом (в днях)» (при условии, что настроено оповещение об отсутствии связи с объектом).

Администратор ЕЦУ Dallas Lock может перемещать подчиненные ДБ в группы (подгруппы) дерева ДБ. Для этого необходимо перетащить значок нужного подчиненного ДБ кнопкой мыши в поле другого значка («Drag-and-drop»).

Настройки на уровне подчиненного ДБ отображаются на нескольких основных вкладках.

17.3.1 Синхронизация

Для приведения в соответствие значениям параметров, выставленным на главном ДБ, на подчиненном ДБ необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между главным и подчиненным доменом:

- при включении подчиненного ДБ;
- периодически (см. «Параметры работы модулей»);
- по команде пользователя из Консоли ЕЦУ главного ДБ.

Команда «Синхронизировать» в Консоли ЕЦУ доступна на вкладке «Сводка» на уровне подчиненного ДБ в дереве ДБ на панели инструментов «Оперативное управление».

17.3.2 Сводка подчиненного ДБ

Вкладка «Сводка» на уровне подчиненного ДБ отображает общее состояние подчиненного ДБ (рис. 251).

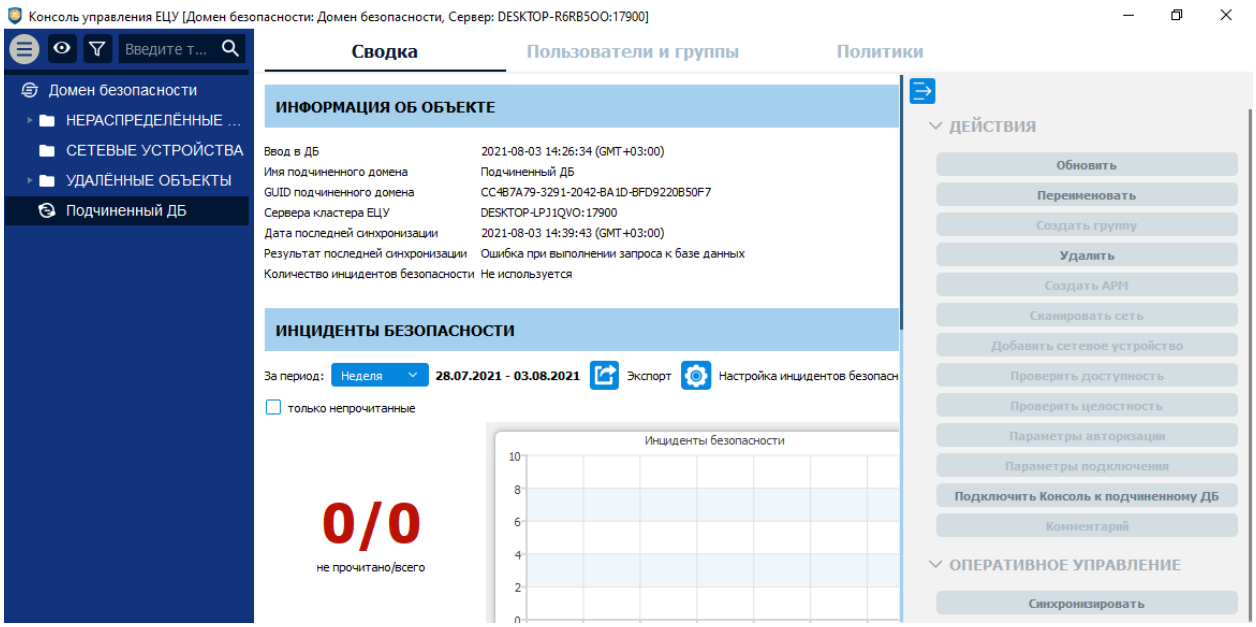

Рис. 251. Вкладка «Сводка»

Доступны следующие разделы информационной панели.

Информация об объекте
В информационной панели отображается следующая информация о текущем состоянии модуля: • информация о дате и времени ввода в ДБ; • имя подчиненного домена; • GUID подчиненного домена; • сервера кластера ЕЦУ; • информация о дате и времени последней синхронизации; • результат последней синхронизации; • количество инцидентов безопасности.

Доступны следующие действия с подчиненным ДБ на панели инструментов:

1. Обновить.
2. Переименовать.
3. Удалить подчиненный домен.
4. Подключить Консоль к подчиненному ДБ.

Доступны следующие команды оперативного управления на панели инструментов:

1. Синхронизировать.

Примечание. Результат выполнения команд оперативного управления не отражается в Журналах ЕЦУ. Также не предусмотрены всплывающие и прочие уведомления о результатах выполнения команд оперативного управления.

Открыть Консоль ЕЦУ Dallas Lock подчиненного ДБ можно с Консоли ЕЦУ Dallas Lock Главного ДБ. Для этого нужно:

1. Нажать «Подключить Консоль к подчиненному ДБ» (рис. 251) на панели инструментов «Действия» вкладки «Сводка».
   Подключить Консоль подчиненного ДБ можно также с помощью одноименной функции контекстного меню (рис. 249)
2. Появится окно «Подключение к серверу» (рис. 252). Далее необходимо заполнить следующие поля:
   - имя консоли;
   - сетевое имя сервера;
   - ключ доступа к ДБ.

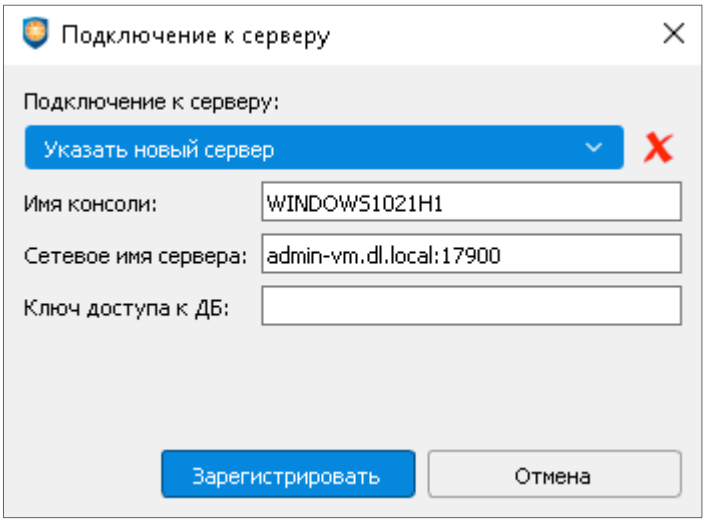

Рис. 252. Окно «Подключение к серверу»

   Затем нажать «Зарегистрировать».
3. В следующем окне (рис. 253), необходимо ввести авторизационные данные и нажать «Подключиться».

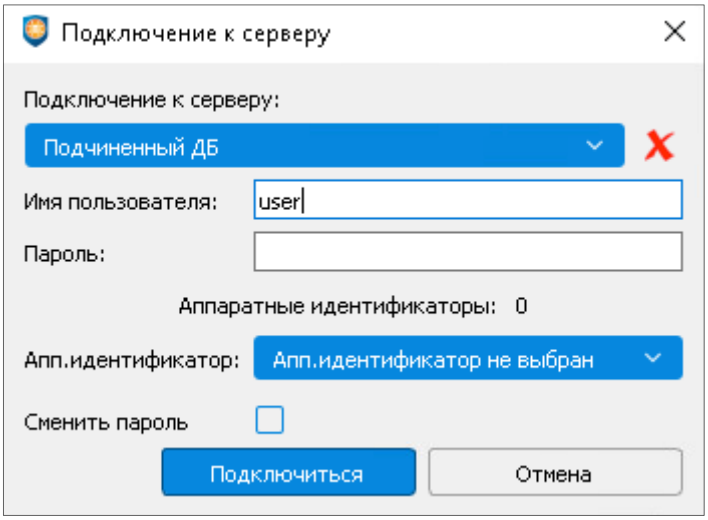

Рис. 253. Ввод авторизационных данных

Если данные введены верно, будет открыто новое окно Консоли управления ЕЦУ Подчиненного ДБ.

17.3.3 Пользователи и группы подчиненного ДБ

Вкладка «Пользователи и группы» на уровне подчиненного ДБ содержит список глобальных и доменных пользователей и групп, наследуемых с уровней выше по иерархии и созданных на уровне данного подчиненного домена.

Примечание. Пользователи и группы, созданные в подчиненном ДБ, не передаются в главный и не отображаются в списке пользователей и групп в Консоли главного ЕЦУ на уровне подчиненного ДБ в дереве.

Управление пользователями и группами на уровне подчиненного ДБ производится аналогично описанному управлению пользователями и группами на уровне группы ДБ (см. «Пользователи и группы для группы ДБ»).

Управление пользователями и группами, созданными в главном ДБ заблокировано в Консоли подчиненного ДБ.

Примечание. Если имя пользователя или группы, созданного в подчиненном ДБ, совпало с именем пользователя или группы в главном ДБ, то параметры такого пользователя или группы подлежат синхронизации со значениями, установленными в главном ДБ.

Для применения изменений на подчиненном ДБ необходима синхронизация.

17.3.4 Политики подчиненного ДБ

Вкладка «Политики» на уровне подчиненного ДБ позволяет редактировать политики на подчиненном ДБ (рис. 254).

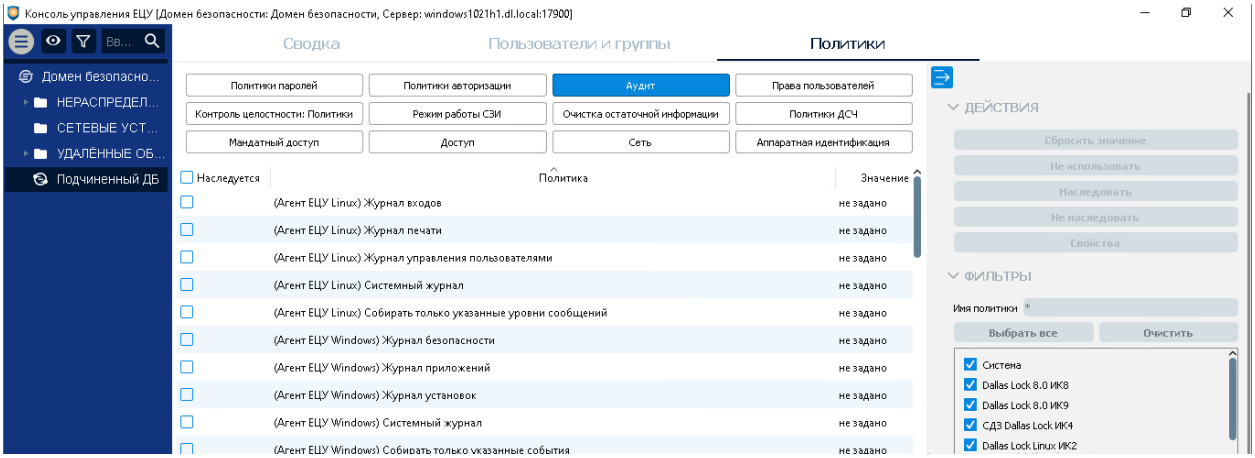

Рис. 254. Вкладка «Политики»

Примечание. Значения политик, установленные в подчиненном ДБ, не передаются в главный и не отображаются в списке политик в Консоли главного ЕЦУ на уровне подчиненного в дереве.

Политики для подчиненного ДБ могут принимать дополнительное значение «Не задано». Для данного значения главный ДБ ЕЦУ не управляет значениями политик подчиненного ДБ, применяется значение, заданное АИБ в консоли подчиненного.

По умолчанию при вводе в подчинение ДБ все его политики в главном ДБ имеют значение «Не задано».

Для сброса переопределенного значения политики на «Не задано» необходимо выбрать политику из списка и далее на панели инструментов «Действия» выбрать команду «Сбросить значение» или из контекстного меню выбрать соответствующий пункт.

Настройка политик для подчиненного ДБ производится аналогично настройке политик для группы ДБ (см. «Политики для группы ДБ»).

Для применения значений необходима синхронизация.