УТВЕРЖДЕН
RU.48957919.501410-01 И6-ЛУ

ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ

Dallas Lock

Инструкция по использованию

RU.48957919.501410-01 И6

Листов 191

СОДЕРЖАНИЕ

ВВЕДЕНИЕ **4**
ТЕРМИНЫ **4**
СОКРАЩЕНИЯ **5**
ПРЕДСТАВЛЕНИЕ МОДУЛЕЙ В ИНТЕРФЕЙСЕ ЕЦУ **6**
1 НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ ЕЦУ DALLAS LOCK **7**
1.1 Структура ЕЦУ 7
1.2 Возможности ЕЦУ 7
2 УСТАНОВКА И УДАЛЕНИЕ ЕЦУ DALLAS LOCK **10**
2.1 Требования к аппаратному и программному обеспечению 10
2.2 Установка ЕЦУ Dallas Lock 11
2.3 Удаление ЕЦУ Dallas Lock 20
2.4 Сохранение и применение конфигурации 24
2.5 О программе 26
3 ОБЩИЕ ПРИНЦИПЫ РАБОТЫ ЕЦУ DALLAS LOCK **27**
3.1 Синхронизация 27
3.2 Репликация 27
4 АДМИНИСТРИРОВАНИЕ ЕЦУ DALLAS LOCK **28**
4.1 Запуск консоли ЕЦУ 28
4.2 Описание консоли ЕЦУ 29
4.3 Ключ доступа к ДБ 31
4.4 Настройки лицензирования 32
4.5 Параметры ЕЦУ 34
5 ДОМЕН БЕЗОПАСНОСТИ ЕЦУ **47**
5.1 Сводка для ДБ 47
5.2 Пользователи и группы ДБ 50
5.3 Ролевая модель учетных записей ДБ 67
5.4 Политики ДБ 68
5.5 Задания ДБ 99
5.6 Журнал ДБ 101
6 ГРУППЫ ДОМЕНА БЕЗОПАСНОСТИ **103**
6.1 Базовые группы 103
6.2 Настройка групп 103
7 АРМ ДОМЕНА БЕЗОПАСНОСТИ ЕЦУ **109**
7.1 Настройка АРМ 109
8 МОДУЛИ ДОМЕНА БЕЗОПАСНОСТИ ЕЦУ **112**
8.1 Настройка модуля 112
9 МОДУЛЬ СЗИ DALLAS LOCK 8.0-C/K **119**
9.1 Ввод модуля в ДБ 119
9.2 Вывод модуля из ДБ 121
9.3 Централизованная установка СЗИ Dallas Lock 8.0 средствами AD 122
9.4 Настройка модуля СЗИ Dallas Lock 8.0 134
10 МОДУЛЬ СЗИ НСД DALLAS LOCK LINUX **140**
10.1 Ввод модуля в ДБ 140

10.2 Вывод модуля из ДБ 141
10.3 Централизованная установка СЗИ НСД Dallas Lock Linux 142
10.4 Настройка модуля СЗИ Dallas Lock Linux 146

11 МОДУЛЬ СЗИ ВИ DALLAS LOCK 152

11.1 Ввод модуля в ДБ 152
11.2 Вывод модуля из ДБ 153
11.3 Настройка СЗИ ВИ Dallas Lock 154

12 МОДУЛЬ СДЗ DALLAS LOCK 161

12.1 Ввод модуля в ДБ 161
12.2 Вывод модуля из ДБ 163
12.3 Настройка модуля СДЗ Dallas Lock 163

13 МОДУЛЬ WAF DALLAS LOCK 167

13.1 Ввод модуля в ДБ 167
13.2 Вывод модуля из ДБ 169
13.3 Настройка модуля WAF Dallas Lock 169

14 СЕТЕВОЕ ОБОРУДОВАНИЕ 175

14.1 Регистрация сетевого устройства в ДБ 175
14.2 Удаление сетевого устройства из ДБ 178
14.3 Настройка сетевого устройства 179

15 ПОДЧИНЕННЫЙ ДОМЕН БЕЗОПАСНОСТИ 184

15.1 Ввод ДБ в подчинение 184
15.2 Вывод ДБ из подчинения 186
15.3 Настройка подчиненного домена безопасности 188

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.

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.spb.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 и СОВ Dallas Lock); • СЗИ НСД Dallas Lock Linux; • СЗИ ВИ Dallas Lock (состоит из компонента Dallas Lock СЗИ ВИ и компонента Агент управления доступом); • СДЗ Dallas Lock; • шлюз безопасности WAF Dallas Lock. 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, расписанием, группой и т. д. Учетная запись должна быть единой для всех модулей ЕЦУ
Суперадминистратор	пользователь, под учетной записью которого выполнена установка ЕЦУ Dallas Lock
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
АИБ	администратор информационной безопасности
АРМ	автоматизированное рабочее место
АУД	агент управления доступом
ДБ	домен безопасности ЕЦУ
ДВК	датчик вскрытия корпуса
ДСЧ	датчик случайных чисел
ЕЦУ	Единый центр управления Dallas Lock

МЭ	межсетевой экран
НСД	несанкционированный доступ
ОС	операционная система
ПК	персональный компьютер
ПО	программное обеспечение
СДЗ	средство доверенной загрузки Dallas Lock
СЗИ	система защиты информации
СЗИ ВИ	система защиты информации в виртуальных инфраструктурах
СОВ	система обнаружения вторжений
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 итераций, указанных в таблице.

Продукт	Наименование модуля	
	Основное обозначение	Поддерживается с итерации
СЗИ Dallas Lock 8.0 редакции «К» и «С» (включая компоненты МЭ и СОВ)	Dallas Lock 8.0	ИК8
СЗИ НСД Dallas Lock Linux	Dallas Lock Linux	ИК2
СЗИ ВИ Dallas Lock	Dallas Lock СЗИ ВИ Агент управления доступом	ИК3
СДЗ Dallas Lock	СДЗ Dallas Lock	ИК4
шлюз безопасности WAF Dallas Lock	по умолчанию соответствует системному имени хоста, может быть задано АИБ вручную	ИК0 (не указывается в наименовании модуля)

Примечание. Так как продукт СЗИ ВИ Dallas Lock представлен в ЕЦУ в качестве двух отдельных модулей, то далее по тексту введены следующие обозначения:

- модуль СЗИ ВИ Dallas Lock — для продукта СЗИ ВИ Dallas Lock;
- модуль Dallas Lock СЗИ ВИ — для компонента СЗИ ВИ Dallas Lock;
- модуль Агент управления доступом — для компонента СЗИ ВИ Dallas Lock.

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», компоненты МЭ и СОВ Dallas Lock, СЗИ НСД Dallas Lock Linux, СЗИ ВИ Dallas Lock, СДЗ Dallas Lock, шлюз безопасности WAF Dallas Lock).

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-клиентов;
- ввод/вывод сетевого оборудования в/из ДБ;
- включение/выключение сетевого оборудования;
- применение файлов конфигурации;
- 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:
  - сохранение конфигурации;
  - применение конфигурации;
  - изменение параметров лицензии и технической поддержки;
  - проверку целостности контролируемых объектов;
- сбор журналов модуля;
- отправка сигнализации об инцидентах безопасности;
- настройка неактивного режима работы модуля;
- управление мандатными метками (только для Dallas Lock 8.0 редакции «С»);
- настройка аппаратных идентификаторов.

При работе с модулями **СЗИ 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:

- завершение работы и перезагрузка модуля;
- 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;
  - сохранение конфигурации;
  - применение конфигурации;
  - получение отчет 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;
  - сохранение конфигурации;
  - применение конфигурации;
  - получение отчета об аппаратном обеспечении;
  - получение отчет о конфигурации;
- сбор журналов модуля;
- отправка сигнализации об инцидентах безопасности;
- взаимодействие с агентом ШОС;
- настройка аппаратных идентификаторов.

При работе с 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;
  - сохранение конфигурации;
  - применение конфигурации;
  - получение логов;
  - получение отчета об аппаратном обеспечении;

  - получение отчет о конфигурации;
  - сброс к заводским настройкам;
- сбор журналов модуля;
- отправка сигнализации об инцидентах безопасности.

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:

- Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
- Windows 8 (Core, Pro, Enterprise);
- 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;

и семейства GNU Linux[2]:

- Debian 9 (systemd, версия ядра 4.9)[3];
- CentOS 7 (версия ядра 3.18);
- Red Hat Enterprise Linux Server 7 (версия ядра 3.18);
- Fedora 29;
- Ubuntu 18.04 LTS (версия ядра 4.4);
- Astra Linux Common Edition (Орел) 2.12 (версия ядра 4.4);
- Astra Linux Special Edition (Смоленск) 1.6 (версия ядра 4.4);
- ALT Linux 8.2 (версия ядра 4.9);
- Альт Сервер 9.

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

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

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

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

- электронные ключи Touch Memory;
- HID Proximity-карты;
- USB-ключи Aladdin eToken Pro/Java;
- смарт-карты Aladdin eToken Pro/SC;
- USB-ключи Рутокен (Rutoken) и Рутокен ЭЦП;
- USB-ключи и смарт-карты JaCarta;
- USB-ключи и смарт-карты ESMART.

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

---

[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.

[3] Для инсталляции ЕЦУ на ОС Debian 9 необходим подключенный репозиторий *deb http://deb.debian.org/debian stretch main contrib*.

2.2 Установка ЕЦУ Dallas Lock

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.

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».*

1. Для установки ЕЦУ Dallas Lock необходимо 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.

2. После запуска приложения на экране будет выведено окно для подтверждения операции.

После подтверждения запустится мастер установки ЕЦУ Dallas Lock (рис. 1).

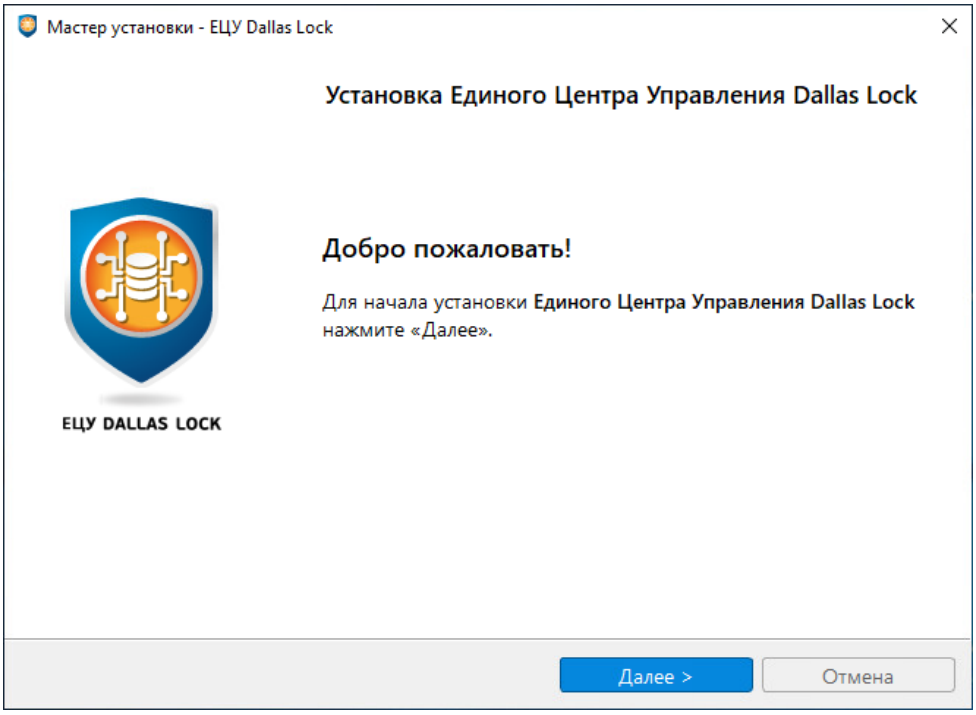

Рис. 1. Окно начала установки ЕЦУ Dallas Lock

Для продолжения установки нажать кнопку «Далее».

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

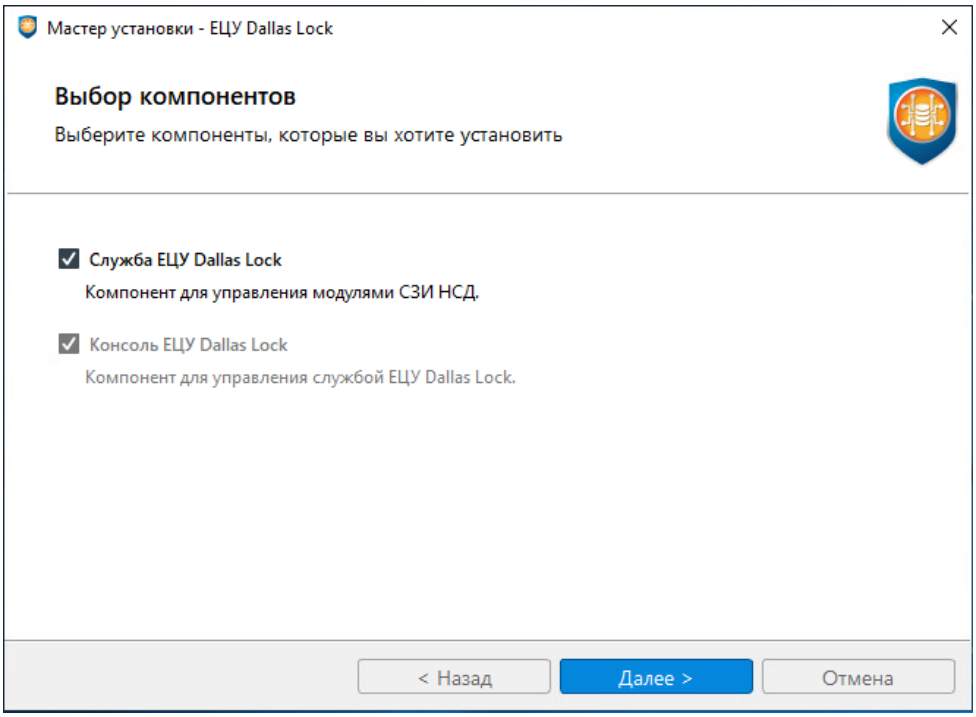

Рис. 2. Выбор компонентов для установки ЕЦУ Dallas Lock

Примечание. Служба ЕЦУ использует подключение TCP/IP по порту 17900. Установка нескольких экземпляров службы 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).

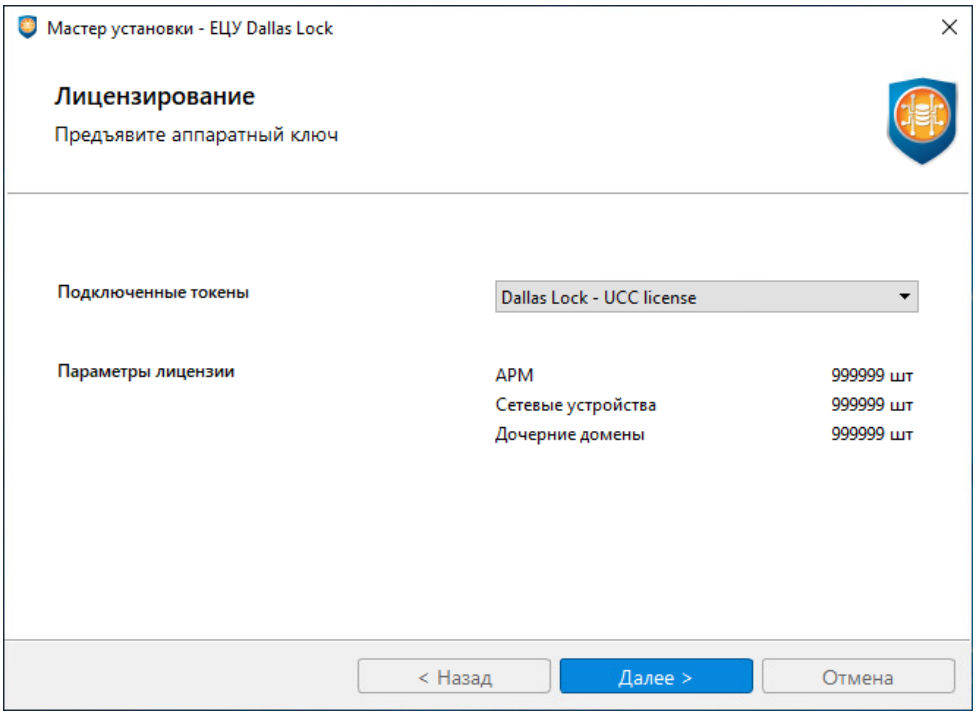

Рис. 3. Предъявление аппаратного ключа

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.

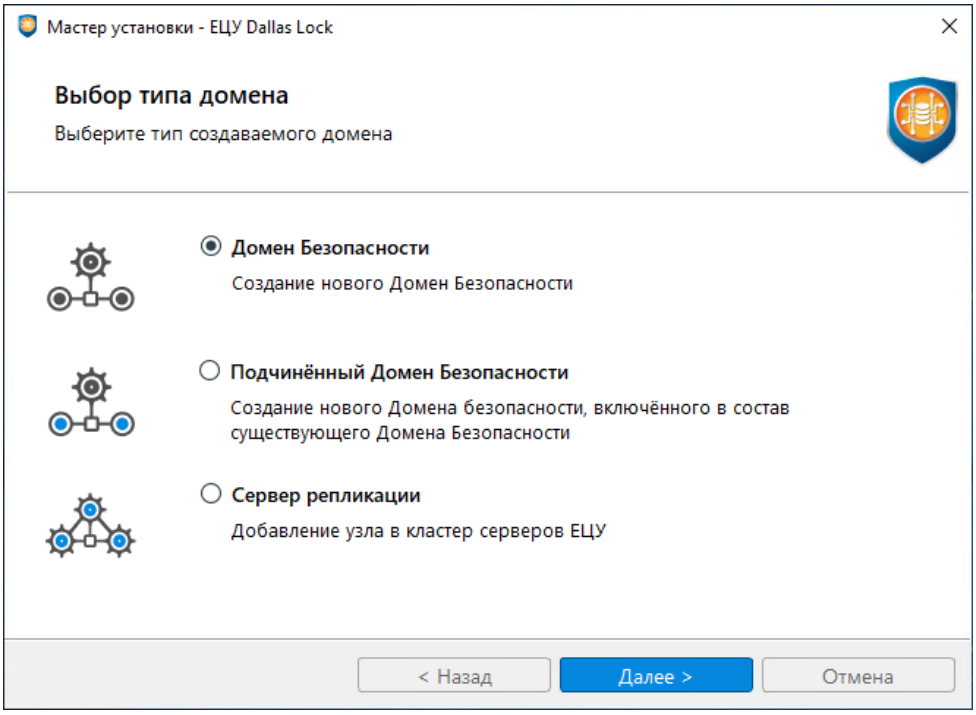

Рис. 4. Выбор типа создаваемого домена

6. Задать параметры ДБ (рис. 5):
   - в поле «Название ДБ» указать имя ДБ;
   - в поля «Ключ доступа» и «Подтвердите ключ доступа» ввести ключ доступа;

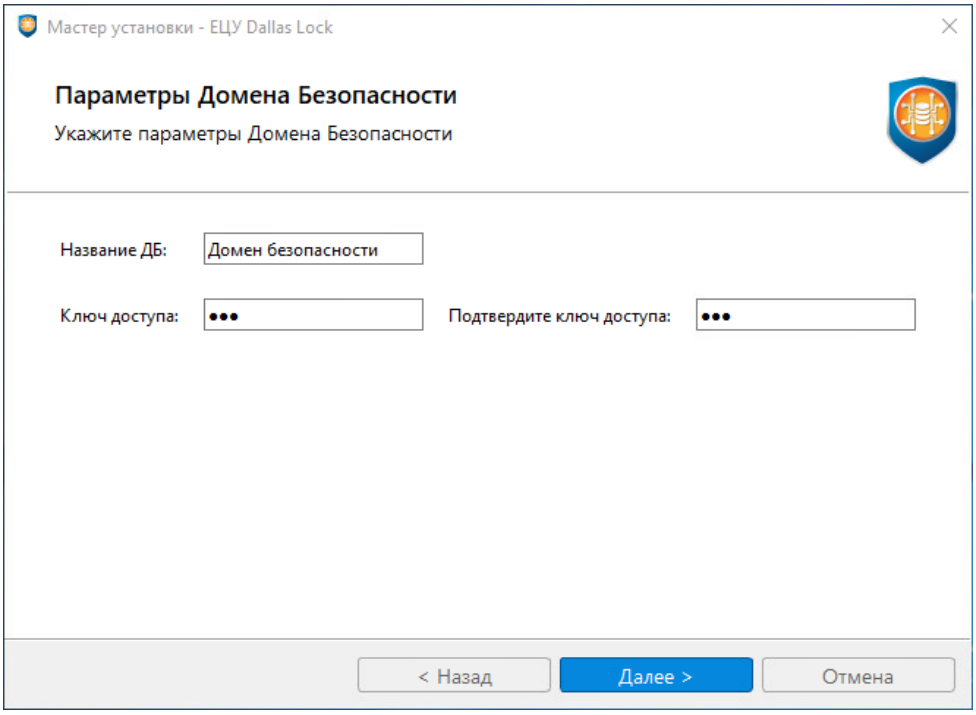

Рис. 5. Настройка параметров ДБ

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

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

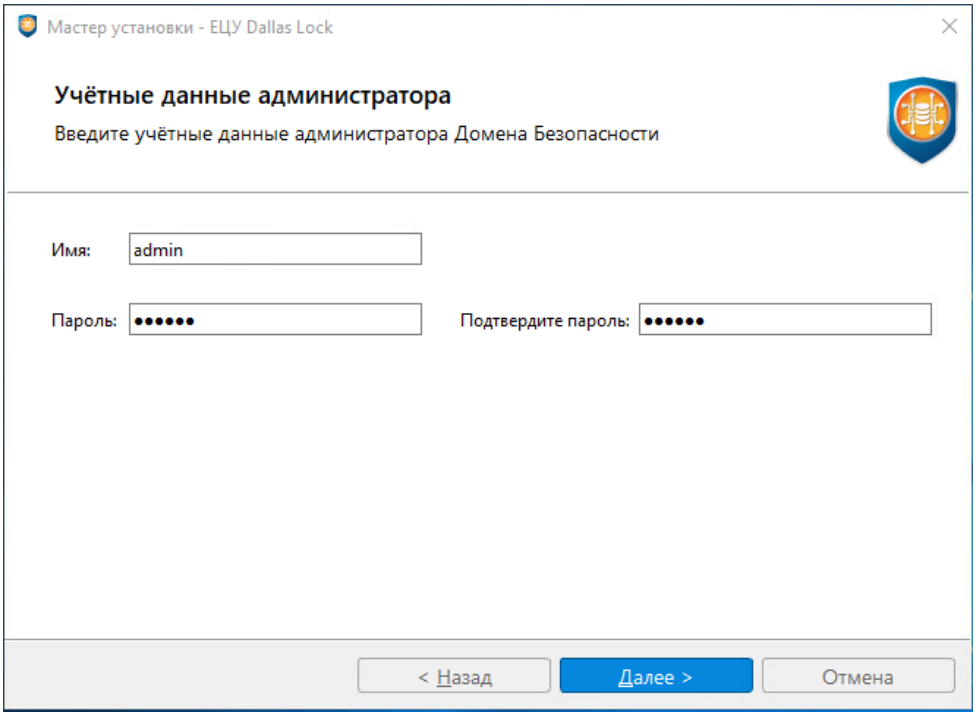

Рис. 6. Настройка параметров учетной записи администратора ДБ

8. Опционально поставить флаг и заполнить поля для использования базы данных PostgreSQL (рис. 7).

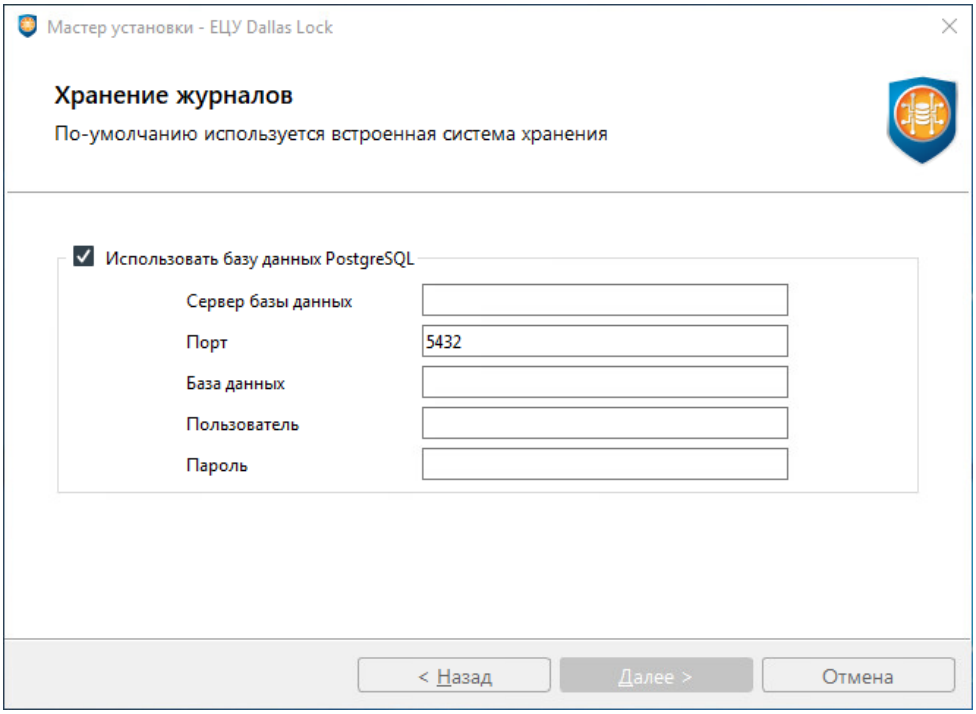

Рис. 7 Настройка базы данных PostgreSQL

Внимание! Способ хранения журналов выбирается в процессе установки ЕЦУ, после установки ЕЦУ изменить способ хранения журналов невозможно.

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 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).

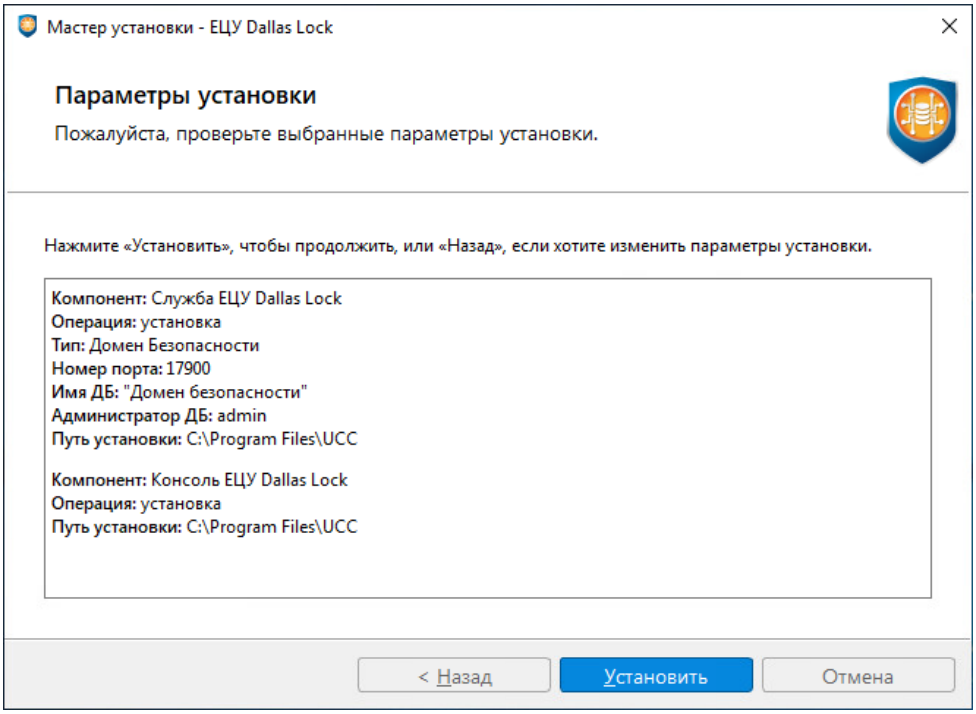

Рис. 8. Проверка параметров установки

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.

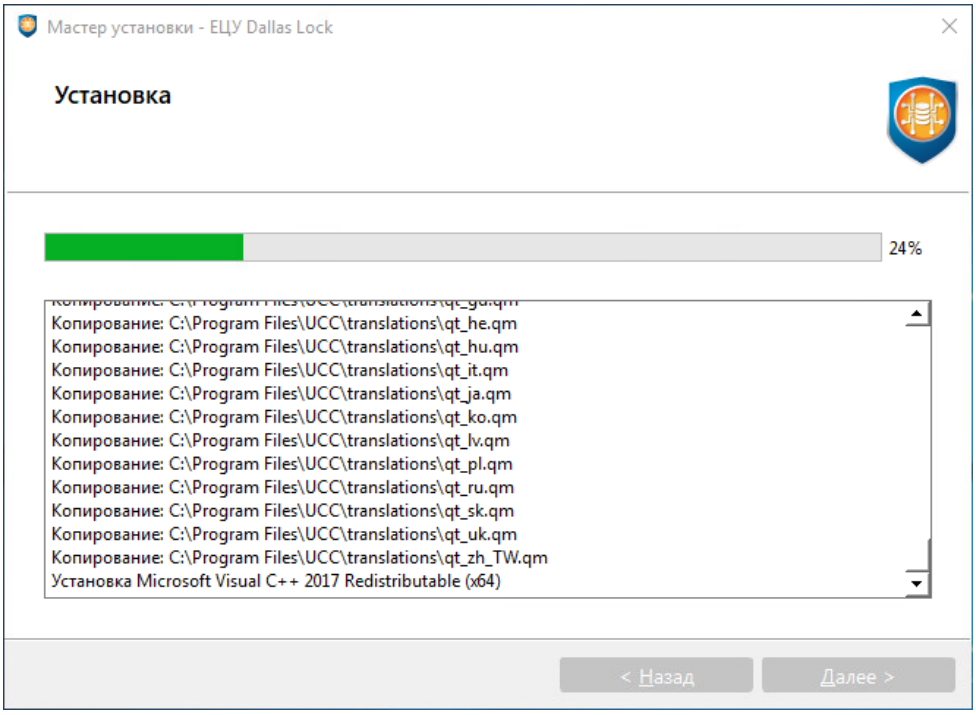

Рис. 9. Процесс установки ЕЦУ Dallas Lock

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

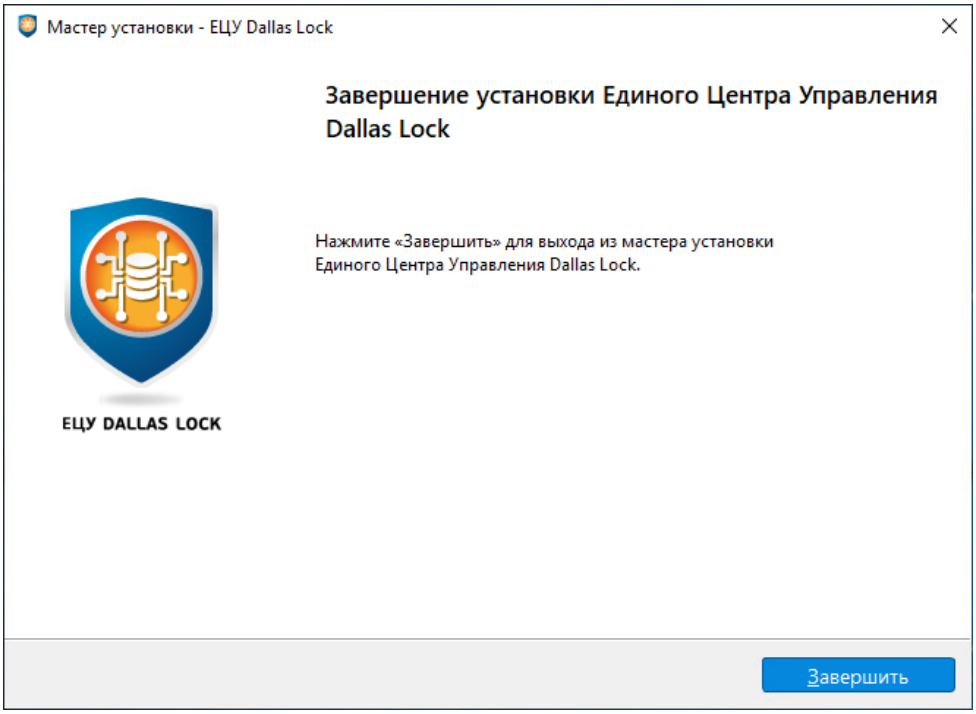

Рис. 10. Завершение процесса установки

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 надо удалить (см. «Порядок удаления ЕЦУ Dallas Lock в ОС семейства Linux») и поставить заново вместе с установкой службы ЕЦУ.

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

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. Для этого следует открыть свойства файла, перейти на вкладку «Права» и убедиться, что в поле «Выполнение» поставлен флаг (рис. 12).

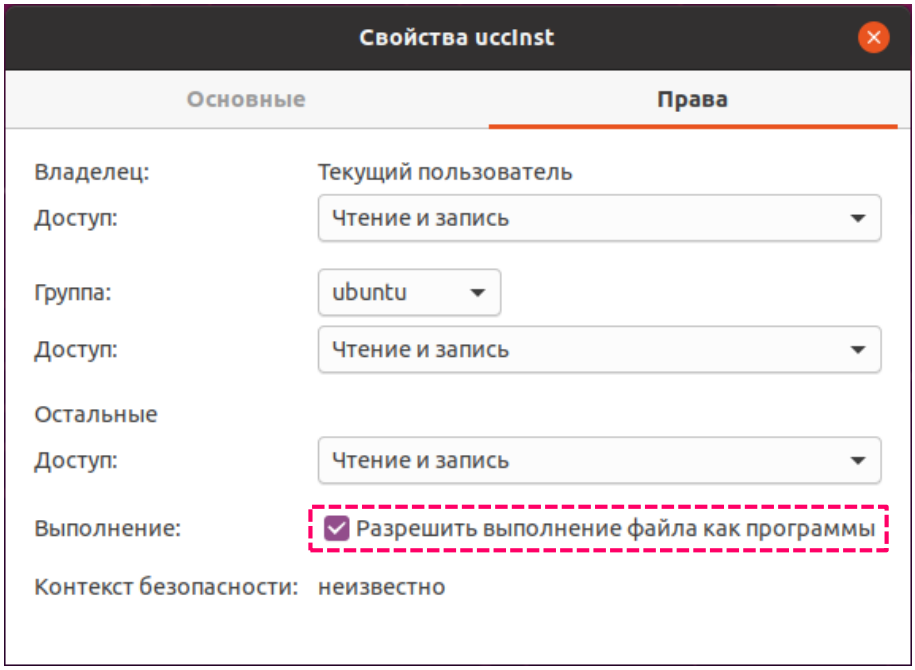

Рис. 12. Добавление прав на выполнение файла программы

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

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

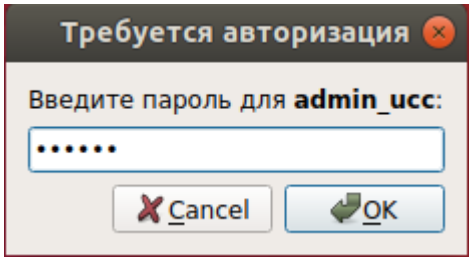

Рис. 13. Запуск программы установки

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

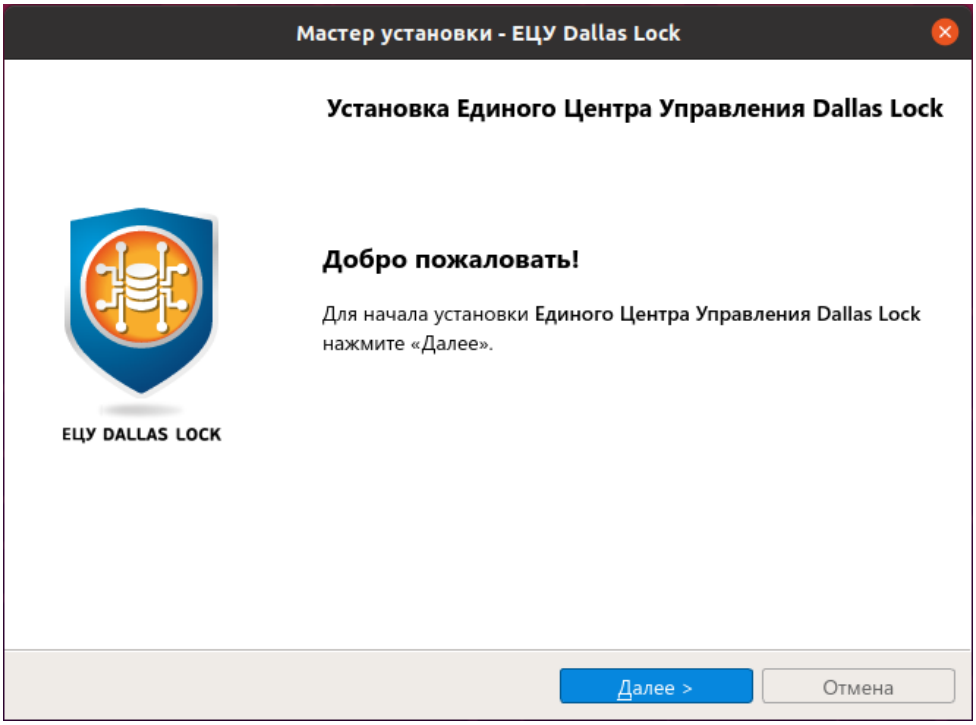

Рис. 14. Окно начала установки ЕЦУ Dallas Lock

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»).

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

2.3 Удаление ЕЦУ Dallas Lock

Примечание. Удаление сервера ЕЦУ, являющегося членом кластера репликации или состоящего в подчинение у другого Домена, не допускается. Перед удалением сервер ЕЦУ 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).

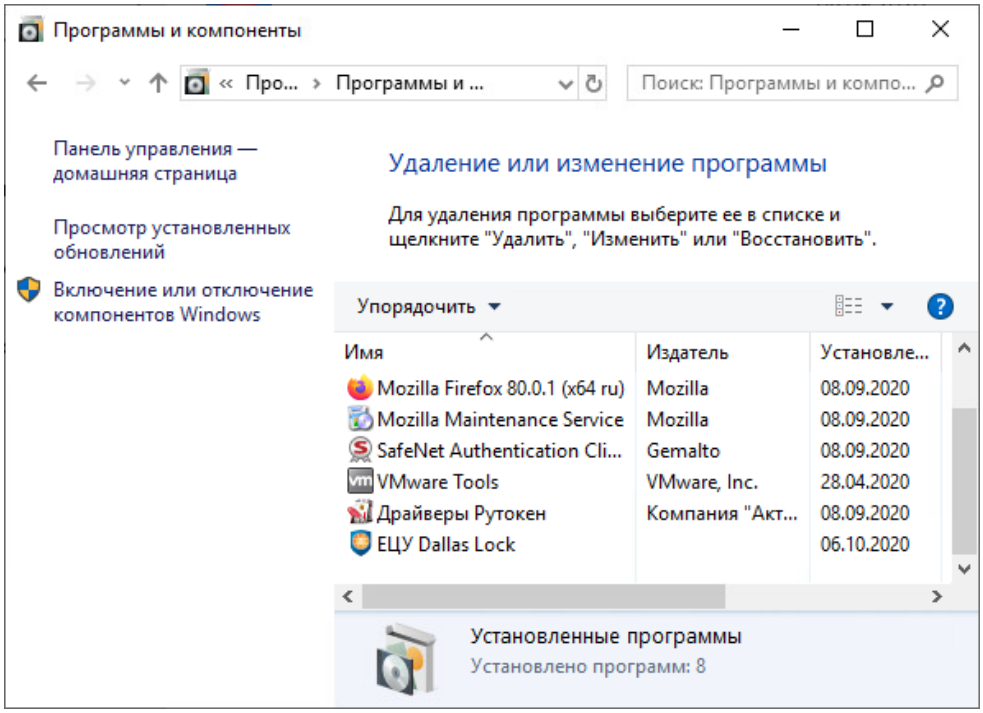

Рис. 16. Удаление ЕЦУ Dallas Lock

1. После подтверждения запустится мастер удаления ЕЦУ Dallas Lock (рис. 17).

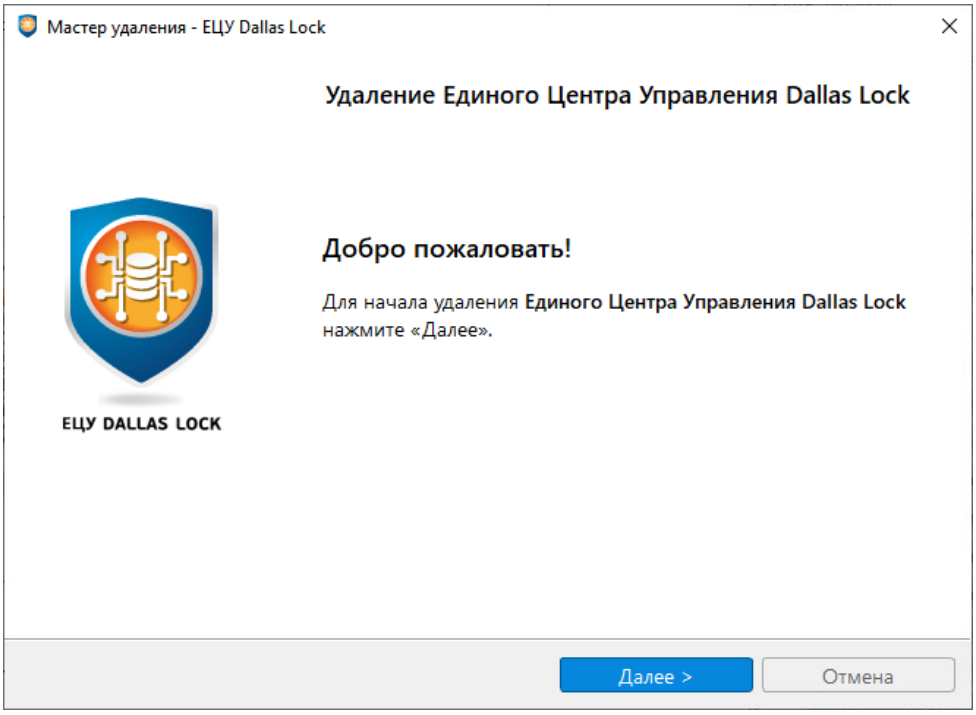

Рис. 17. Окно начала удаления ЕЦУ Dallas Lock

Для продолжения удаления нажать кнопку «Далее».

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

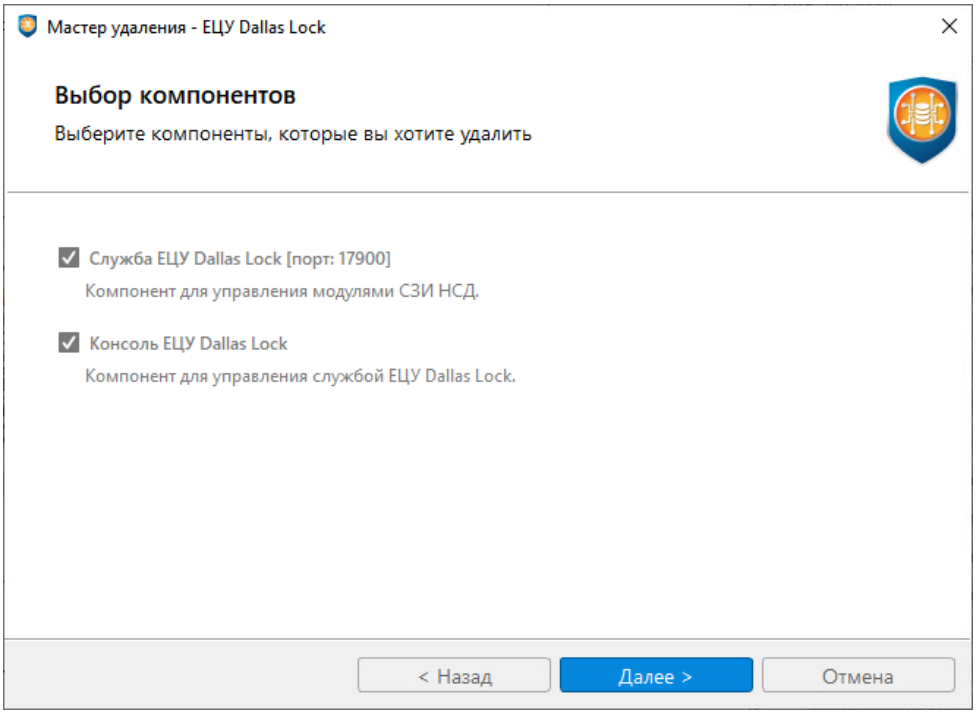

Рис. 18. Выбор компонентов для удаления ЕЦУ Dallas Lock

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

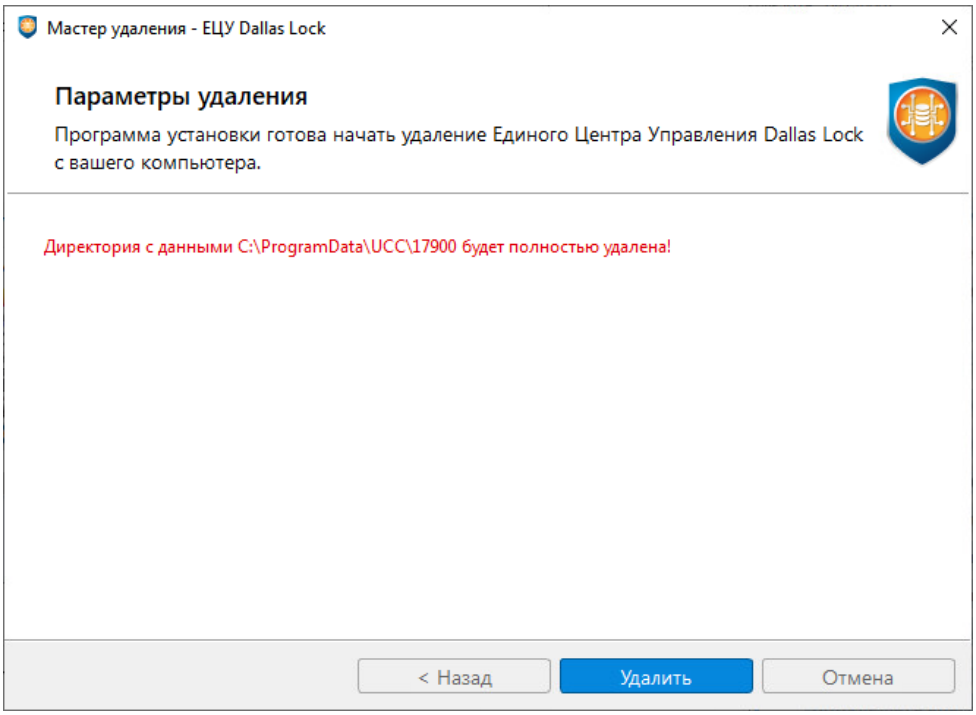

Рис. 19. Параметры удаления

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.

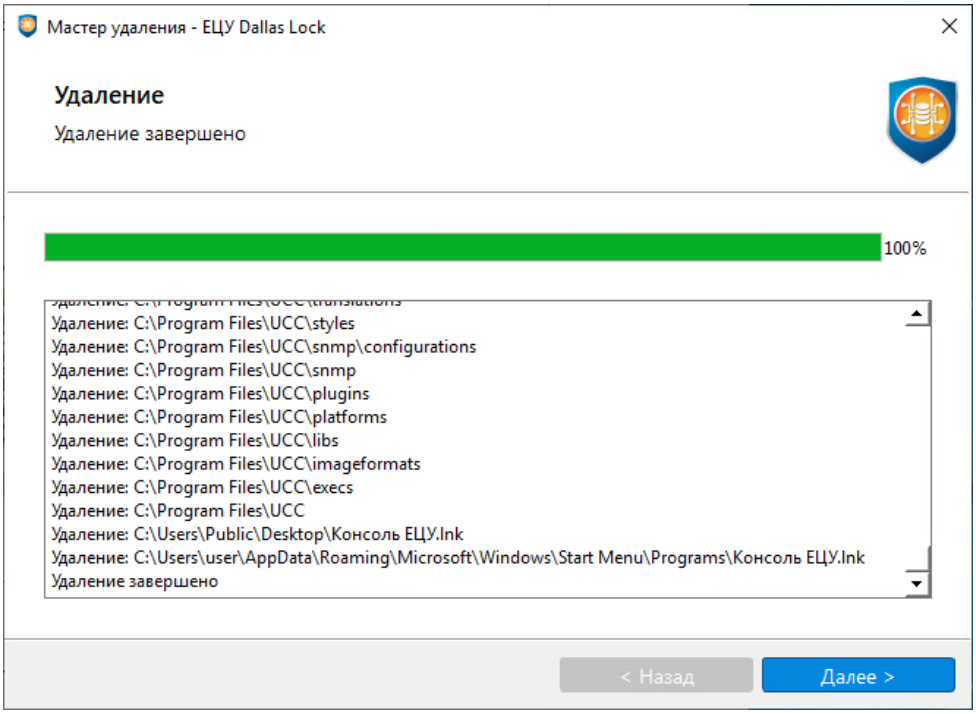

Рис. 20. Процесс удаления ЕЦУ Dallas Lock

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

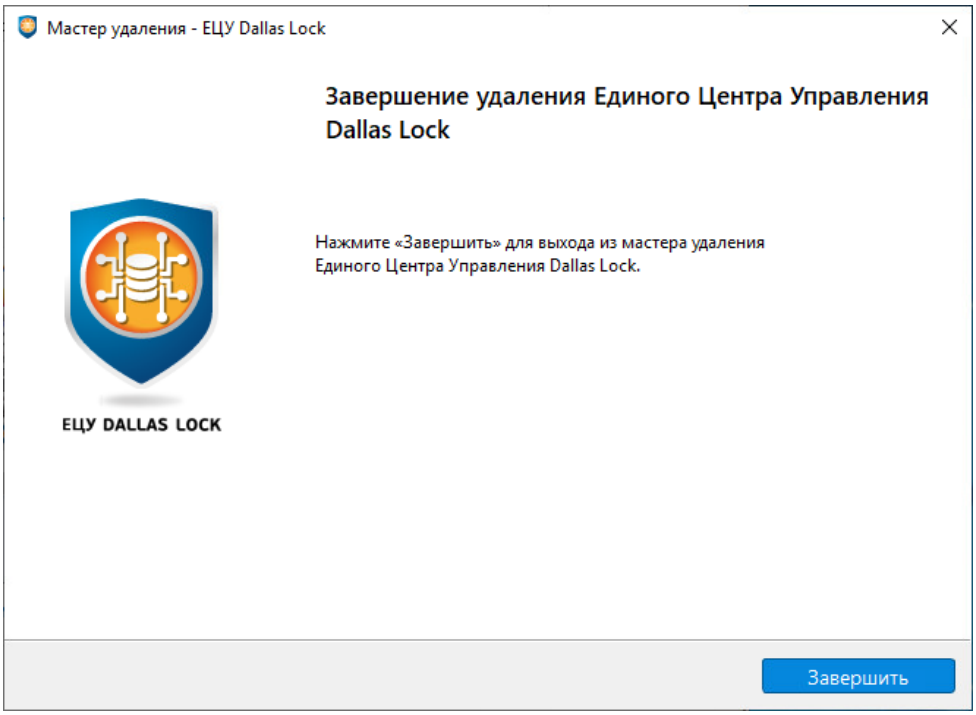

Рис. 21. Завершение процесса удаления

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 в терминале. Для этого необходимо выполнить в терминале команду:

- «*sudo /opt/UCC/uccUninst*».

2. После выполнения команды запустится окно мастера удаления ЕЦУ Dallas Lock (рис. 22).

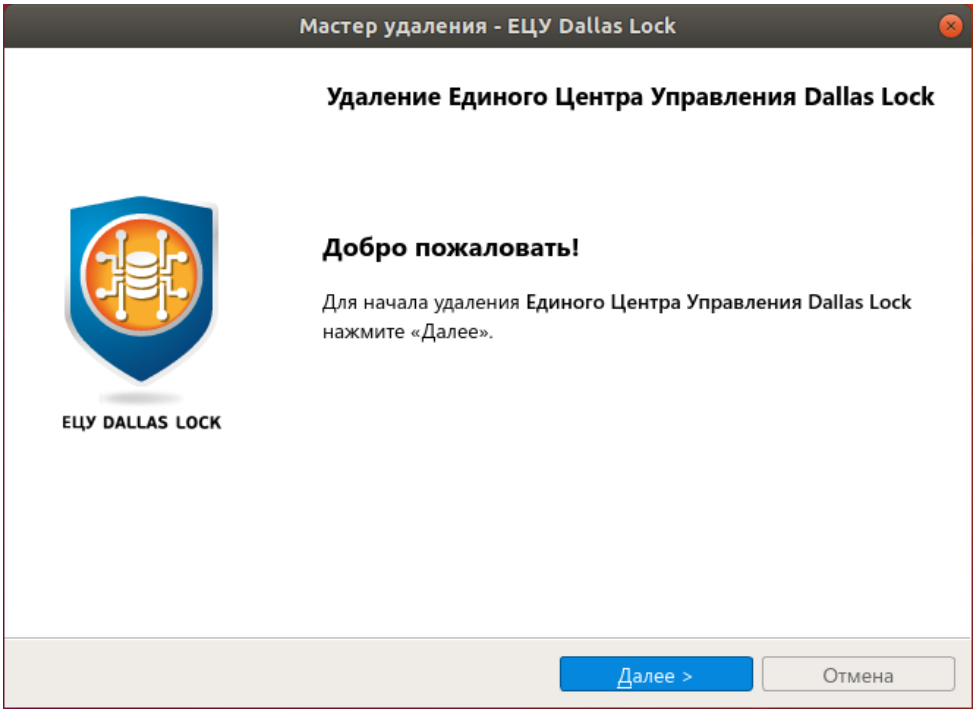

Рис. 22. Окно начала удаления ЕЦУ Dallas Lock

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 существует возможность сохранить текущую конфигурацию сервера для применения на новом сервере после установки.

Примечание. Для применения конфигурации необходимо выполнение следующего условия: сетевое имя ТС, с которого сохраняется конфигурация, и сетевое имя целевого ТС должны совпадать.

2.4.1 Сохранение конфигурации ЕЦУ Dallas Lock в ОС семейства Windows

Для сохранения конфигурации в ОС семействе Windows необходимо выполнить следующую последовательность шагов:

1. открыть службы Windows. Для этого перейти «Панель управления» → «Администрирование» → «Службы» или использовать на клавиатуре сочетание клавиш «Win+R», в открывшемся окне ввести команду «services.msc» и нажать «ОК»;
2. в появившемся списке найти службу ЕЦУ «uccCore-17900» (рис. 23);

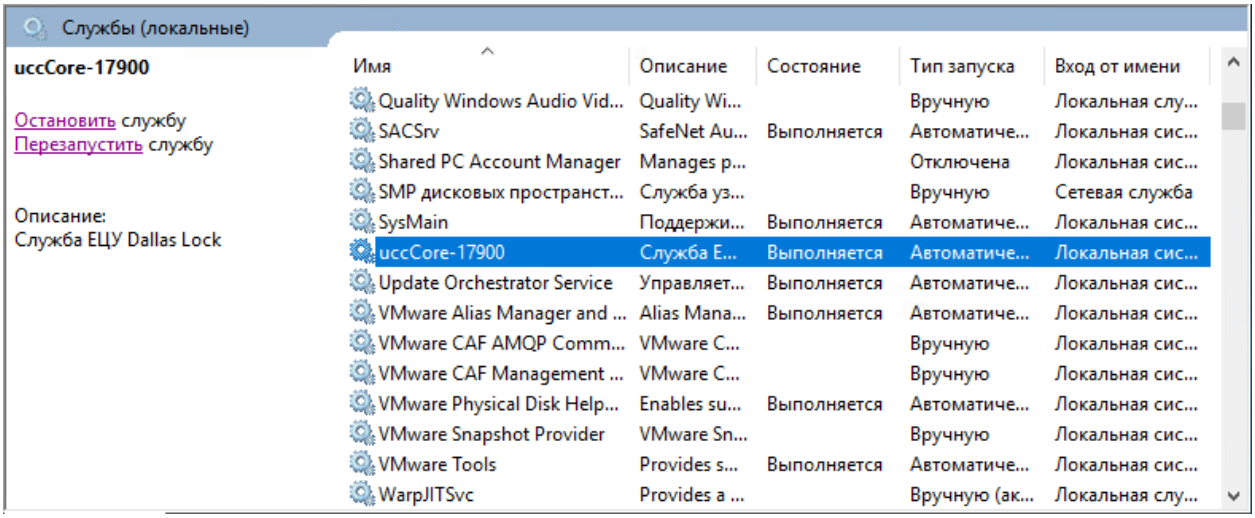

Рис. 23. Служба ЕЦУ

3. остановить службу ЕЦУ, выбрав команду «Остановить службу» на панели справа или выбрав пункт «Остановить» в контекстном меню, вызванном щелчком правой кнопки мыши по имени службы в списке;
4. перейти в папку «C:\ProgramData\UCC\» и скопировать папку «17900» с содержимым на носитель информации для передачи на целевое ТС.

2.4.2 Применение конфигурации ЕЦУ Dallas Lock в ОС семейства Windows

Для применения конфигурации в ОС семействе Windows необходимо выполнить следующую последовательность шагов:

1. задать целевому ТС сетевое имя и IP-адрес исходного ТС;
2. перенести с носителя информации папку «17900» на целевое ТС;
3. установить ЕЦУ на целевом ТС с настройками по умолчанию (если не установлен);
4. открыть службы Windows. Для этого перейти «Панель управления» → «Администрирование» → «Службы» или использовать на клавиатуре сочетание клавиш «Win+R», в открывшемся окне ввести команду «services.msc» и нажать «ОК»;
5. в появившемся списке найти службу ЕЦУ «uccCore-17900» (рис. 23);
6. остановить службу ЕЦУ, выбрав команду «Остановить службу» на панели справа или выбрав пункт «Остановить» в контекстном меню, вызванном щелчком правой кнопки мыши по имени службы в списке;
7. перейти в папку «C:\ProgramData\UCC\» и заменить папку «17900» на папку, перемещенную с носителя информации на шаге 2;
8. открыть службы Windows и запустить «uccCore-17900», выбрав команду «Запустить службу» на панели справа или выбрав пункт «Запустить» в контекстном меню, вызванном щелчком правой кнопки мыши по имени службы в списке.

2.4.3 Сохранение конфигурации ЕЦУ Dallas Lock в ОС семейства Linux

Для сохранения конфигурации ЕЦУ Dallas Lock необходимо обладать правами администратора операционной системы (root) на данном ТС.

Необходимо выполнить следующую последовательность шагов:

1. осуществить остановку службы ЕЦУ, для этого запустить терминал и выполнить команду:
   - «*systemctl stop uccCore-17900*»;
2. перейти в папку «/opt/UCC/» и скопировать папку «17900» с содержимым на носитель информации для передачи на целевое ТС.

2.4.4 Применение конфигурации ЕЦУ Dallas Lock в ОС семейства Linux

Для применения конфигурации ЕЦУ Dallas Lock необходимо обладать правами администратора операционной системы (root) на данном ТС.

Необходимо выполнить следующую последовательность шагов:

1. задать целевому ТС сетевое имя и IP-адрес исходного;
2. установить ЕЦУ на целевом ТС с настройками по умолчанию (если не установлен);
3. осуществить остановку службы ЕЦУ, для этого запустить терминал и выполнить команду:
   - «*systemctl stop uccCore-17900*»;
4. удалить папку с конфигурацией по умолчанию, для этого в терминале выполнить команду:
   - «*rm -rf /opt/UCC/17900*»;
5. перейти в папку «/opt/UCC/» и переместить в нее с носителя информации папку «17900», переданную с исходного ТС;
6. запустить службу ЕЦУ, для этого в терминале выполнить команду:
   - «*systemctl start uccCore-17900*».

2.5 О программе

Со следующими сведениями о ЕЦУ можно ознакомиться в информационном окне «О программе» (рис. 24), вызвав его из списка дополнительных функций кнопки главного меню в консоли ЕЦУ :

- полное наименование программы;
- номер сборки консоли;
- номер сборки службы ЕЦУ.

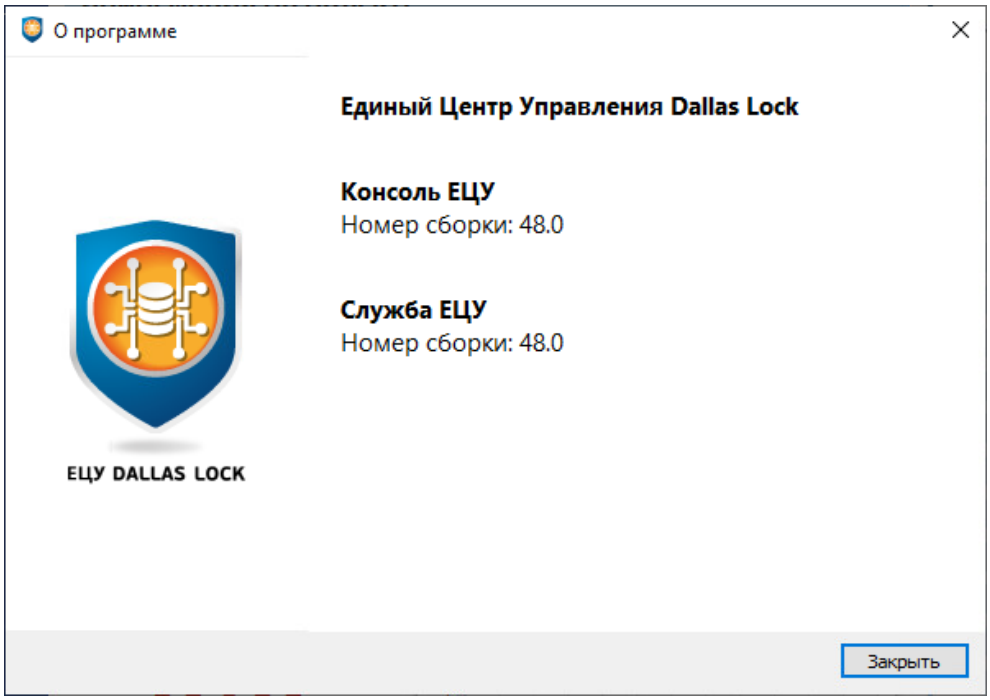

Рис. 24. Окно «О программе»

3 ОБЩИЕ ПРИНЦИПЫ РАБОТЫ ЕЦУ DALLAS LOCK

3.1 Синхронизация

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

Что бы ни происходило на подчиненном объекте, какие бы настройки параметров умышленные или злоумышленные ни производились, при синхронизации все настраивается согласно записям Домена безопасности ЕЦУ. 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 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 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 в следствие того, что 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 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 размера 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

Если консоль и служба ЕЦУ расположены на разных компьютерах, то запуск Консоли будет осуществляться 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. 25).

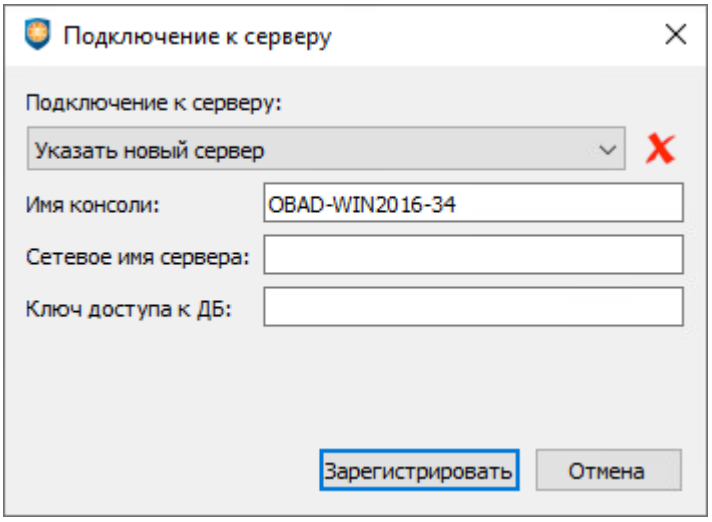

Рис. 25. Регистрация консоли ЕЦУ в Домене безопасности

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

Далее в окне подключения к серверу требуется ввести данные (рис. 26):

- выбрать из списка доступных сервер, к которому необходимо подключиться;
- указать имя пользователя ДБ;
- предъявить и выбрать аппаратный идентификатор (если настроено использование средств аппаратной идентификации);
- ввести пароль учетной записи пользователя ДБ.

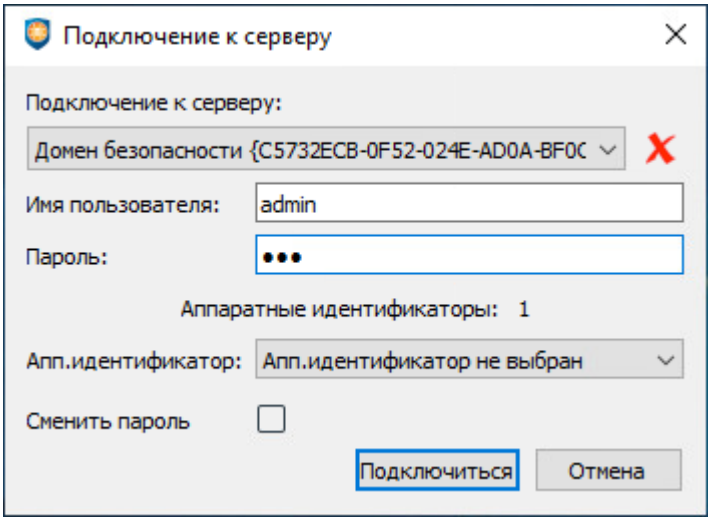

Рис. 26. Ввод пароля учетной записи для входа в Консоль ЕЦУ

При необходимости можно произвести смену пароля для указанной учетной записи, поставив перед нажатием кнопки «Продолжить» флаг в поле «Сменить пароль» (рис. 27).

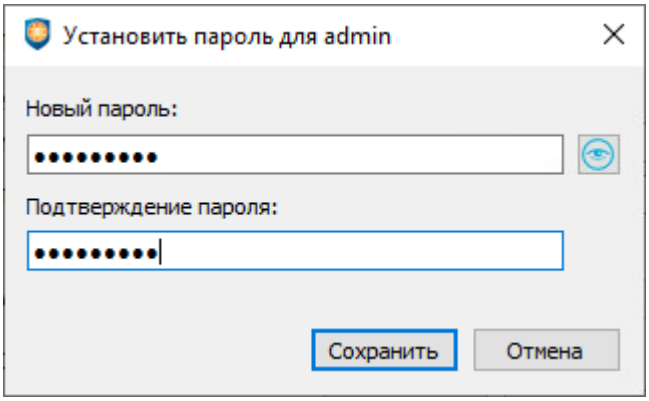

Рис. 27. Установка нового пароля пользователя

4.2 Описание консоли ЕЦУ

Главное окно консоли ЕЦУ содержит следующие рабочие области (рис. 28):

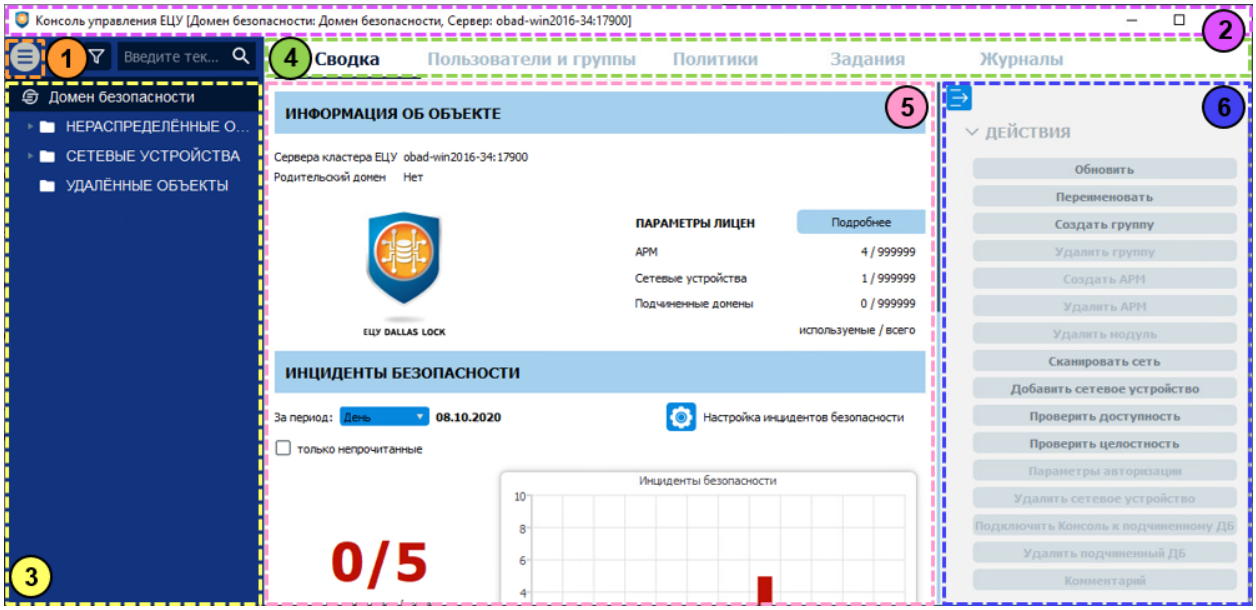

Рис. 28. Главное окно консоли ЕЦУ

1. кнопка главного меню ЕЦУ;
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;
5. содержание рабочей области вкладки управления объектом ЕЦУ;
6. панель инструментов.

Кнопка главного меню консоли ЕЦУ содержит следующие пункты (рис. 29):

- «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»);
- «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»);
- «Удаленное развертывание DL Linux» (см. «Централизованная установка СЗИ НСД Dallas Lock Linux»);
- «Подготовить дистрибутив DL8.0 для AD» (см. «Централизованная установка СЗИ Dallas Lock 8.0 средствами AD»);
- «Параметры…» (см. «Параметры работы»);
- «О программе» (см. «О программе»);
- «Выход».

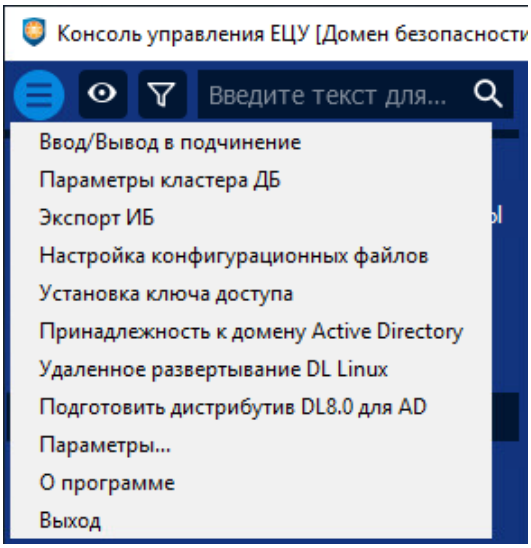

Рис. 29. Пункты главного меню

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 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 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, 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» времени (при условии, что настроено оповещение об отсутствии связи с объектом), состояние АРМ — «долго не выходил на связь».

В дереве напротив объекта, на котором произошли инциденты безопасности индицируется их количество (рис. 30).

Рис. 30. 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. 31).

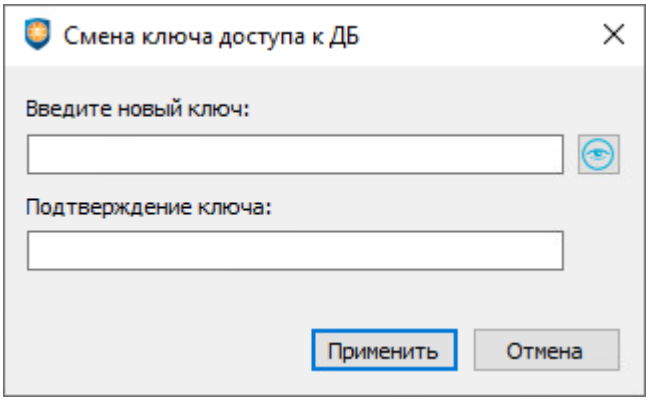

Рис. 31. Ключ доступа к ДБ

Примечание. Политики сложности паролей в ЕЦУ 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 устанавливает количественные ограничения по следующим подчиненным объектам:

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

Управление лицензией на ЕЦУ 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. 32).

Рис. 32. Информация о параметрах лицензии

При нажатии кнопки «Подробнее» появляется окно «Состояние лицензии» (рис. 33), которое содержит информации о состоянии лицензии для данного сервера, а также для каждого сервера в кластере ДБ.

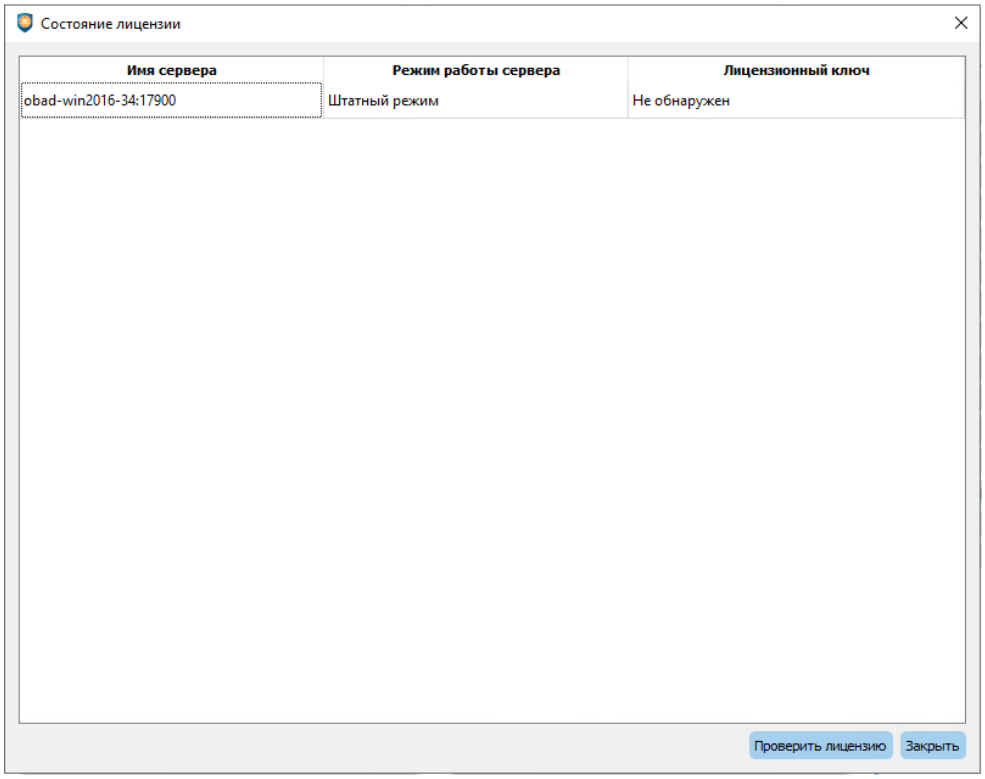

Рис. 33. Окно «Состояние лицензии»

Для применения лицензии на сервер ЕЦУ необходимо предъявить аппаратный ключ и нажать кнопку «Проверить лицензию». 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. 34).

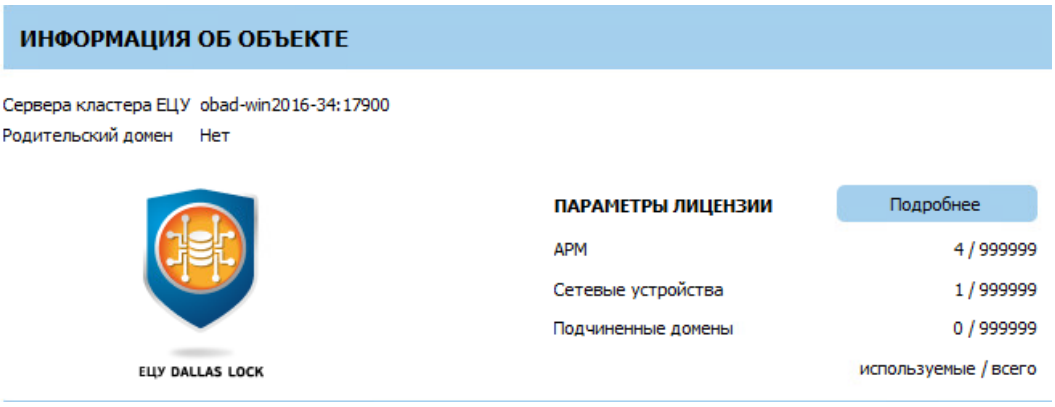

Рис. 34. Информация о параметрах лицензии

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, и 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 распростятся на отображение всех уровней ДБ.

В ЕЦУ предусмотрена возможность пользовательской настройки визуализации диаграмм инцидентов безопасности и управления оповещениями в зависимости от приоритета и типа события. Кнопка настройки доступна на вкладке «Состояние» → «Настройка инцидентов безопасности» (рис. 35).

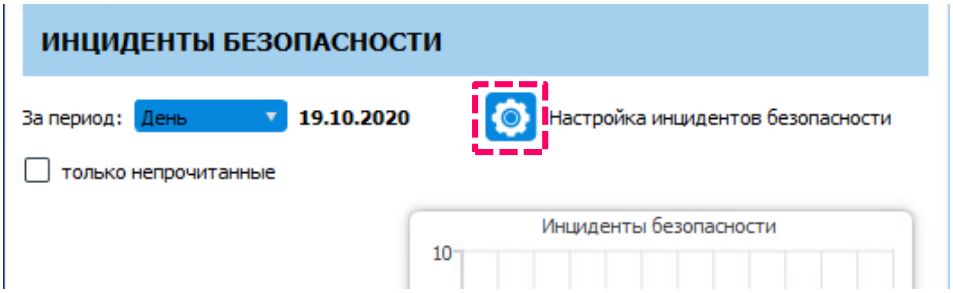

Рис. 35. Настройка инцидентов безопасности

При нажатии кнопки, появляется окно «Настройка инцидентов безопасности» (рис. 36).

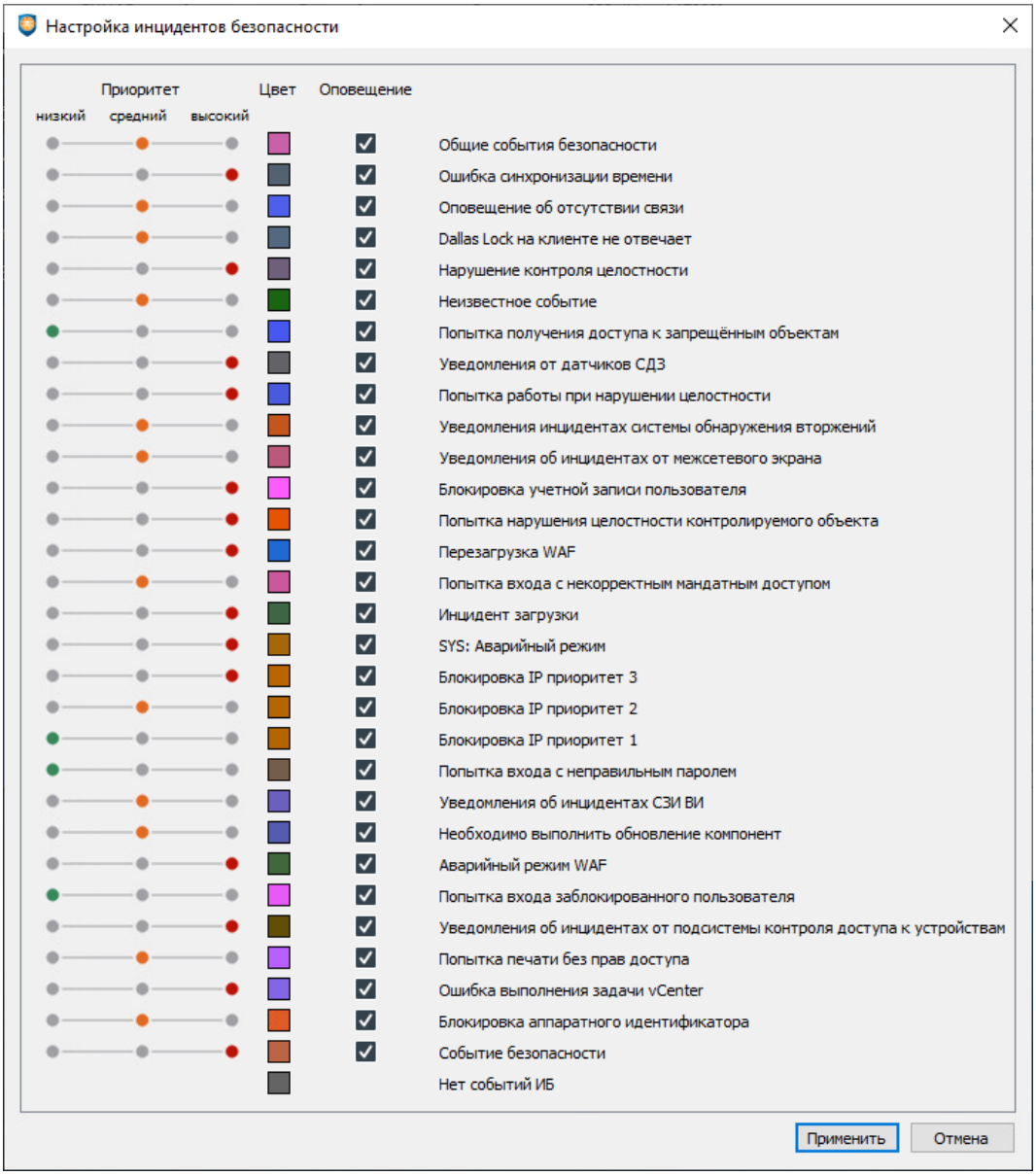

Рис. 36. Настройка инцидентов безопасности

В окне расположена таблица, состоящая из четырех полей. В правом поле приведен список доступных инцидентов безопасности, для которых осуществляется настройка.

В левом поле 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» на вкладке «Сводка» → «Инциденты безопасности».

Во втором поле слева производится настройка раскраски сегментов диаграммы «По типу» на вкладке «Сводка» → «Инциденты безопасности». Для смены цвета инцидента безопасности нужно нажать левой кнопкой мыши на навигаторе цвета и выбрать цвет из палитры (рис. 37).

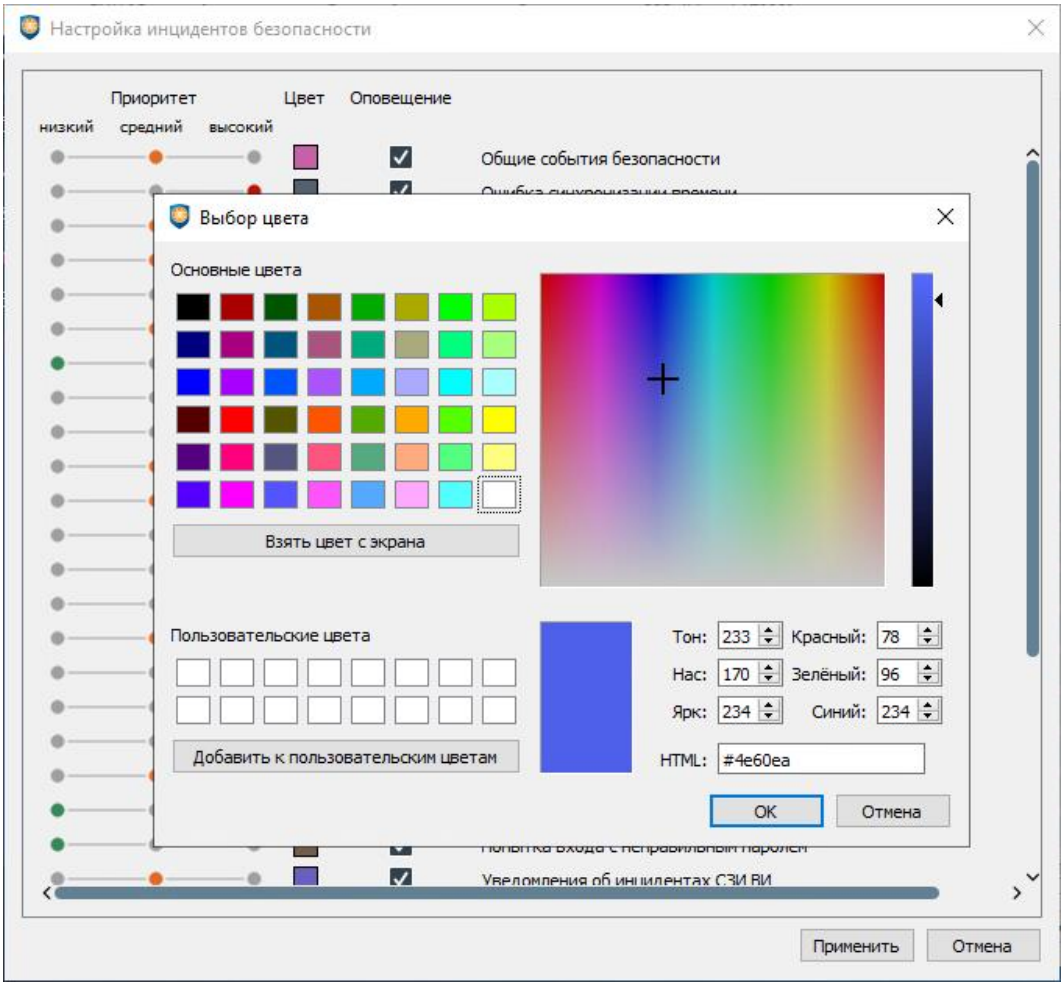

Рис. 37. Выбор цвета инцидента безопасности

Инциденты безопасности на модулях отслеживаются и сопровождаются сигнализацией на ЕЦУ. На ПК с запущенной консолью ЕЦУ воспроизводится звуковой сигнал о событии безопасности и выводится всплывающее сообщение в области уведомлений (рис. 38).

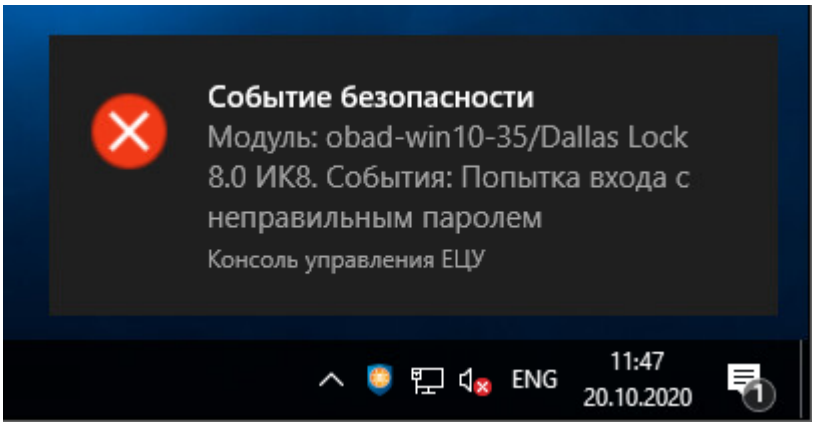

Рис. 38. Уведомление о событии безопасности на модуле

Включение/отключение сообщений в области уведомлений осуществляется в третьем слева поле в «Настройке инцидентов безопасности». Для включения сообщения в строке, относящейся к данному типу событий, нужно поставить флаг в столбце «Оповещение». Для отключения сообщения в соответствующей строке необходимо убрать флаг в столбце «Оповещение».

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 корректно 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);
   - раскомментировать в файле *postgresql.conf* следующую строку:

     «*listen_addresses = '*'*»

     Это позволит PostgreSQL отвечать на любом интерфейсе сервера (или настроить работу на определённом сетевом интерфейсе, доступном по сети с сервера ЕЦУ);
   - создать отдельную базу данных и учетную запись в PostgreSQL для ЕЦУ, 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 и легкого 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. После разворачивания кластера серверов ЕЦУ не допускаются изменения настроек сетевых адаптеров, сетевого имени сервера, FQDN имени в записи DNS-сервера и добавление DNS-записей, связанных с серверами ЕЦУ, т.к. это может повлечь неработоспособность кластера.

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

Ввод в кластер ДБ в процессе установки

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

1. запустить процесс установки ЕЦУ;
2. на шаге «Выбор типа домена» выбрать пункт «Сервер репликации» (рис. 39);

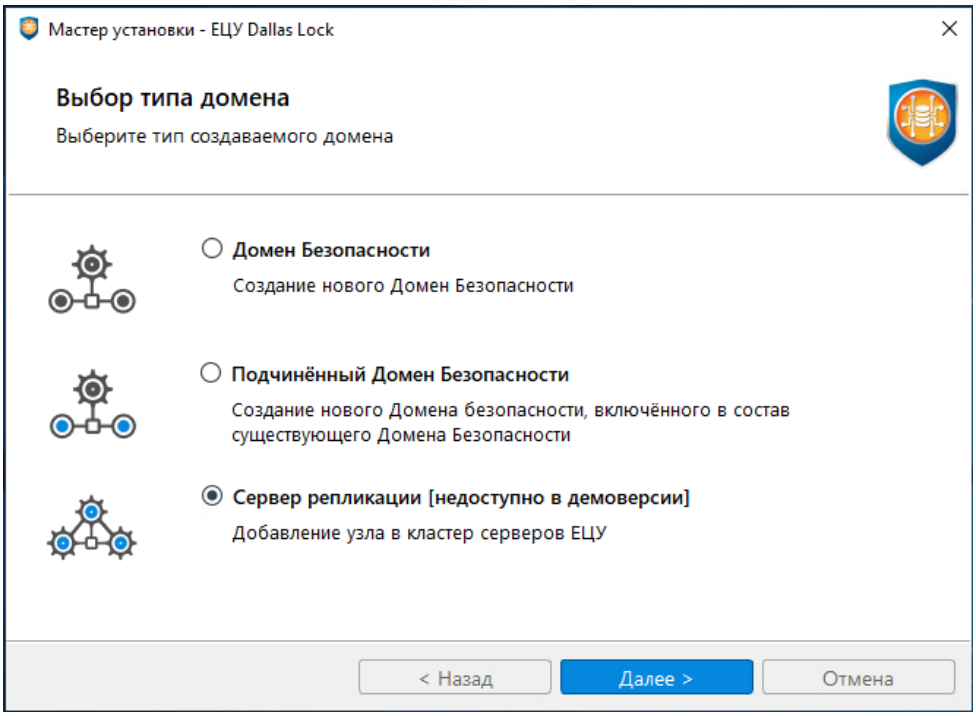

Рис. 39. Выбор типа создаваемого домена

3. задать параметры главного ДБ (рис. 40):
   - адрес главного ДБ;
   - ключ доступа к ДБ;

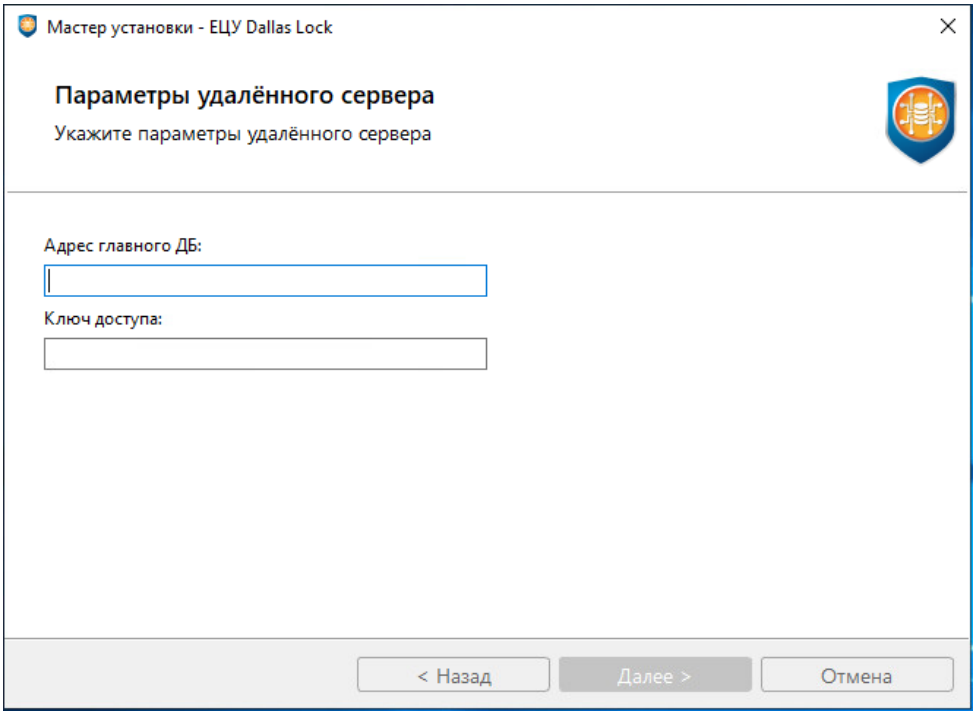

Рис. 40. Параметры удаленного сервера

4. далее продолжить и завершить установку ЕЦУ;
5. после завершения установки на серверах кластера ЕЦУ на вкладке «Сводка» → «Информация об объекте» появится имя добавленного узла.

Ввод в кластер ДБ после установки

Внимание! При вводе в кластер ДБ будут потеряны ранее добавленные в сервер ЕЦУ 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».

Появится окно «Параметры кластера ДБ», где можно ввести текущий сервер ЕЦУ в кластер ДБ для репликации (рис. 41).

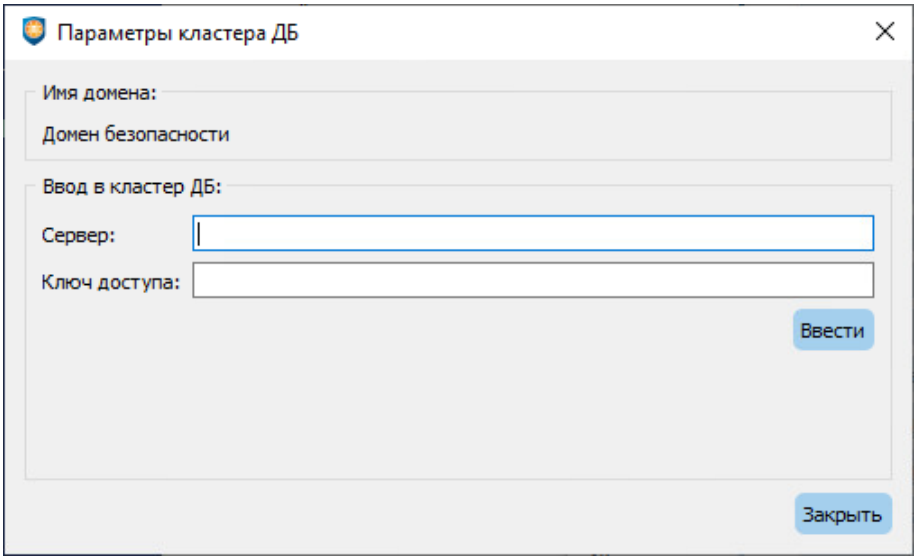

Рис. 41. Параметры кластера ДБ

После заполнения данных главного сервера ДБ и нажатия кнопки «Ввести» появится информационное сообщение об успешной регистрации сервера (рис. 42).

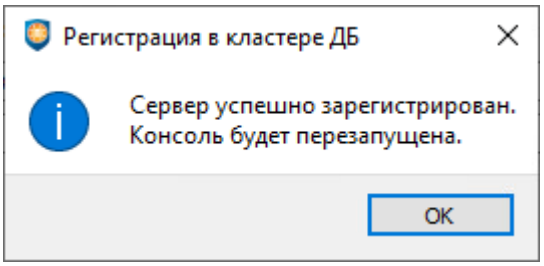

Рис. 42. Сообщение о регистрации в кластере ДБ

Далее консоль ЕЦУ перезапускается и необходимо выполнить регистрацию экземпляра консоли ЕЦУ как при первом запуске (см. «Запуск консоли ЕЦУ») и подключиться к серверу. На уровне ДБ на вкладке «Сводка» → «Информация об объекте» отобразятся имена всех серверов кластера ЕЦУ, а также рассчитаются количественные ограничения лицензии согласно особенностям назначения квот для домена (см. «Особенности лицензирования кластера ДБ») (рис. 43).

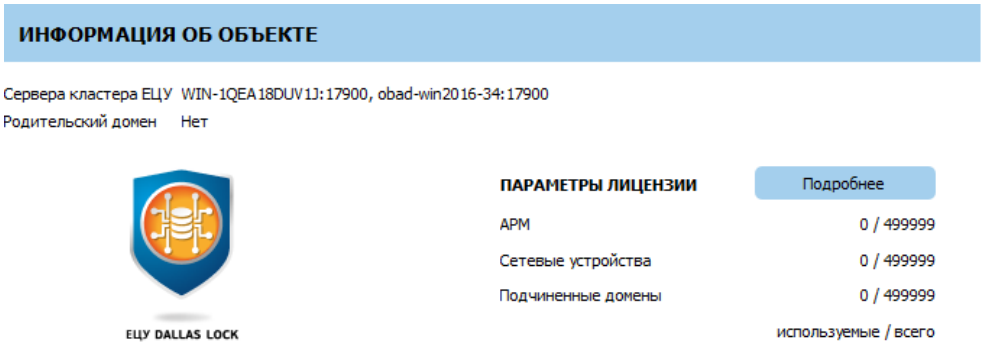

Рис. 43. Информация о кластере серверов

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 нужно выбрать сервер для вывода и нажать кнопку «Вывести» (рис. 44). Появится сообщение об успешном выводе сервера из кластера ЕЦУ и далее консоль ЕЦУ перезапустится.

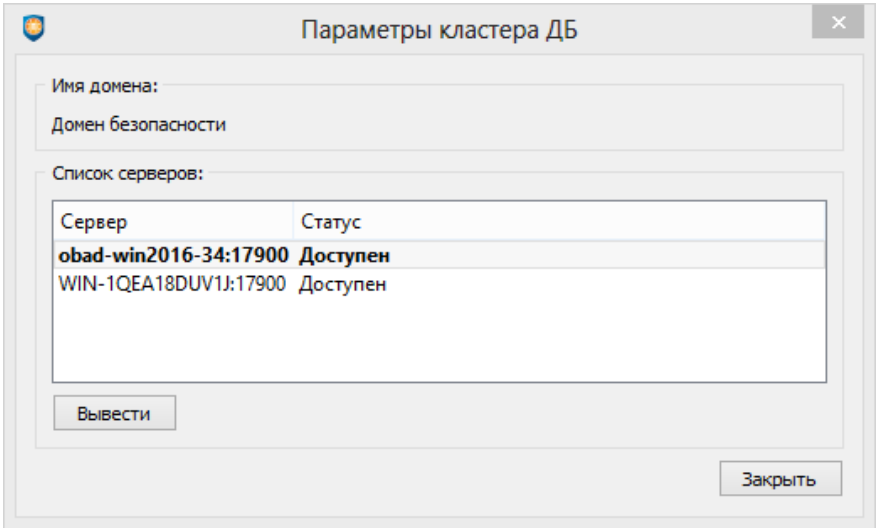

Рис. 44. Список серверов кластера ДБ

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. 45).

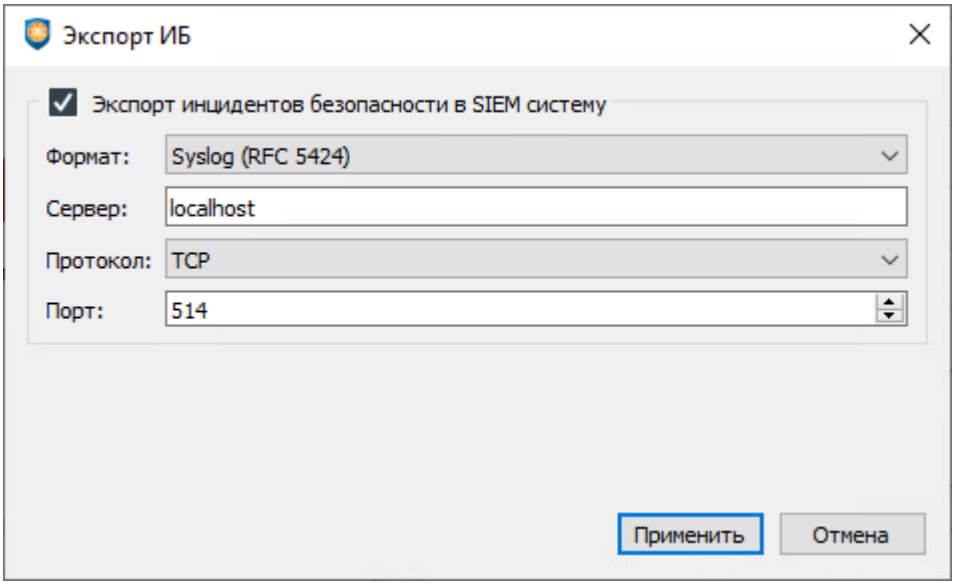

Рис. 45. Экспорт инцидентов безопасности в SIEM

В окне необходимо:

1. поставить флаг «Экспорт инцидентов безопасности в SIEM систему»;
2. указать сетевое имя сервера;
3. выбрать протокол и порт подключения;
4. выбрать формат экспорта.
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 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. 46).

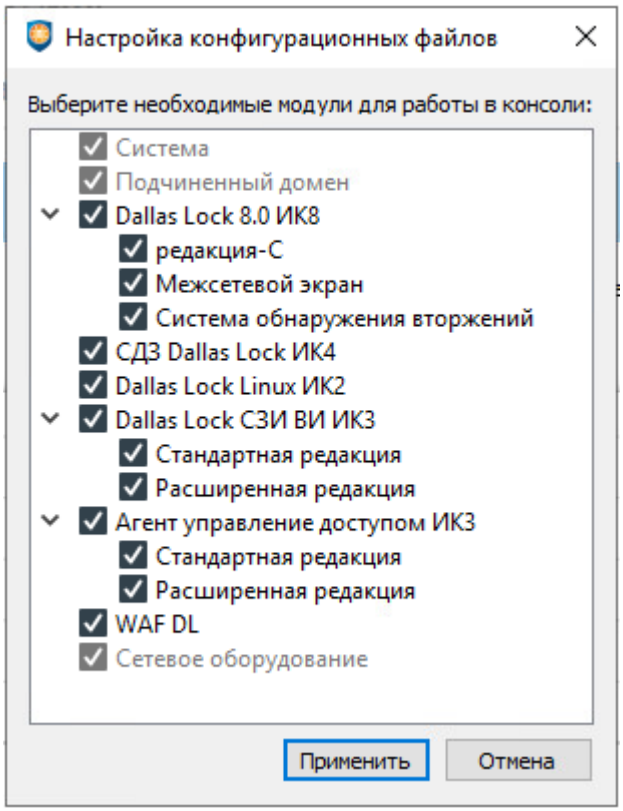

Рис. 46. Настройка конфигурационных файлов

В окне необходимо проставить флаги в соответствии с тем, с какими объектами предполагается работа в данном экземпляре консоли.

4.5.5 Принадлежность к домену Active Directory

Для обеспечения возможности регистрации в Домене безопасности ЕЦУ 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 контроллера домена.

Для просмотра информации о том, к какому домену AD принадлежит ЕЦУ, необходимо открыть главное меню консоли ЕЦУ → «Принадлежность к домену Active Directory».

Появится окно «Принадлежность к домену Active Directory» (рис. 47).

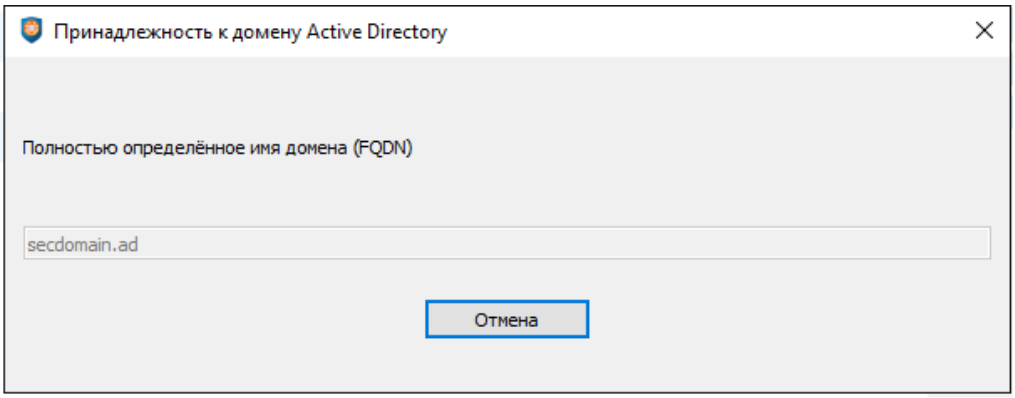

Рис. 47. Принадлежность к домену Active Directory

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 настраиваются в главном меню консоли ЕЦУ → «Параметры…» (рис. 48).

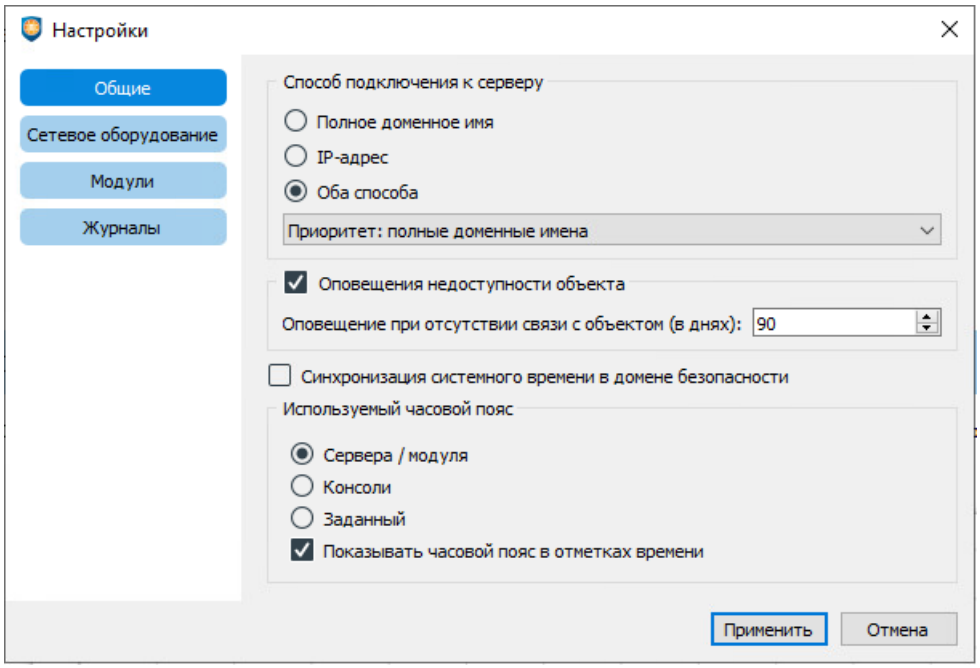

Рис. 48. Общие параметры

Общие параметры работы

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

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

- полные доменные имена;
- IP-адреса;
- оба способа с приоритетом подключения по:
  - полным доменным именам;
  - по 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.

Параметр «Используемый часовой пояс» задает вид отображения времени в журналах в консоли ЕЦУ.

Параметры сетевого оборудования

На вкладке «Сетевое оборудование» задается периодичность проверок сетевого оборудования по протоколу SNMP (рис. 49).

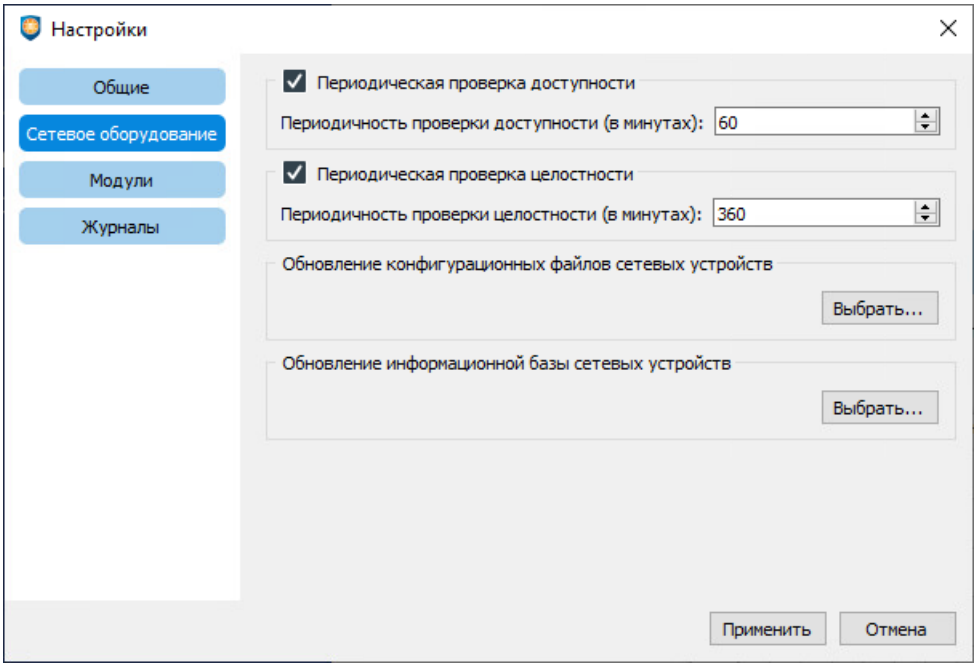

Рис. 49. Параметры SNMP

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.

Добавить не указанные в ЕЦУ соответствия цифровых значений и названий для *systemObjectId* можно, отредактировав вручную файл *snmp-sysobject-ids.ids*, который располагается:

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

Также по запросу через техподдержку можно получить обновления конфигурационных файлов и информационной базы сетевых устройств. Для применения полученных обновлений необходимо воспользоваться командами «Обновление конфигурационных файлов сетевых устройств» или «Обновление информационной базы сетевых устройств» соответственно.

Дополнительно предусмотрена возможность загрузки обновлений базы конфигурационных файлов с сайта разработчика. После загрузки необходимо разархивировать конфигурационные файлы и указать путь к ним.

Параметры работы модулей

На вкладке «Модули» задается периодичность сбора журналов и синхронизации ЕЦУ с модулями (рис. 50).

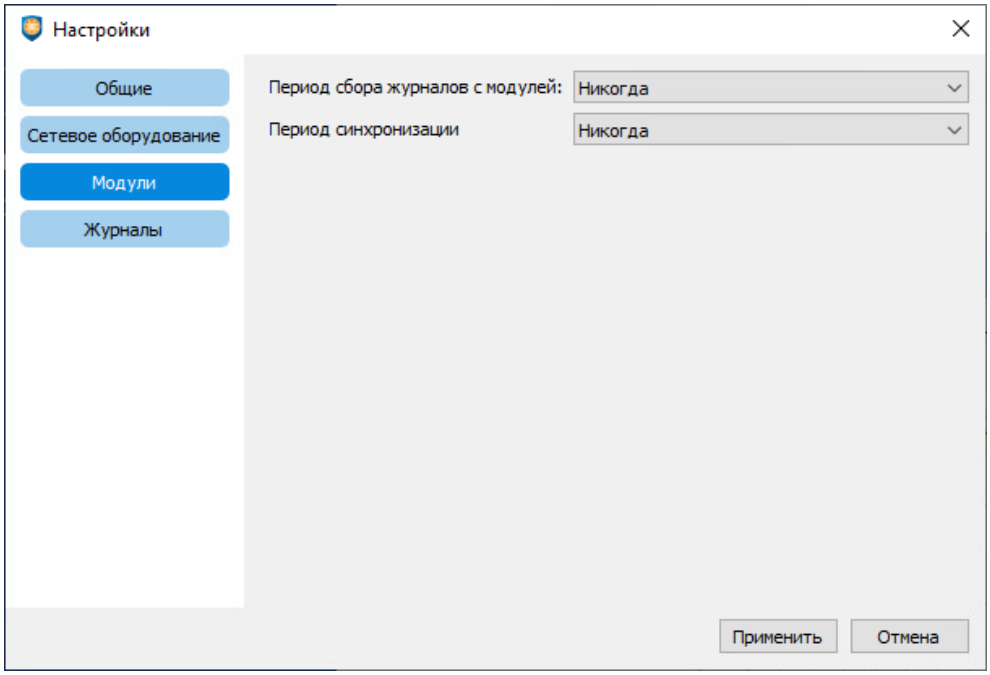

Рис. 50. Параметры модулей

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

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

Параметры хранения журналов

На вкладке «Журналы» (рис. 51) отображается информация о текущем способе хранения журналов, выбранном в процессе установки (см. «Порядок установки ЕЦУ Dallas Lock в ОС семейства Windows»).

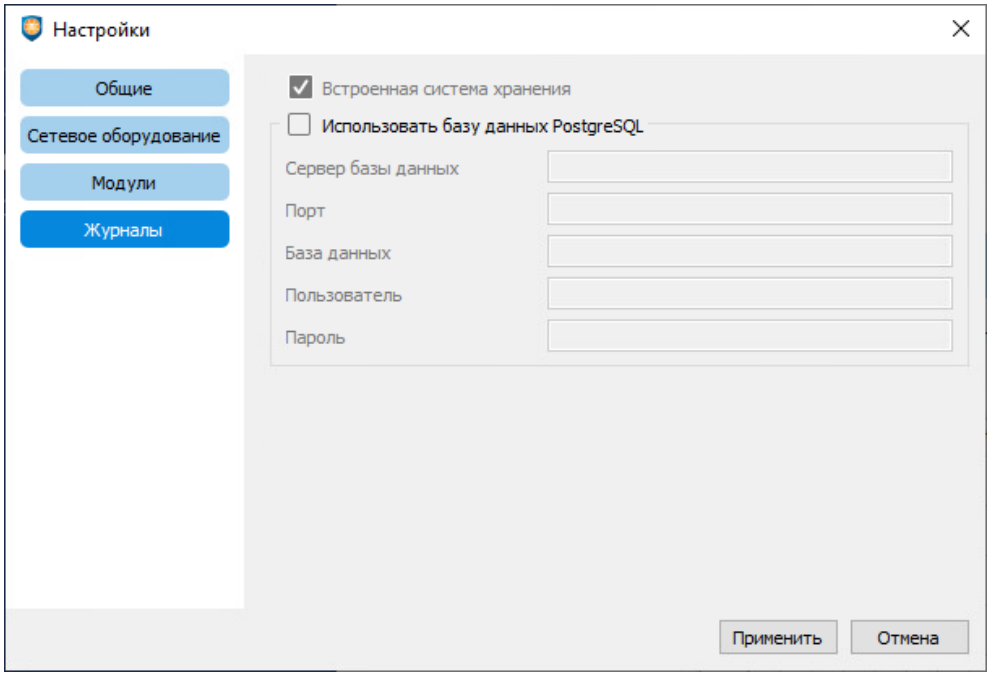

Рис. 51. Параметры хранения журналов

5 ДОМЕН БЕЗОПАСНОСТИ ЕЦУ

На уровне ДБ в дереве объектов в 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.

5.1 Сводка для ДБ

Для удобства работы возможно узнать общее состояние всего ДБ, данные сведения отображаются на вкладке «Сводка» (рис. 52).

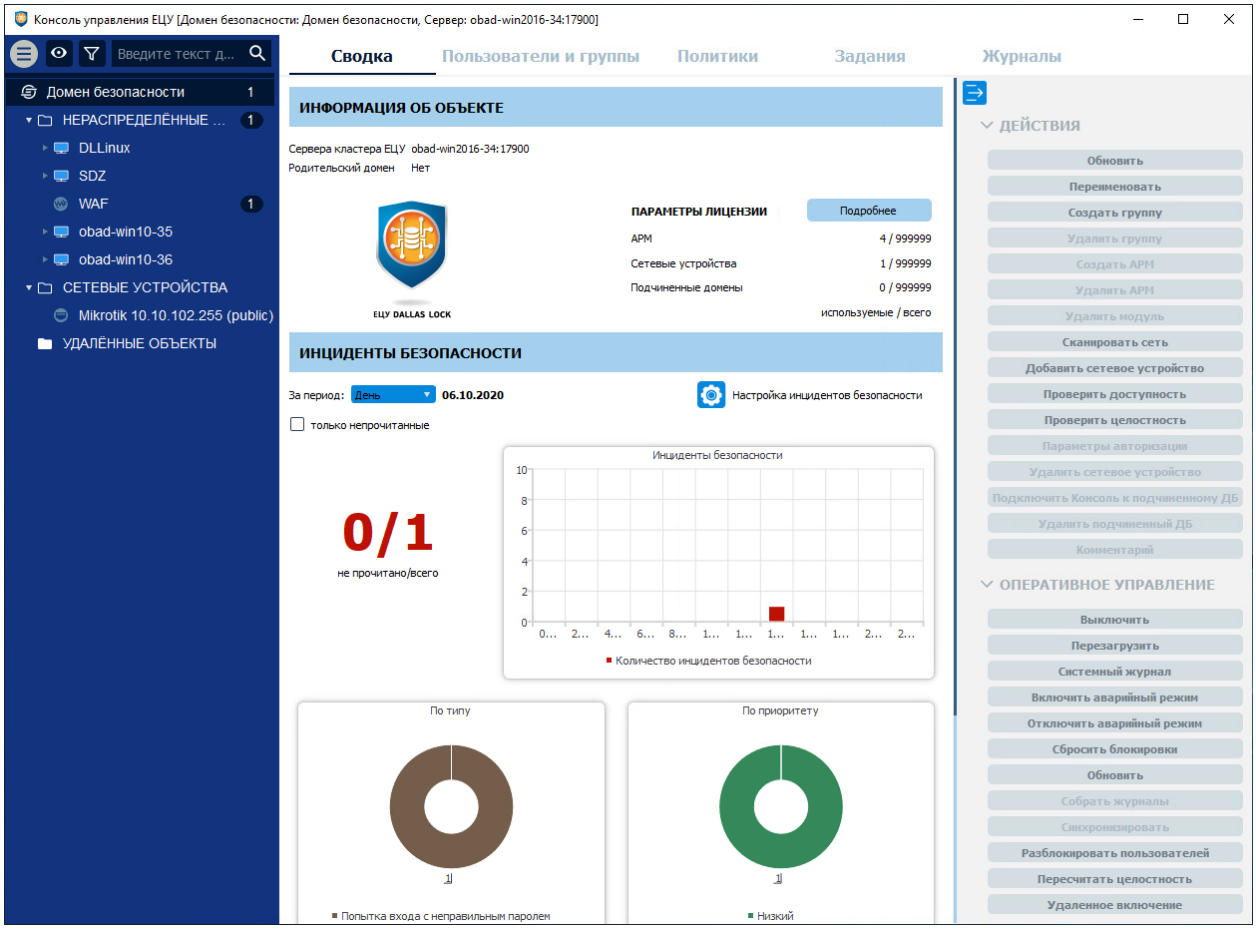

Рис. 52. «Сводка» Домена безопасности ЕЦУ

Доступны следующие действия с ДБ на панели инструментов:

1. обновить информацию об объекте, расположенную 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.

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.

В рабочей области вкладки «Сводка» расположены следующие разделы:

1. «Информация об объекте» (рис. 53).

В данном разделе выводится информация:

- о серверах, введенных в кластер домена безопасности;
- о наличии родительского домена;
- о состоянии и параметрах лицензии на ЕЦУ (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.

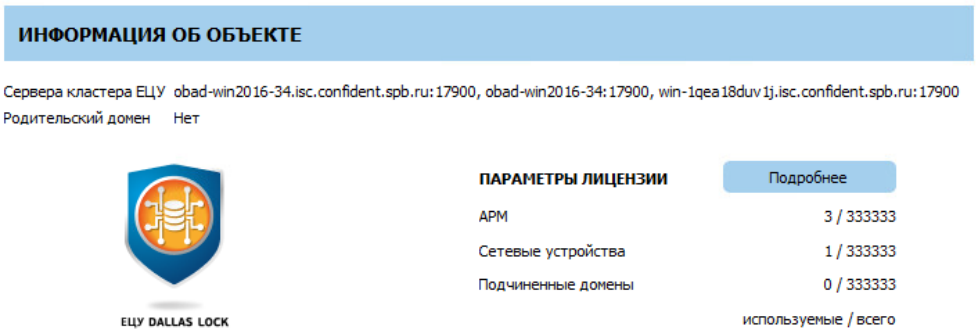

Рис. 53. Раздел «Информация об объекте»

2. «Инциденты безопасности» (рис. 54).

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 для непрочитанных инцидентах безопасности.

Рис. 54. Раздел «Инциденты безопасности»

Период времени можно изменить в верхней части информационной панели «Инциденты безопасности», использовав выпадающий список «За период» и выбрав период времени:

- день;
- неделю;
- месяц;
- год;
- период — при выборе данного пункта в появившемся окне (рис. 55) возможно задать необходимый отрезок времени;
- все время.

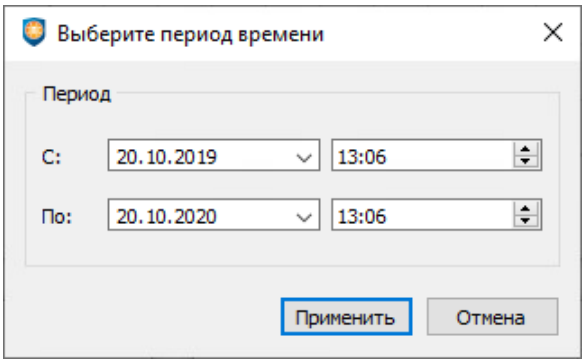

Рис. 55. Выбор периода времени

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

Под гистограммой расположены круговые диаграммы:

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

Описание настройки отображения информационной панели «Инциденты безопасности» приведено в разделе «Настройка инцидентов безопасности».

В нижней части данной информационной панели расположена таблица с сообщениями об инцидентах безопасности. Двойной клик по сообщению откроет сообщение об инциденте в отдельном окне, в таблице данное сообщение квитируется как прочитанное. Нажимая на кнопки «вверх» и «вниз» можно отмечать сообщения как прочитанные, просматривая предыдущие или следующие инциденты.

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.

5.2 Пользователи и группы ДБ

Вкладка «Пользователи и группы» на уровне ДБ позволяет управлять глобальными учетными записями и группами пользователей ДБ ЕЦУ (рис. 56).

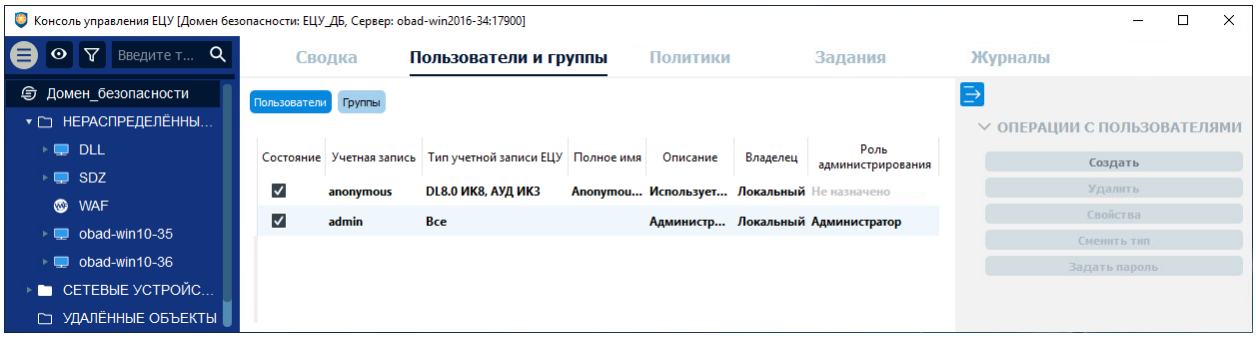

Рис. 56. Список учетных записей ДБ ЕЦУ

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», которое 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»).

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 ДБ, работа учетной записи отключается для всех вложенных групп, АРМ (модулей в составе АРМ), модулей без АРМ и иных объектов.

2. «Учетная запись», которое содержит имя учетной записи;
3. «Тип учетной записи ЕЦУ», которое содержит информацию о том, для модулей какого типа применяется данная учетная запись. Возможные значения:
   - Все — учетная запись применима для всех модулей (кроме модуля WAF);
   - DL8.0 — 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 Dallas Lock Linux (см. «МОДУЛЬ СЗИ НСД DALLAS LOCK LINUX»);
   - DL8.0 СЗИ ВИ — учетная запись применима для модуля СЗИ ВИ Dallas Lock (см. «МОДУЛЬ СЗИ ВИ DALLAS LOCK»);
   - АУД — 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», которое содержит полное имя учетной записи;
5. «Описание», которое содержит описание учетной записи;
6. «Владелец», которое указывает на каком уровне дерева ЕЦУ 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 выбору пункта «Свойства» на панели инструментов «Операции с пользователями».

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

После выполнения одного из этих действий открывается окно «Редактирование полей пользователя» (рис. 57).

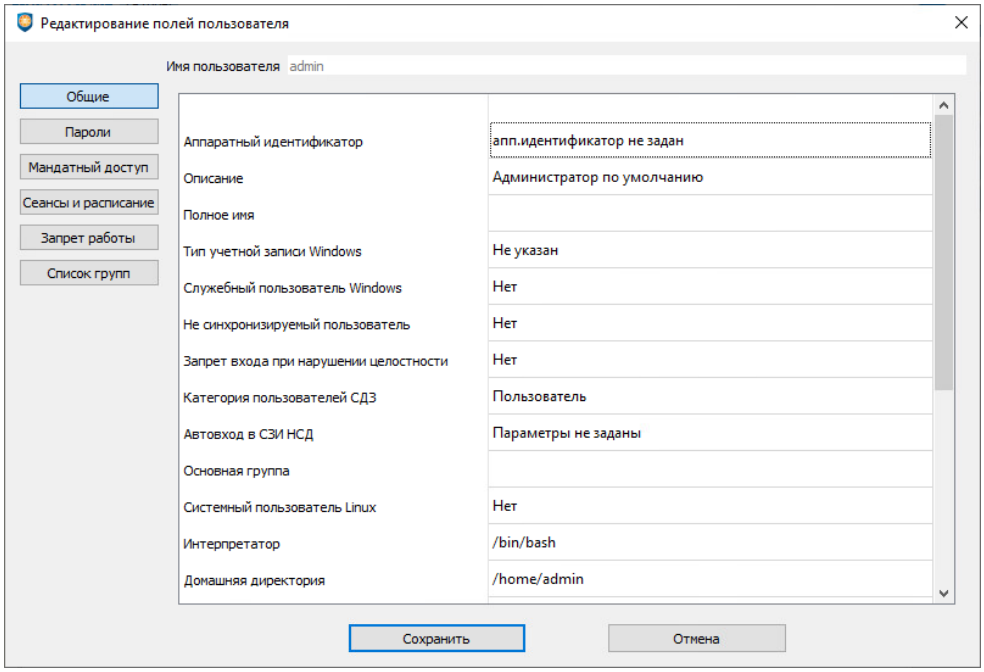

Рис. 57. Редактирование полей пользователя

На вкладке «Общие» предлагается заполнить учетные данные и параметры пользователей (таблица 1).

Таблица 1. Общие параметры пользователей

Заполняемые данные и параметры	Применение
поле «**Аппаратный идентификатор**»	ЕЦУ Dallas Lock; СЗИ Dallas Lock 8.0; СДЗ Dallas Lock; СЗИ Dallas Lock Linux; Dallas Lock СЗИ ВИ; Агент управления доступом
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; Агент управления доступом
заполнить «**Полное имя пользователя**». Вводить полное имя не обязательно. По умолчанию поле имеет пустое значение	ЕЦУ Dallas Lock; СЗИ Dallas Lock 8.0; Dallas Lock СЗИ ВИ; Агент управления доступом
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; Агент управления доступом
значение «Да» в поле «**Служебный пользователь Windows**» предоставляет данной учетной записи	СЗИ Dallas Lock 8.0; Агент управления доступом

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»	
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; Dallas Lock СЗИ ВИ; Агент управления доступом
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; Агент управления доступом
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
значение «Да» в поле «**Системный пользователь Linux**» указывает на то, что учетная запись пользователя является системной. По умолчанию поле имеет значение «Нет»	СЗИ Dallas Lock Linux
поле «**Интерпретатор**» указывает на интерпретатор командной строки. Обязательный атрибут учетной записи пользователя. По умолчанию имеет значение «/bin/sh»	СЗИ Dallas Lock Linux
в поле «**Домашняя директория**» указывается путь к домашней директории пользователя	СЗИ 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 Dallas Lock Linux
значение «Да» в поле «**Администратора СЗИ Dallas Lock Linux**» указывает на то, что пользователь является администратором СЗИ НСД Dallas Lock Linux. По умолчанию поле имеет значение «Нет»	СЗИ Dallas Lock Linux
в поле «**Домен для Linux**» указывается имя домена Active Directory. Атрибут обязателен для доменных учетных записей пользователей	СЗИ Dallas Lock Linux
указать «**Имя**» пользователя. Заполнять поле не обязательно	Dallas Lock СЗИ ВИ

указать «**Фамилия**» пользователя. Заполнять поле не обязательно	Dallas Lock СЗИ ВИ
указать «**E-mail**» пользователя. Заполнять поле не обязательно	Dallas Lock СЗИ ВИ
выбрать «**Тип учетной записи СЗИ ВИ**» для пользователей гипервизора. По умолчанию поле имеет значение «Пользователь VMware vSphere»	Dallas Lock СЗИ ВИ
значение «Да» в поле **«Администратор СЗИ ВИ»** указывает на: • возможность авторизации пользователя в ЦУ СЗИ ВИ; • назначение пользователя на роль «Администратор ВИ» в ЦУ СЗИ ВИ. По умолчанию поле имеет значение «Нет». **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».	Агент управления доступом
поле **«Разрешить вход в ОС»** по умолчанию имеет значение «Нет»	Агент управления доступом

На вкладке «Пароли» предлагается заполнить учетные данные и параметры пользователей, относящиеся к настройкам паролей (таблица 2).

Таблица 2. 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; Агент управления доступом
поле «**Запрет изменения пароля**». По умолчанию поле имеет значение «Нет»	СЗИ Dallas Lock 8.0; СДЗ Dallas Lock; Агент управления доступом
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; Агент управления доступом
поле «**Минимальный срок действия пароля (в днях)**» указывает на минимальный срок действия пароля в днях. Обязательное поле. Принимает значения от «1» до «180»[1]. Установка значения «Не используется» обозначает, что для	СЗИ Dallas Lock Linux

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

данной учетной записи пользователя ограничений на период ее неиспользования накладываться не будет. По умолчанию имеет значение «Не используется».	
поле «**Максимальный срок действия пароля (в днях)**» указывает на максимальный срок действия пароля в днях. Обязательное поле. Принимает значения от «1» до «180»[1]. 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 Dallas Lock Linux
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 Dallas Lock Linux
поле «**Дата последней смены пароля**». По умолчанию поле имеет значение «Не определено»	СЗИ 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 3).

Таблица 3. Мандатный доступ пользователей

Заполняемые данные и параметры	Применение
необходимо выбрать «**Уровень мандатного доступа»** (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»), под которым 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 4).

Таблица 4. 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 Dallas Lock Linux; Агент управления доступом
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»).	СЗИ Dallas Lock 8.0; СДЗ Dallas Lock

Примечание. «Расписание работы» пользователя может быть определено с дискретностью 30 минут.	
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 данной учетной записи пользователя ограничений на период ее неиспользования накладываться не будет. По умолчанию имеет значение «Не используется»	СЗИ Dallas Lock Linux
задать дату «**Истечение срока действия учетной записи**». По умолчанию поле имеет значение «Без ограничений». При установленном флаге становится активным поле «Дата». В поле «Дата» указывается дата, когда данная учетная запись будет заблокирована системой. В этом случае поле «Дата» обязательно для заполнения. При пустом флаге поле «Дата» неактивно, время действия учетной записи не ограничено	СЗИ 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 5).

Таблица 5. 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; Dallas Lock СЗИ ВИ; Агент управления доступом
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»	СДЗ Dallas Lock

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»).	
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» администратор имеет возможность включить пользователя в определенную группу. Также отображены названия групп, в которые включен пользователь (рис. 58).

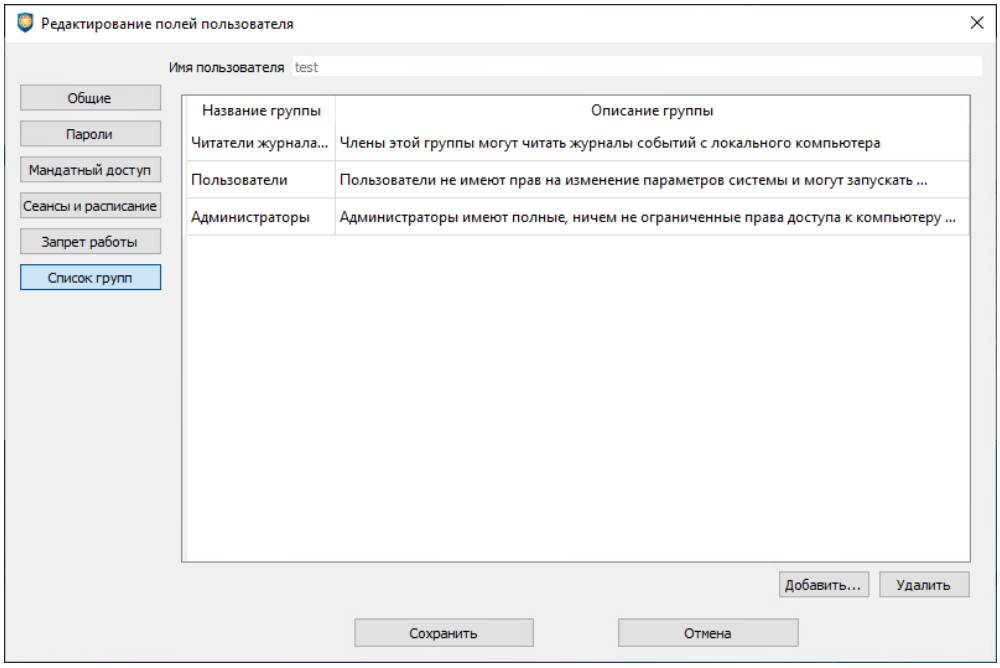

Рис. 58. Список групп пользователя

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», которое 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»).

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.

2. «Название группы», которое содержит имя группы пользователей;
3. «Тип», которое содержит информацию, о том для модулей какого типа применяется данная группа пользователей;
4. «Описание», которое содержит описание группы пользователей;
5. «Владелец», которое указывает на каком уровне дерева ЕЦУ 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;
- редактирование описания групп;
- 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. 59).

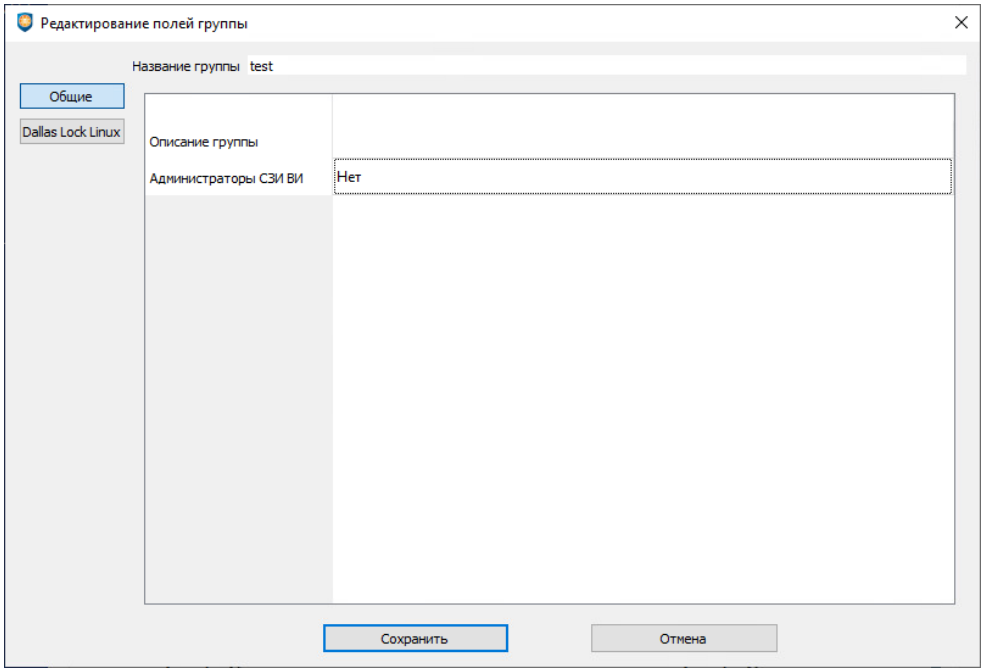

Рис. 59. Редактирование полей групп

На вкладке «Общие» предлагается оставить комментарий в поле «Описание группы» и назначить пользователей, входящих в группу, на роль «Администратор ВИ» в ЦУ СЗИ ВИ в поле «Администраторы 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 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. глобальных пользователей, созданных средствами консоли ЕЦУ;
2. доменных пользователей, созданных 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 кнопку «Создать» или выбрать соответствующую из контекстного меню, нажав правую кнопку мыши.
4. На экране появится окно создания пользователя (рис. 60).

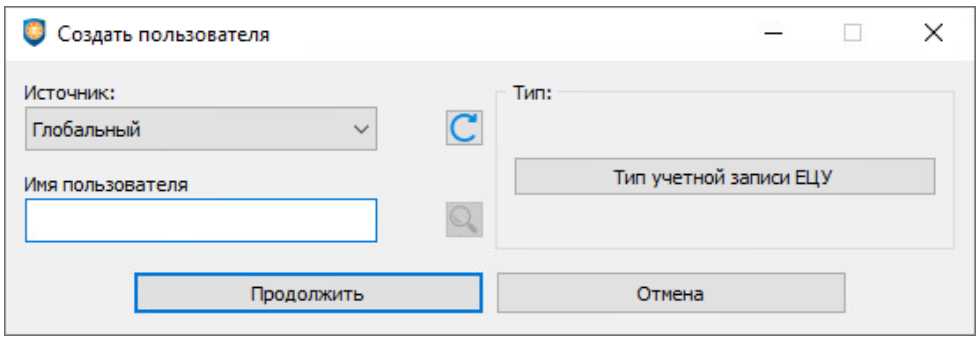

Рис. 60. Создание пользователя

5. В поле источник необходимо выбрать «Глобальный».
6. В поле «Имя пользователя» необходимо 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.

5.2.4 Назначение аппаратной идентификации

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

Примечание. Для корректной работы аппаратных идентификаторов eToken и JaCarta Pro необходимо использовать драйверы SafeNet.

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. 61).

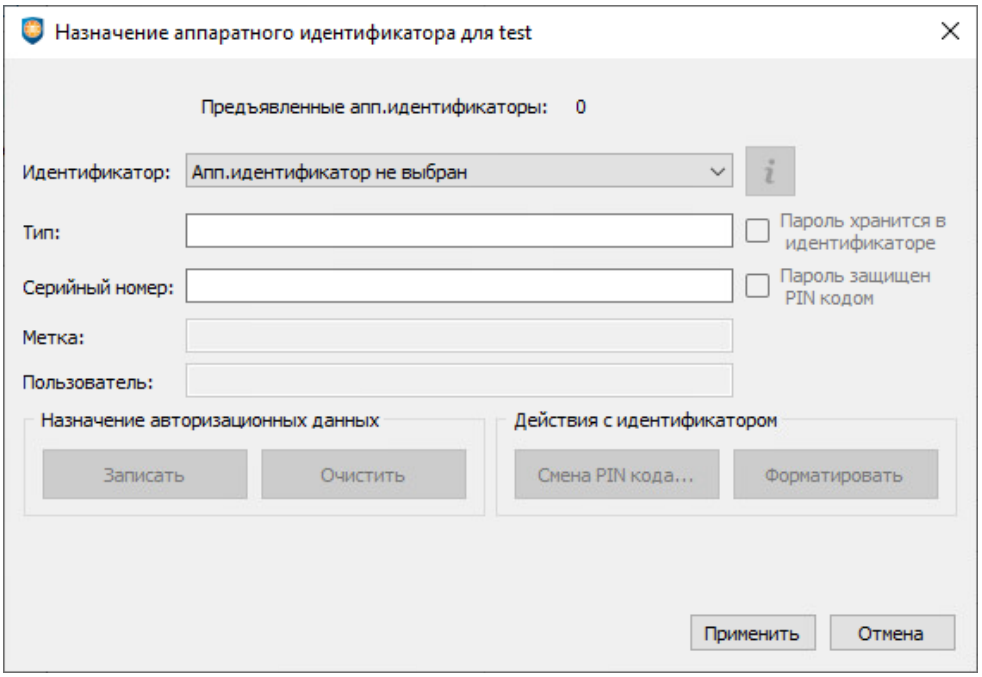

Рис. 61. Окно назначения аппаратного идентификатора

5. Необходимо 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. Дополнительная кнопка позволяет открыть окно с информацией о параметрах выбранного идентификатора (рис. 62).

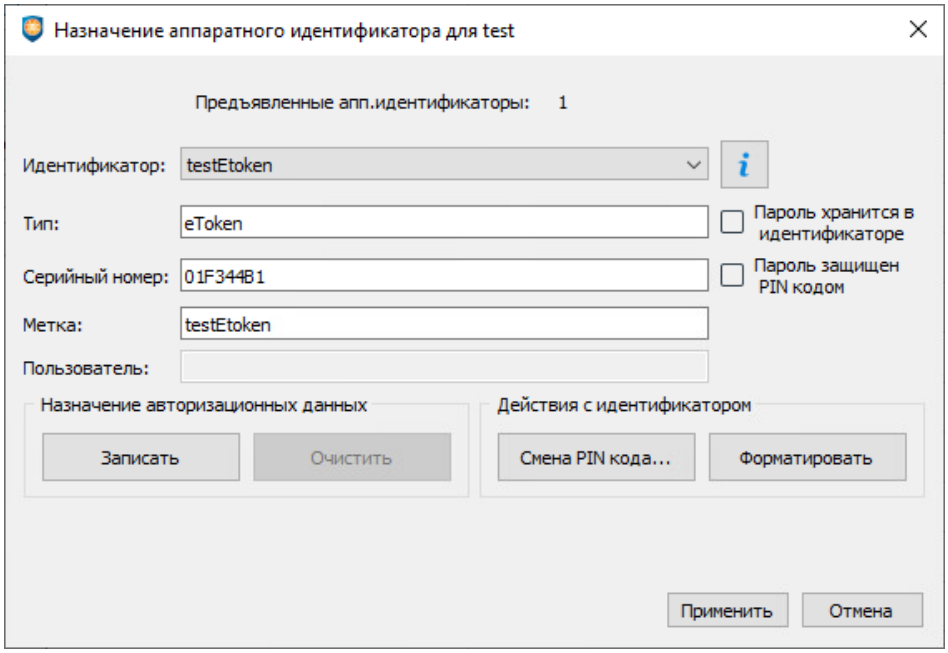

Рис. 62. Параметры назначенного идентификатора

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

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

5.2.5 Удаление пользователей ДБ

Внимание! Следует внимательно относится 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 органичен 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.

5.2.6 Назначение пароля

Для назначения пароля пользователю необходимо выделить его имя в списке и нажать кнопку «Задать пароль». Появится окно, в котором требуется ввести новый пароль и подтвердить его (рис. 63).

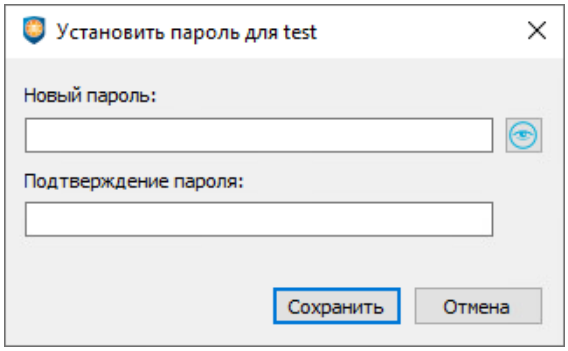

Рис. 63. Форма ввода пароля

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»).

Дополнительная кнопка 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 не противоречил 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, образуют 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 учётных записей в ЕЦУ, установленном в ОС семейства Linux, необходимо на DNS-серверах, к которым обращается АРМ с ЕЦУ, 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 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 доменных учётных записей Active Directory необходимо, чтобы время сервера ЕЦУ было синхронизировано с временем контроллера домена Active Directory.

Для регистрации в Домене безопасности ЕЦУ доменных пользователей в качестве глобальных, необходимо выполнить следующее.

1. Убедиться, что Домен безопасности ЕЦУ 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. 64).

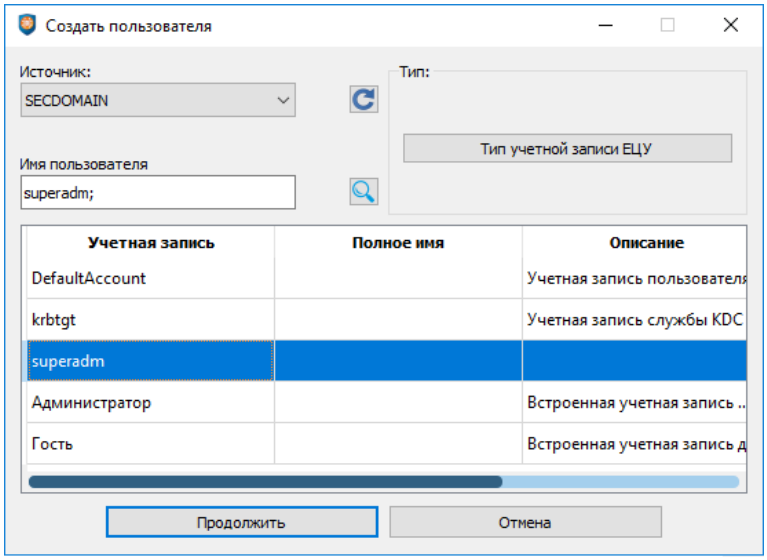

Рис. 64. Заполнение учетной записи пользователя

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. 65).

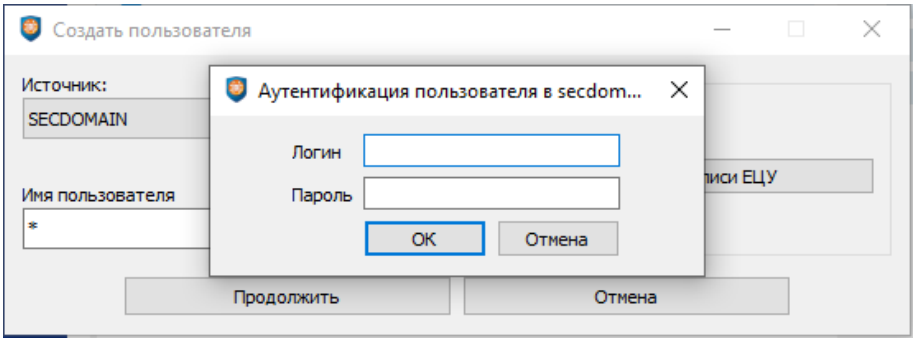

Рис. 65. Авторизационные данные администратора домена AD

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, 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.

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 доменными пользователями можно проводить любые операции по реализации политик безопасности, однако нельзя менять пароль средствами ЕЦУ. 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 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. 66).

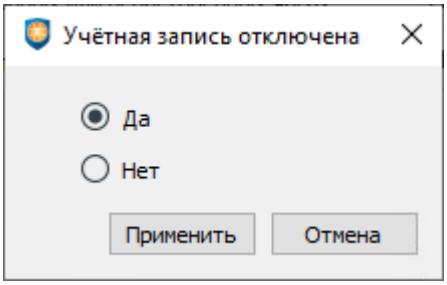

Рис. 66. Учетная запись отключена

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. 67).

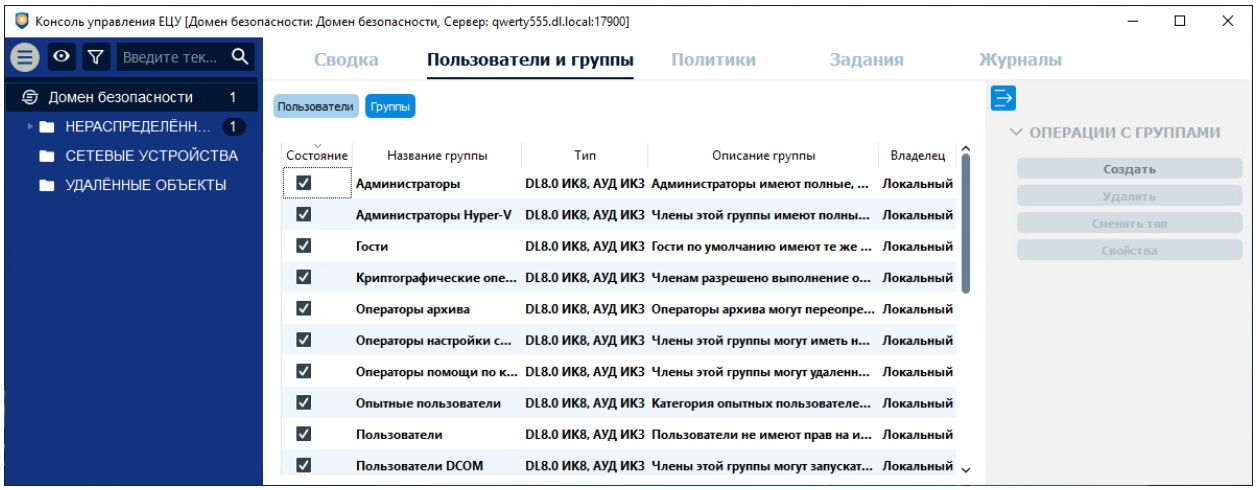

Рис. 67. Группы пользователей

Вновь созданные с помощью ЕЦУ глобальные группы автоматически создадутся и в подчиненных модулях после синхронизации. Удаленные глобальные группы удалятся 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. 68).

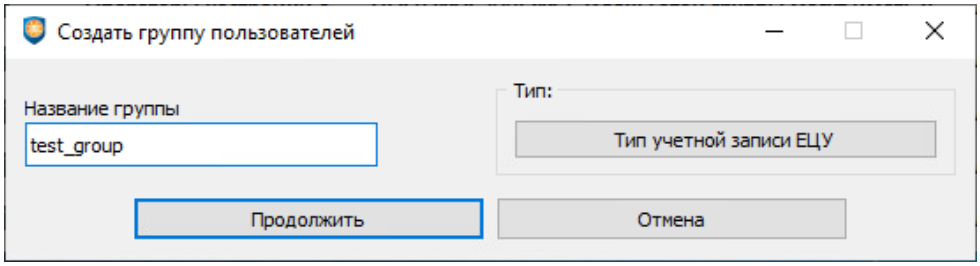

Рис. 68. Создание глобальной группы

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.

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. 69).

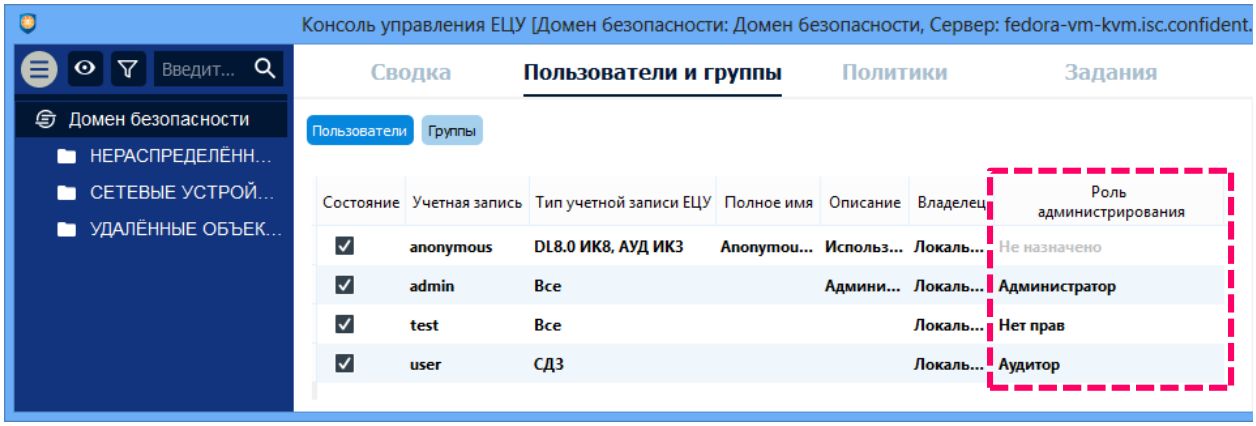

Рис. 69. Роль администрирования

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

Ролевая модель пользователей в ЕЦУ подразумевает наличие двух типов ролей: серверной и доменной.

Особенность серверной роли заключается в том, что пользователь, которому назначена серверная роль, может пользоваться привилегиями как на управление кластером серверов ЕЦУ, так и на управление ДБ. Серверная роль назначается только на уровне ДБ в дереве. Доменная же роль наделяется привилегиями на управление только ДБ и может быть назначена как на уровне группы ДБ, так и на уровне АРМ.

Примечание. Серверную роль можно назначить только на уровне текущего ДБ. Роль не может быть назначения для зарегистрированной учетной записи по маске.

Для удобства на основе групп привилегий в ЕЦУ сформированы следующие роли:

- «Администратор» — максимальные привилегии на управление доменом безопасности или его частью, в зависимости от уровня назначения роли;
- «Аудитор» обладает набором привилегии на просмотр информации о домене безопасности или его части, в зависимости от уровня назначения роли:
    - 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».

Для каждого глобального и доменного пользователя имеется назначение на роль. 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» глобальной или доменной учетной записи пользователя ей назначена 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.
- если на подчиненных узлах 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 относится 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. 70).

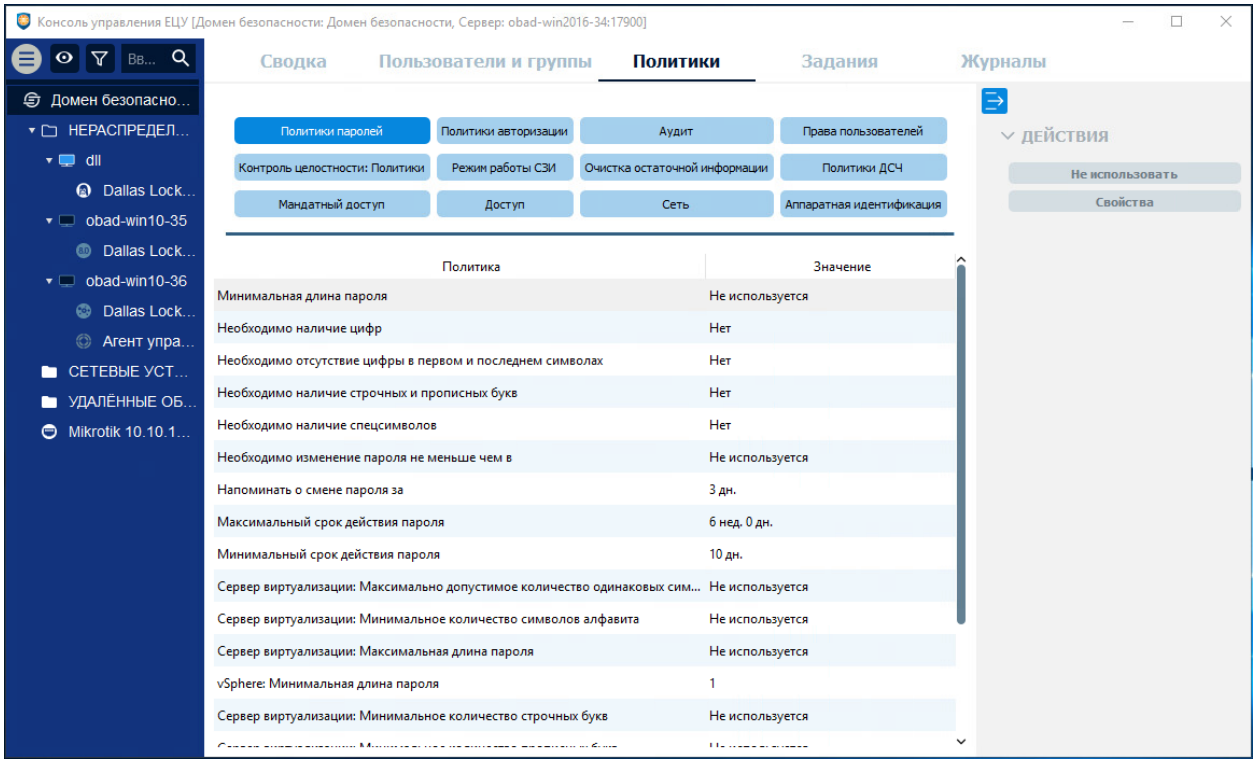

Рис. 70. Вкладка Политики ДБ

Для открытия редактора политики нужно дважды щелкнуть левой кнопкой мыши по изменяемой политике или 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 6. Парольные политики

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 Dallas Lock Linux;
  - Dallas Lock СЗИ ВИ;
  - Агент управления доступом.

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 Dallas Lock Linux;
  - Агент управления доступом.

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;
  - Агент управления доступом.

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 Dallas Lock Linux;
- Агент управления доступом.

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 Dallas Lock Linux;
  - Агент управления доступом.

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;
- Агент управления доступом.

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;
  - Dallas Lock СЗИ ВИ;
  - Агент управления доступом.

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 «42 дн.».

Политика применяется на:

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

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.

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

Политика применяется на:

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

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 Dallas Lock СЗИ 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 Dallas Lock СЗИ 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 Dallas Lock СЗИ 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 Dallas Lock СЗИ 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 Dallas Lock СЗИ 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 Dallas Lock СЗИ 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 Dallas Lock СЗИ 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 Dallas Lock СЗИ 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 Dallas Lock СЗИ 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 Dallas Lock СЗИ ВИ.

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 7. Политики авторизации

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-K/C;
  • СЗИ Dallas Lock Linux;
  • СДЗ Dallas Lock;
  • Dallas Lock СЗИ ВИ;
  • Агент управления доступом.

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-K/C;
  • СДЗ Dallas Lock;
  • Dallas Lock СЗИ ВИ;
  • Агент управления доступом.

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-K/C; • Агент управления доступом.
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 Агента управления доступом (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-K/C;
- СДЗ Dallas Lock;
- Агент управления доступом.

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-K/C;
- СДЗ Dallas Lock;
- Агент управления доступом.

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-K/C;
- Агент управления доступом.

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-K/C;
- Агент управления доступом.

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 Dallas Lock Linux и ЕЦУ Dallas Lock.

Политика применяется на модулях:

- СЗИ Dallas Lock 8.0-K/C;
- СЗИ Dallas Lock Linux;
- Агент управления доступом.

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-К/С; • Агент управления доступом.
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-К/С.
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 Dallas Lock СЗИ 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 Dallas Lock СЗИ 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 Dallas Lock СЗИ ВИ.
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-К/С.
Заблокировать выгрузку журналов 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 Dallas Lock СЗИ ВИ.

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 Dallas Lock Linux, пока не зарегистрированные в СЗИ Dallas Lock Linux, будут регистрироваться в нем по мере прохождения процесса авторизации в СЗИ Dallas Lock Linux. Политика применяется на модулях СЗИ Dallas Lock Linux.
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-К/С; • Агент управления доступом.
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 Dallas Lock СЗИ 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 Dallas Lock СЗИ ВИ.
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.
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 Dallas Lock СЗИ 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 Dallas Lock СЗИ ВИ.

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.
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 Dallas Lock СЗИ ВИ.
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 Dallas Lock Linux.
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.
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-К/С.
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-К/С.
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 Dallas Lock СЗИ 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 Dallas Lock СЗИ ВИ.

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-К/С. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Ввести в домен Active Directory
Политика позволяет ввести наименование домена, для которого настроено взаимодействие с модулями СЗИ Dallas Lock Linux. По умолчанию значение данной политики: «Не используется». Политика применяется на модулях СЗИ Dallas Lock Linux.
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 Dallas Lock СЗИ 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 Dallas Lock СЗИ ВИ.
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.
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 Dallas Lock СЗИ ВИ.
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.

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 8. Политики аудита

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; • Агент управления доступом.
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; • Агент управления доступом.
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-K/C; • СЗИ Dallas Lock Linux; • Агент управления доступом.
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-K/C; • СЗИ Dallas Lock Linux; • Агент управления доступом.
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 Dallas Lock Linux;
- Агент управления доступом.

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 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;
- Агент управления доступом.

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-К/С;
- Агент управления доступом.

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;
- Агент управления доступом.

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;
- Агент управления доступом.

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; • Агент управления доступом.
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-К/С; • Агент управления доступом.
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; • Агент управления доступом.
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; • Агент управления доступом.
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-К/С; • Агент управления доступом.
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;
- Агент управления доступом.

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 Dallas Lock СЗИ 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 состоянием ВМ виртуальной инфраструктуры Hyper-V.

Политика применяется на модулях Dallas Lock СЗИ ВИ.

Срок хранения журналов в месяцах

Данная политика позволяет управлять сроком хранения журналов на модулях. По истечению заданного в политике срока, формируется архив, и журналы начинаю 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 Dallas Lock Linux.

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 Dallas Lock Linux.

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.

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 Dallas Lock СЗИ 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 Dallas Lock СЗИ 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 Dallas Lock СЗИ ВИ.
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 Агент управления доступом.
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 Dallas Lock СЗИ ВИ.
Журнал агента гипервизора
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию событий службы vpxa в журнале гипервизора ESXi. Политика применяется на модулях Dallas Lock СЗИ 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 Dallas Lock СЗИ ВИ.
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-К/С.
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 Dallas Lock СЗИ 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 Dallas Lock СЗИ ВИ.

VMM: Блокировка SC VMM
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Включение данной политики (значение «Да») позволяет заблокировать определенный операции SC VMM, независимо от назначенных прав пользователей. Политика применяется на модулях Dallas Lock СЗИ 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 Dallas Lock СЗИ ВИ.
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 Dallas Lock Linux.
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 Dallas Lock СЗИ 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 Dallas Lock СЗИ ВИ.
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 от 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.
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 Dallas Lock СЗИ ВИ.

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.

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 9. 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; • Агент управления доступом.
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; • Агент управления доступом.
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; • Агент управления доступом.
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; • Агент управления доступом.
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; • Агент управления доступом.
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; • Агент управления доступом.
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; • Агент управления доступом.

Учетные записи: Управление
Если в значении данной политики стоит учетная запись или группа, то она обладает полномочиями по создания, удаления и изменения 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 «Политики: Контроль целостности» настраиваются параметры проверки целостности отдельно для объектов ФС, отдельно для объектов программно-аппаратной среды и отдельно для реестра. По умолчанию проверка целостности установлена только при загрузке модуля.

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

Таблица 10. Политики контроля целостности

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; • Агент управления доступом.
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 Dallas Lock Linux; • Агент управления доступом.
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; • Агент управления доступом.
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; • Агент управления доступом.
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;
- Агент управления доступом.

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;
- Агент управления доступом.

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-К/С;
- Агент управления доступом.

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-К/С;
- Агент управления доступом.

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-К/С;
- Агент управления доступом.

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;
- Агент управления доступом.

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;
- Агент управления доступом.

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; • Агент управления доступом.
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; • Агент управления доступом.
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; • Агент управления доступом.
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; • Агент управления доступом.
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; • Агент управления доступом.
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; • Агент управления доступом.
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; • Агент управления доступом.

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-К/С; • Агент управления доступом.
Контроль целостности прогр. апп. среды: Службы
Данная политика управляет контролем установки или удаления служб ОС. По умолчанию данная политика выключена. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • Агент управления доступом.
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-К/С; • Агент управления доступом.
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-К/С; • Агент управления доступом.
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-К/С; • Агент управления доступом.
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; • Агент управления доступом.
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: «Разрешит». Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • Агент управления доступом.
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 Dallas Lock Linux.

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 модуля Агент управления доступом.

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

Таблица 11. 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.
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.
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 Агент управления доступом.
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.

5.4.7 Настройка политик очистки остаточной информации

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

Реальное содержимое файла остается на запоминающем устройстве, и его можно достаточно легко просмотреть до тех пор, пока ОС заново не использует это пространство для хранения новых данных. Данная остаточная информация может легко 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 12. 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; • Агент управления доступом.
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; • Dallas Lock СЗИ ВИ; • Агент управления доступом.
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; • Агент управления доступом.
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; • Агент управления доступом.
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; • Агент управления доступом.

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 13. 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-С 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 14. 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-С.

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 15. 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.

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

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 будет проверяться все равно, 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 на модули, с ожидаемым результатом выполнения со стороны модуля называются в ЕЦУ заданиями.

Управление заданиями осуществляется на вкладке «Задания» (рис. 71).

Рис. 71. Вкладка «Задания»

Список заданий на уровне ДБ представляет собой таблицу с полями:

1. «Создано», которое 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. «Тип», которое содержит название задания;

3. «Автор», которое содержит имя учетной записи пользователя ЕЦУ, создавшего задание;
4. «АРМ», которое содержит имя ПК, для выполнения на котором создано данное задание;
5. «Модуль», которое содержит информацию о типе модуле, для выполнения на котором создано данное задание;
6. «Статус», которое 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. 72);

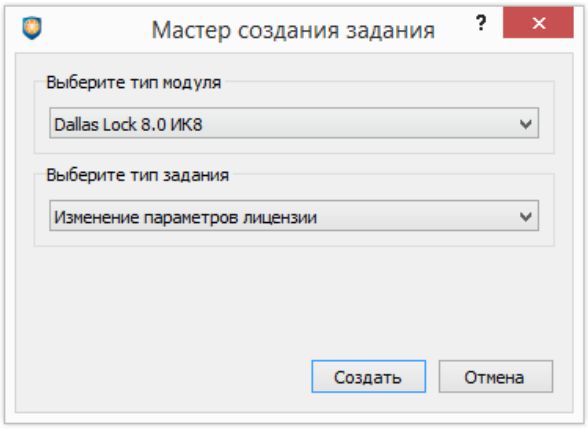

Рис. 72. Мастер создания задания

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.

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. 73), происходит обновление задания, при этом старое задание удаляется и остается только более новое.

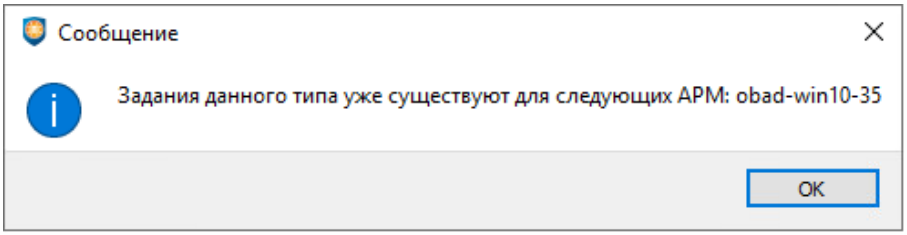

Рис. 73. Предупреждение о создании дубликата задания

5.5.2 Результат выполнения задания

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

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

Для сохранения отчета о результате в файл необходимо нажать кнопку «Сохранить» и выбрать путь сохранения файла.

5.5.3 Удаление заданий

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

Также на панели инструменты доступны команды для удаления нескольких заданий:

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

5.6 Журнал ДБ

На вкладке «Журналы» на уровне Домена безопасности в категории «Журнал ЕЦУ» отображаются регистрируемые события, связанные непосредственно с работой текущего ДБ ЕЦУ (рис. 74).

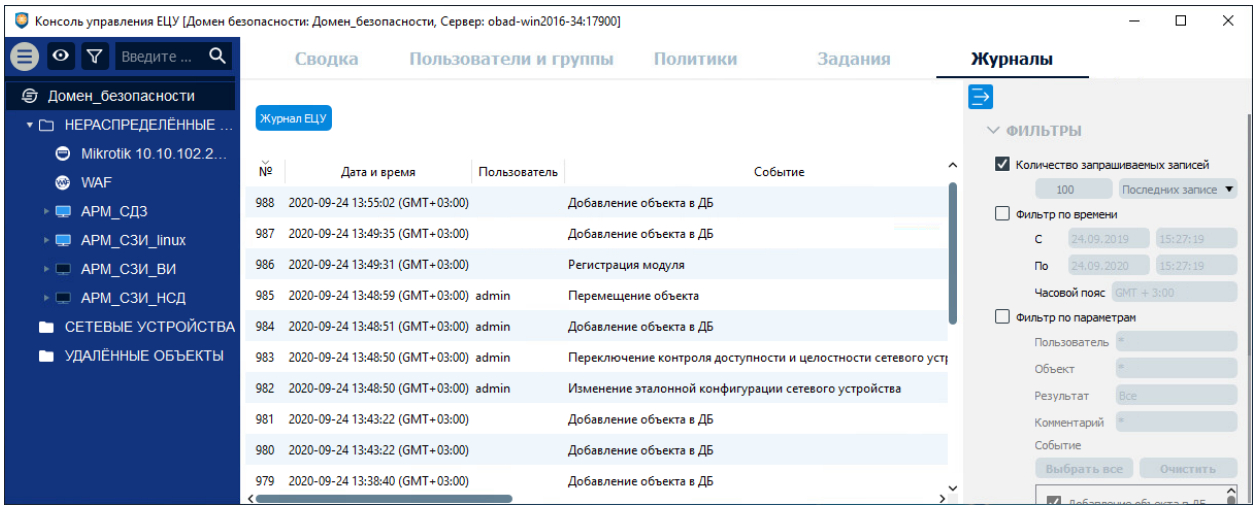

Рис. 74. Вкладка «Журналы» Домена безопасности

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 12 или выше.

Справа расположены панель инструментов «Фильтры» и панель инструментов «Действия» (рис. 75).

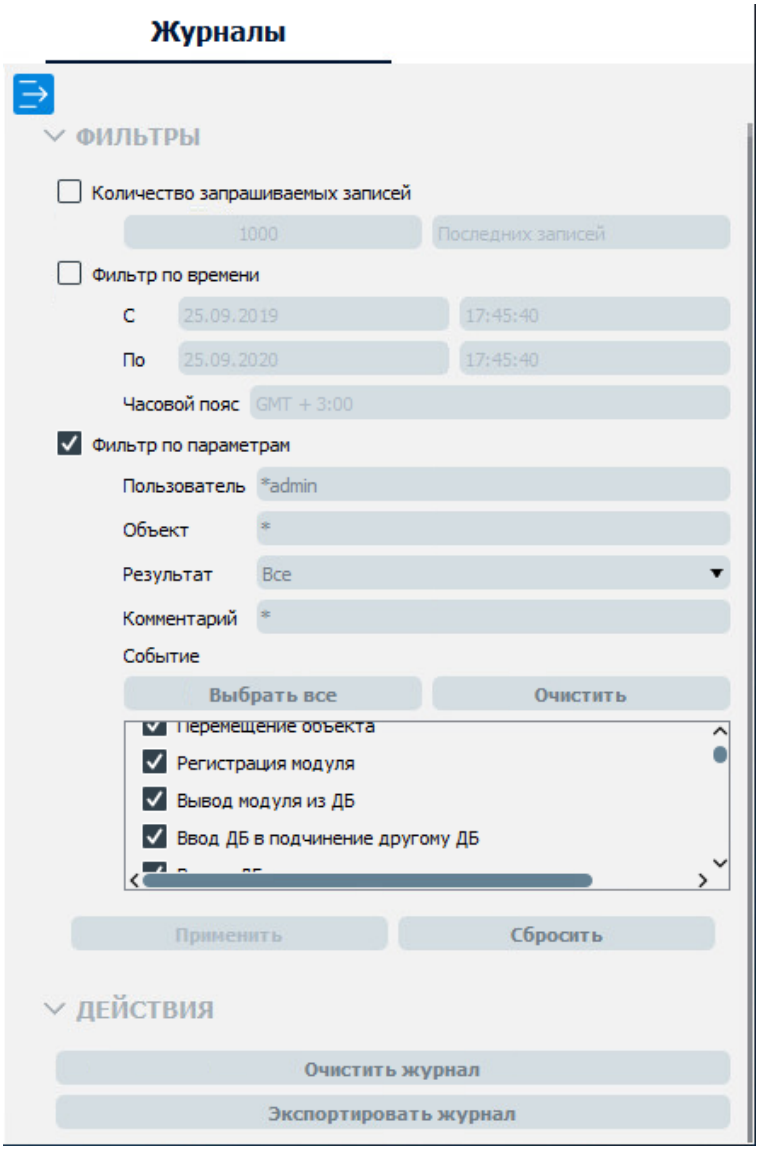

Рис. 75. Параметры фильтрации журналов

Фильтрация журналов осуществляется:

- по количеству запрашиваемых записей;
- по времени;
- по параметрам:
  - пользователь;
  - объект;
  - результат (успешный/с ошибками);
  - комментарий;
  - событие.

Сброс примененных фильтров осуществляется по команде «Сбросить».

Отфильтрованные записи журнала можно сохранить в выбранную папку в выбранном типе файла (TXT, CSV), воспользовавшись командой «Экспортировать журнал» на панели инструментов «Действия».

Для очистки журнала ЕЦУ необходимо выбрать команду «Очистить журнал».

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 он всегда помещается в группу «Сетевые устройства».

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

В дальнейшем администратор ЕЦУ может перенести из базовой группы «Нераспределенные объекты» новое АРМ, модуль без АРМ или сетевое устройство в любую другую группу, а также любую подгруппу в качестве подгруппы в другую группу. Для этого можно перетащить значок нужного объекта кнопкой мыши в поле другого значка («Drag-and-drop»).

6.2 Настройка групп

Чтобы создать группу, необходимо выбрать элемент дерева ДБ для добавления в него новой группы и далее нажать кнопку «Создать группу» на панели инструментов «Действия» или воспользоваться контекстным меню в дереве ДБ. При создании группы потребуется ввести ее наименование, которое 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. 76).

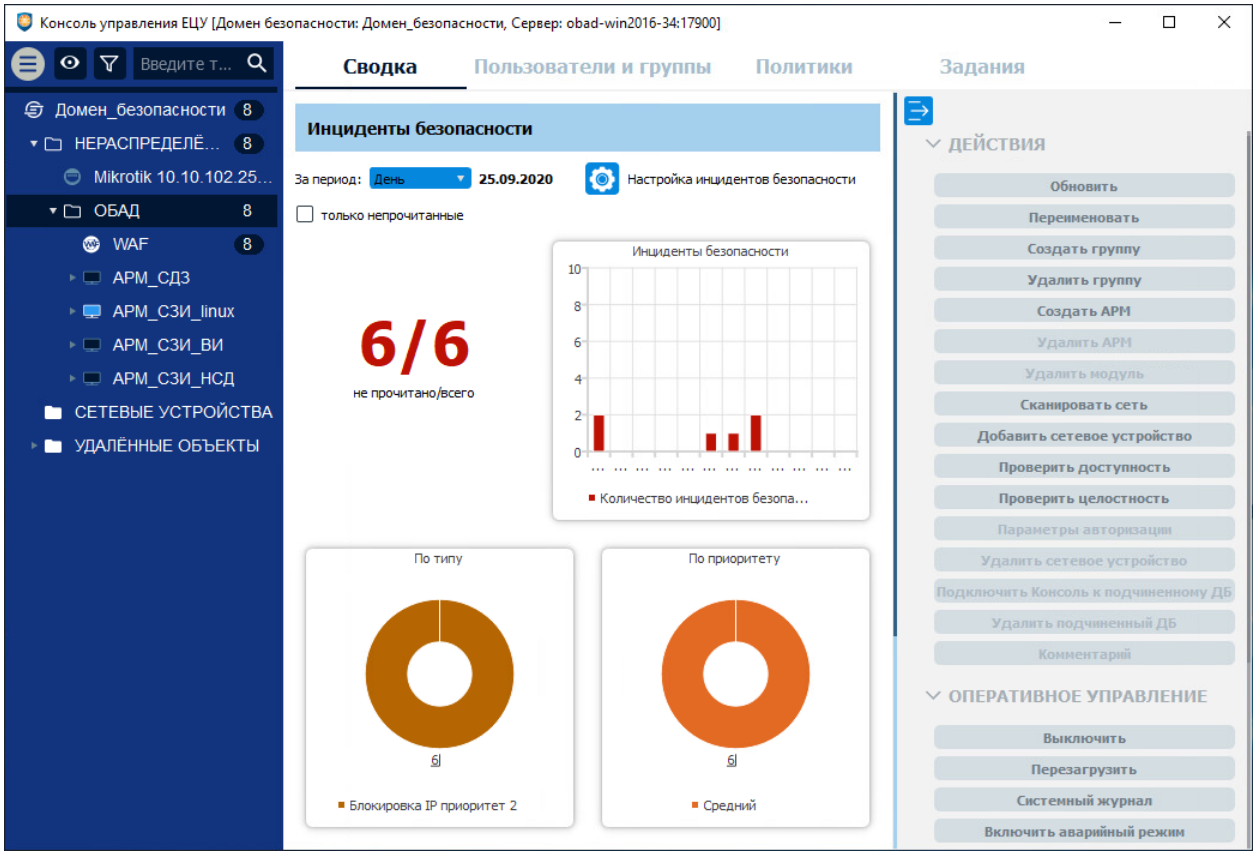

Рис. 76. Вкладка «Сводка» для группы ДБ

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.

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» вкладки содержит список учетных записей пользователей группы ДБ (рис. 77).

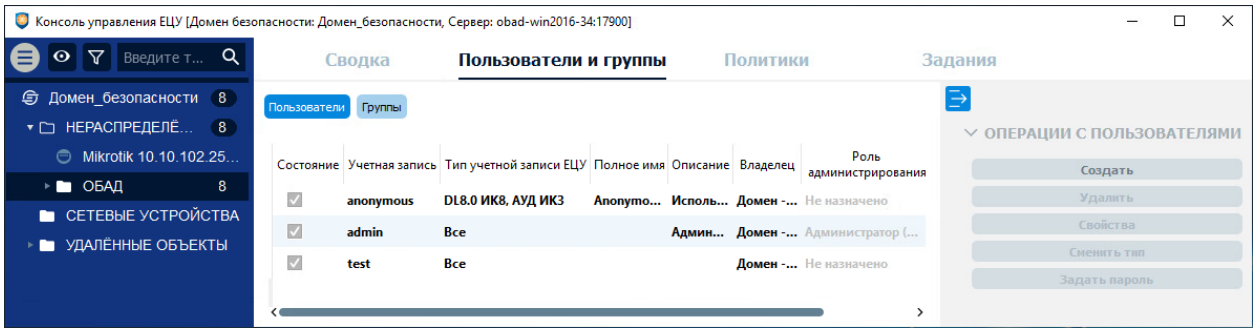

Рис. 77. Список учетных записей пользователей группы ДБ

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;
- смена пароля учетной записи пользователя (см. «Назначение пароля»).

Группы пользователей группы ДБ

Дополнительным инструментом управления правами учетных записей группы ДБ являются «Группы». Этот инструмент функционирует аналогично «Локальным группам» в ОС семейства Windows и доступен в категории «Группы» на вкладке «Пользователи и группы» (рис. 78).

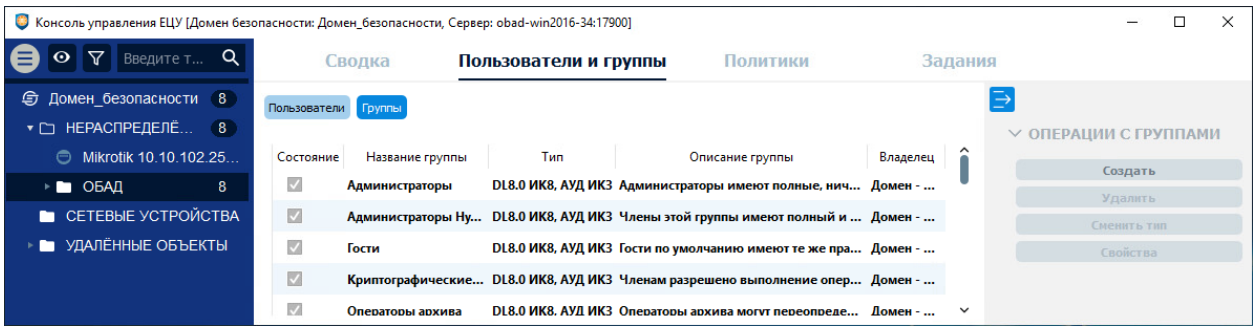

Рис. 78. Список групп пользователей группы ДБ

Управление группами пользователей на уровне группы ДБ производится аналогично управлению группами пользователей для ДБ (см. «Параметры групп»).

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» доступно:

- 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.

6.2.3 Политики для группы ДБ

Вкладка «Политики» на уровне группы позволяет редактировать параметры безопасности на уровне группы (подгруппы) (рис. 79).

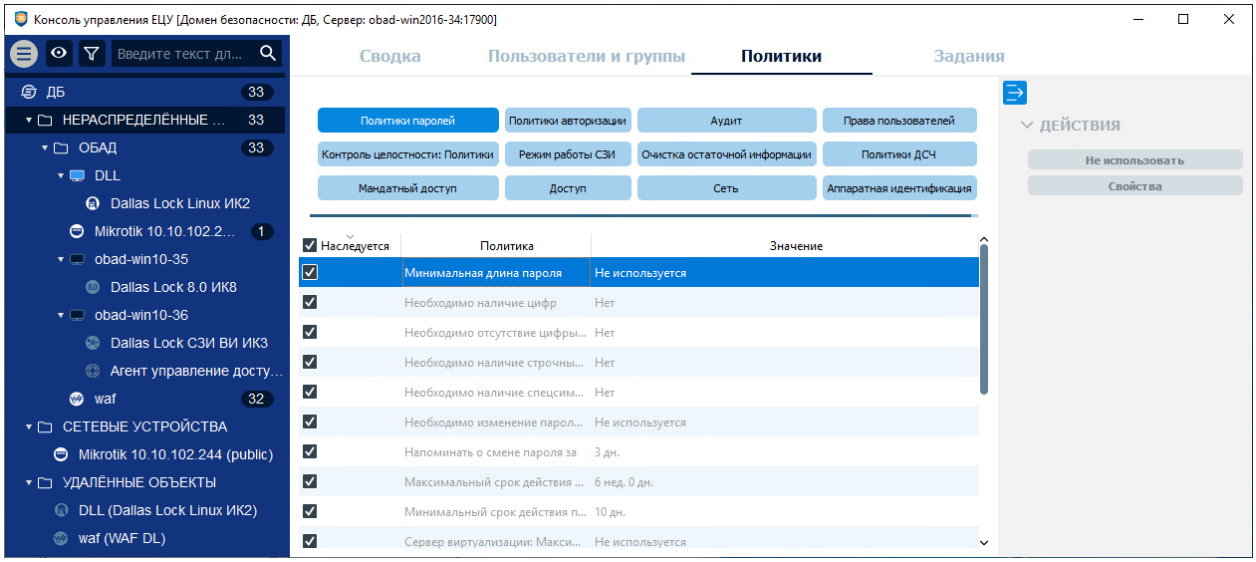

Рис. 79. Политики для групп Домена безопасности

Настройка политик для группы 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. 80);

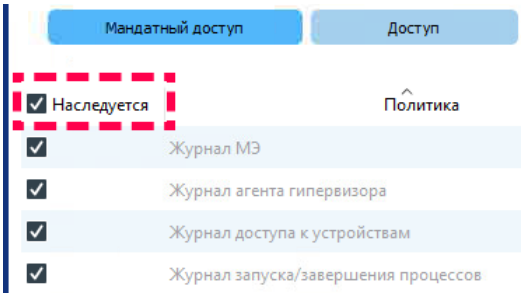

Рис. 80. Включение наследования политик объекта

2. если снять флаг из поля «Наследуется», то все параметры одновременно станут обозначены как индивидуально настроенные (рис. 81);

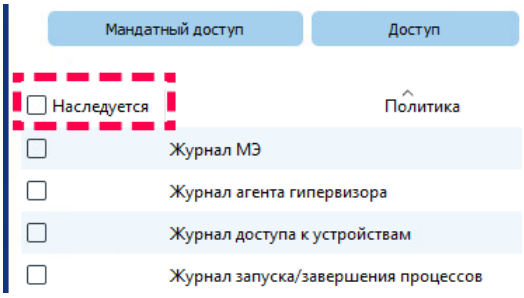

Рис. 81. Выключение наследования политик объекта

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. 82).

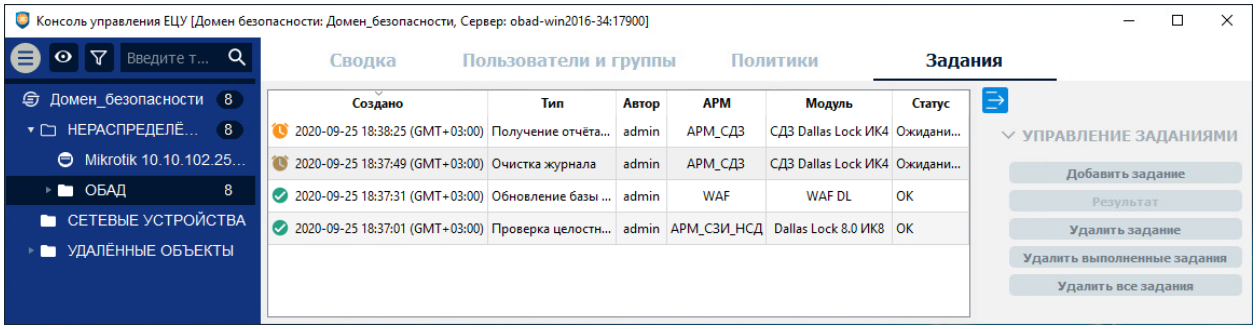

Рис. 82. Задания для групп Домена безопасности

Управление заданиями на уровне группы ДБ производится аналогично управлению заданиями для ДБ (см. «Задания ДБ»).

7 АРМ ДОМЕНА БЕЗОПАСНОСТИ ЕЦУ

В ЕЦУ АРМ используется как способ представления совокупности нескольких модулей в качестве единой машины (рис. 83).

Рис. 83. АРМ в дереве ЕЦУ

АРМ может включать в себя модули следующих типов:

- СЗИ НСД Dallas Lock 8.0-К/С;
- СЗИ НСД Dallas Lock Linux;
- СДЗ Dallas Lock;
- Агент управления доступом;
- Dallas Lock СЗИ ВИ.

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 АРМ» 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. 84).

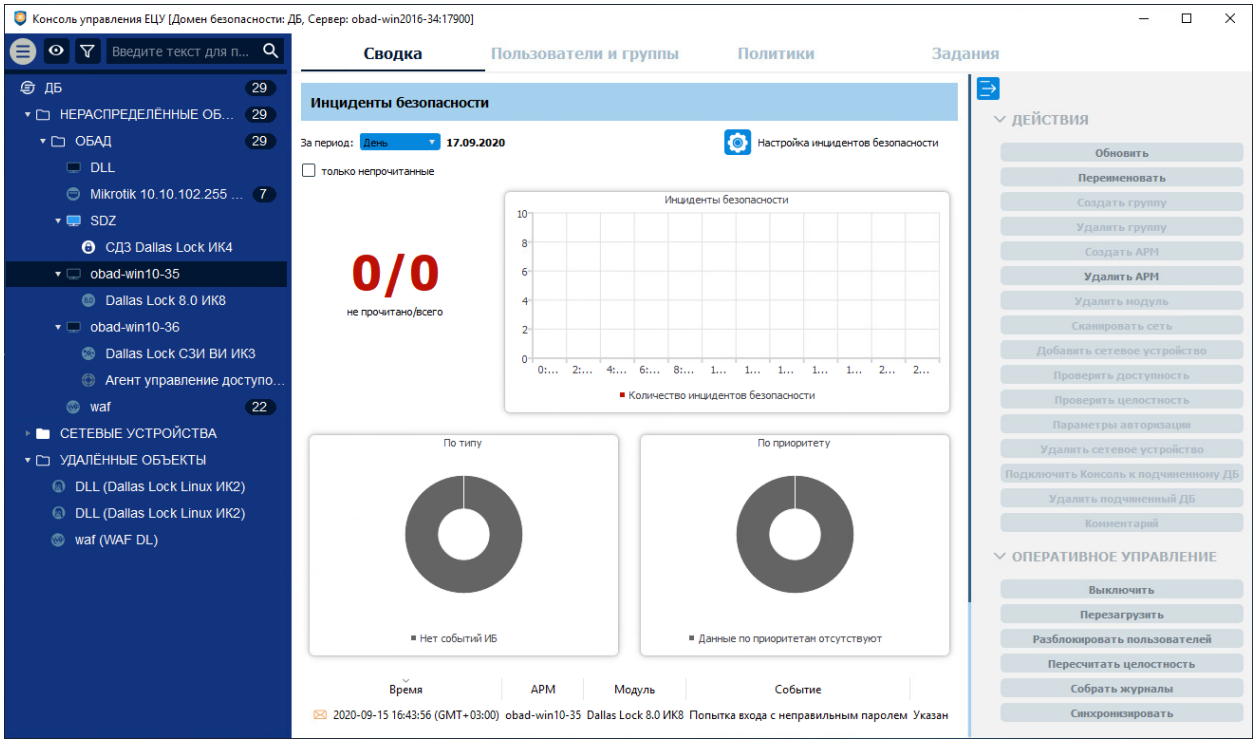

Рис. 84. Вкладка «Сводка» АРМ

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 включение.

Набор команд оперативного управления для каждого АРМ зависит от входящих в него модулей.

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. 85).

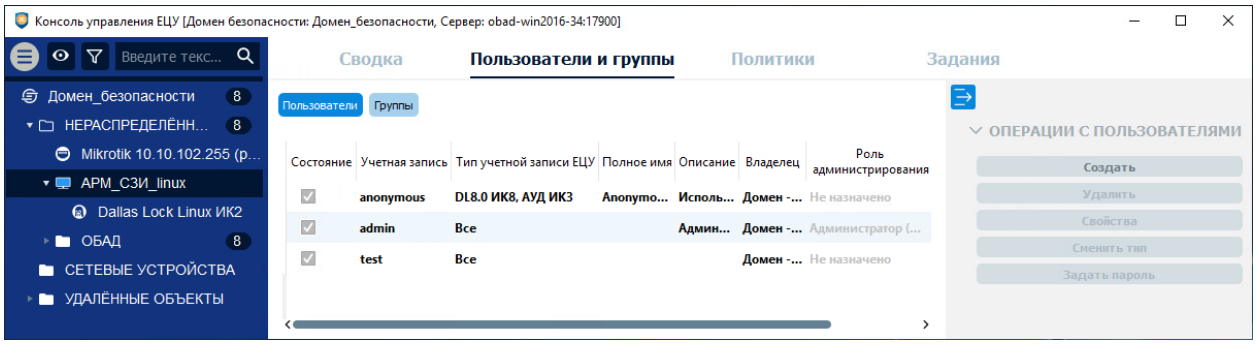

Рис. 85. Вкладка «Пользователи и группы» АРМ

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. 86).

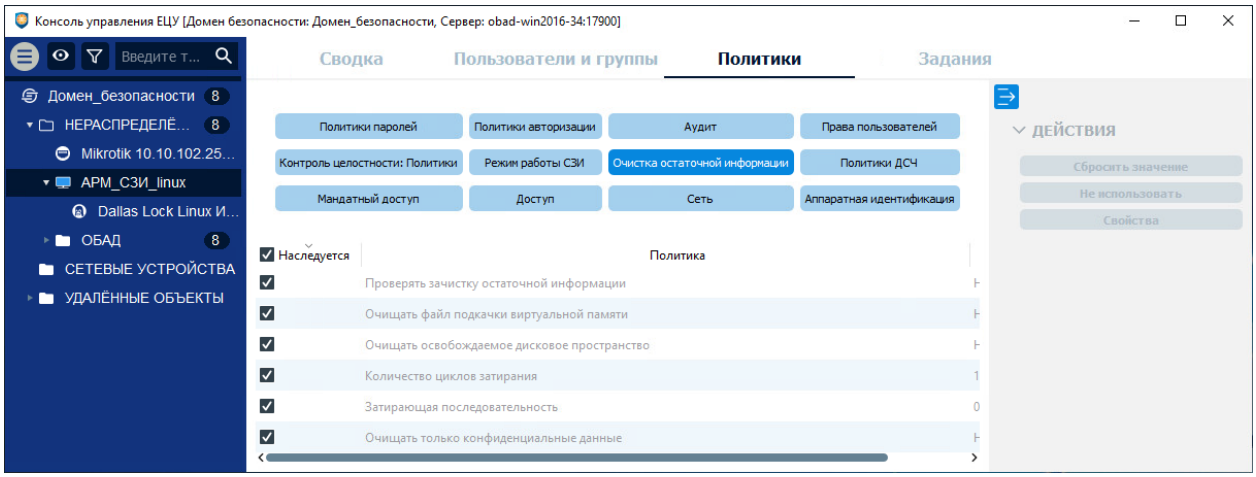

Рис. 86. Вкладка «Политики» АРМ

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. 87).

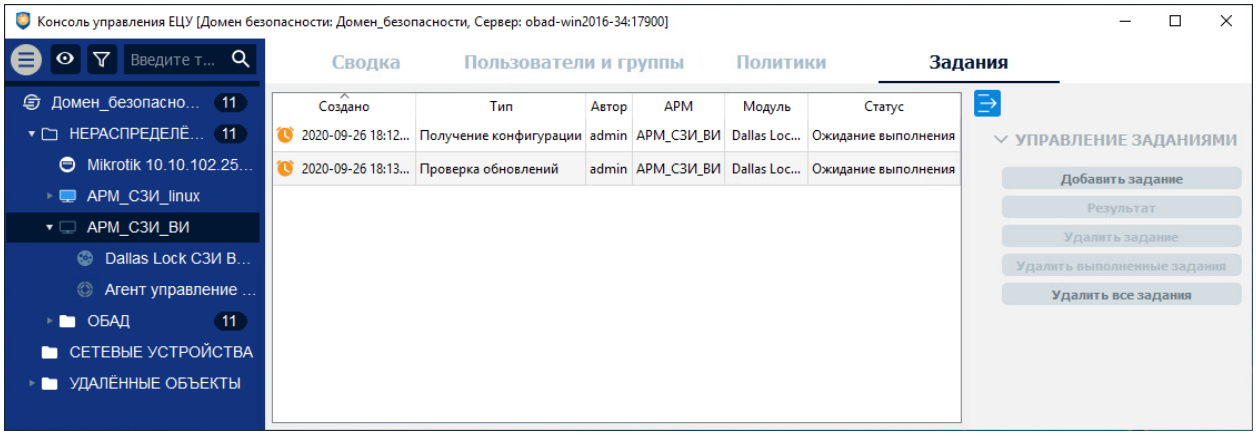

Рис. 87. Вкладка «Задания» АРМ

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 и СЗИ НСД Dallas Lock Linux), 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. 88).

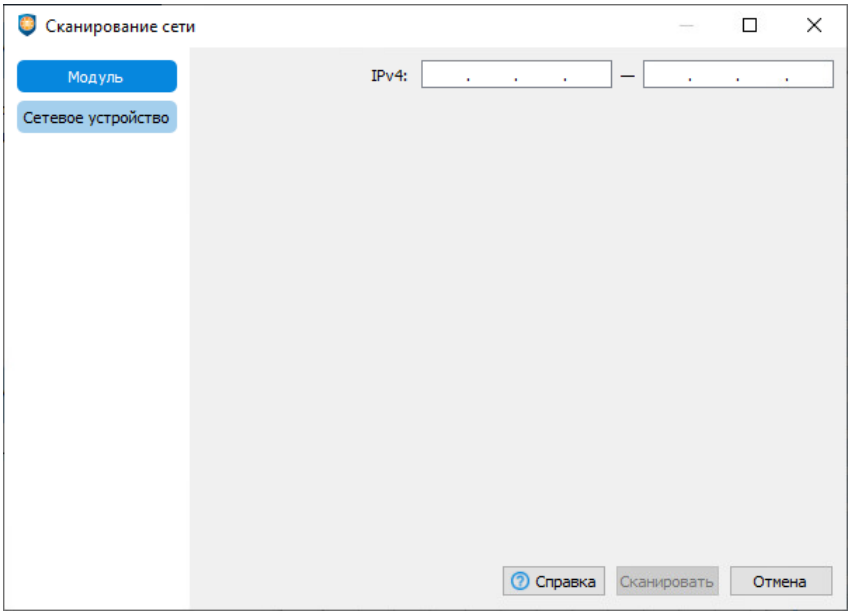

Рис. 88. Окно «Сканирование сети»

3. По завершению процесса сканирования из списка обнаруженных объектов можно выбрать те модули, которые необходимо зарегистрировать в ДБ, либо нажать кнопку «Выбрать все» для выбора всех обнаруженных модулей (рис. 89).

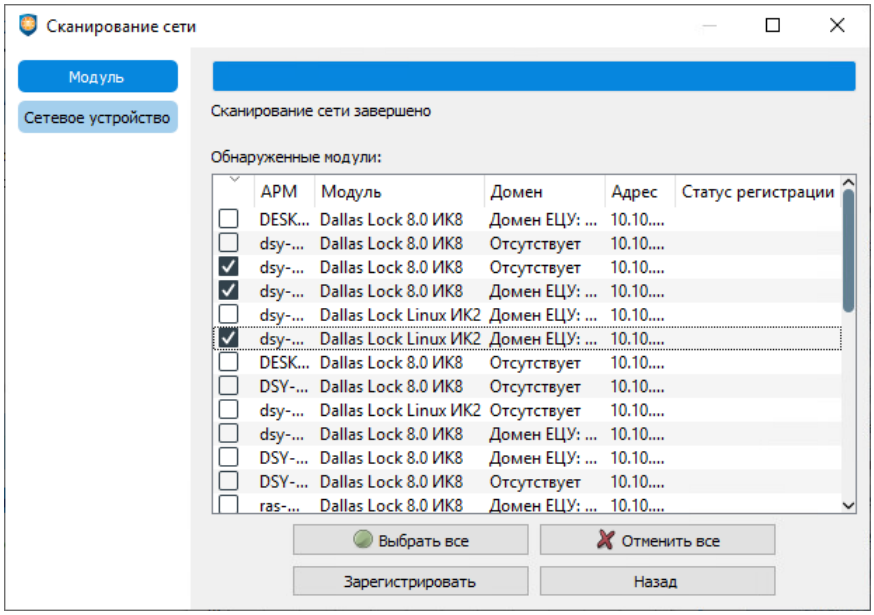

Рис. 89. Выбор объектов для регистрации в ДБ

После выбора всех регистрируемых модулей нужно нажать кнопку «Зарегистрировать».

4. Появится окно «Регистрация модулей», в котором нужно ввести авторизационные данные администратора модуля и ключ доступа к ДБ (рис. 90).

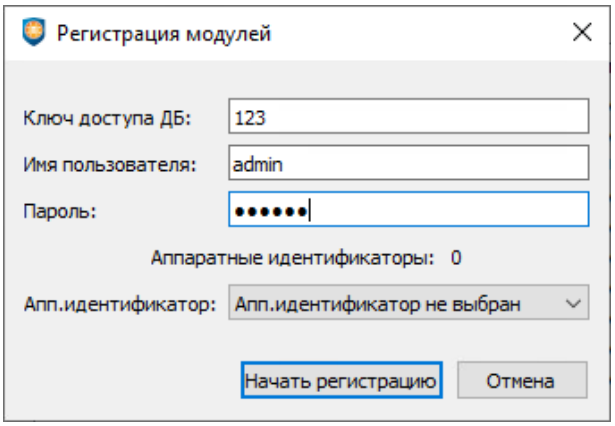

Рис. 90 Ввод данных для регистрации

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».

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. Добавленный комментарий отобразится в разделе «Информация об объекте» вкладки «Сводка».

Для вывода модуля из Домена безопасности ЕЦУ необходимо:

1. Выбрать пункт «Удалить модуль» из контекстного меню, нажав правой кнопкой мыши на нужный модуль в дереве ДБ (рис. 91), или воспользоваться командой «Удалить модуль» на панели инструментов «Действия» вкладки «Сводка» на уровне модуля в дереве ДБ (рис. 92).

Примечание. Для вывода модуля СЗИ ВИ Dallas Lock понадобится по отдельности удалить модуль Dallas Lock СЗИ ВИ и модуль Агент управления доступом.

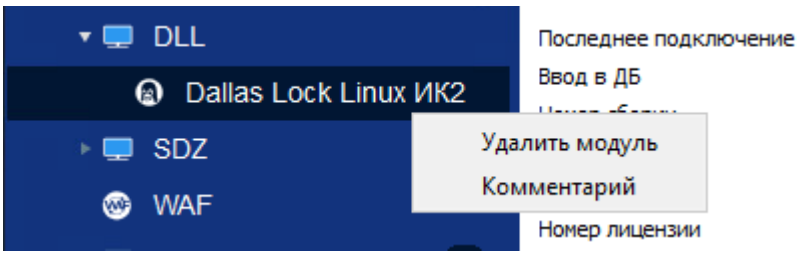

Рис. 91. Удаление модуля посредством контекстного меню

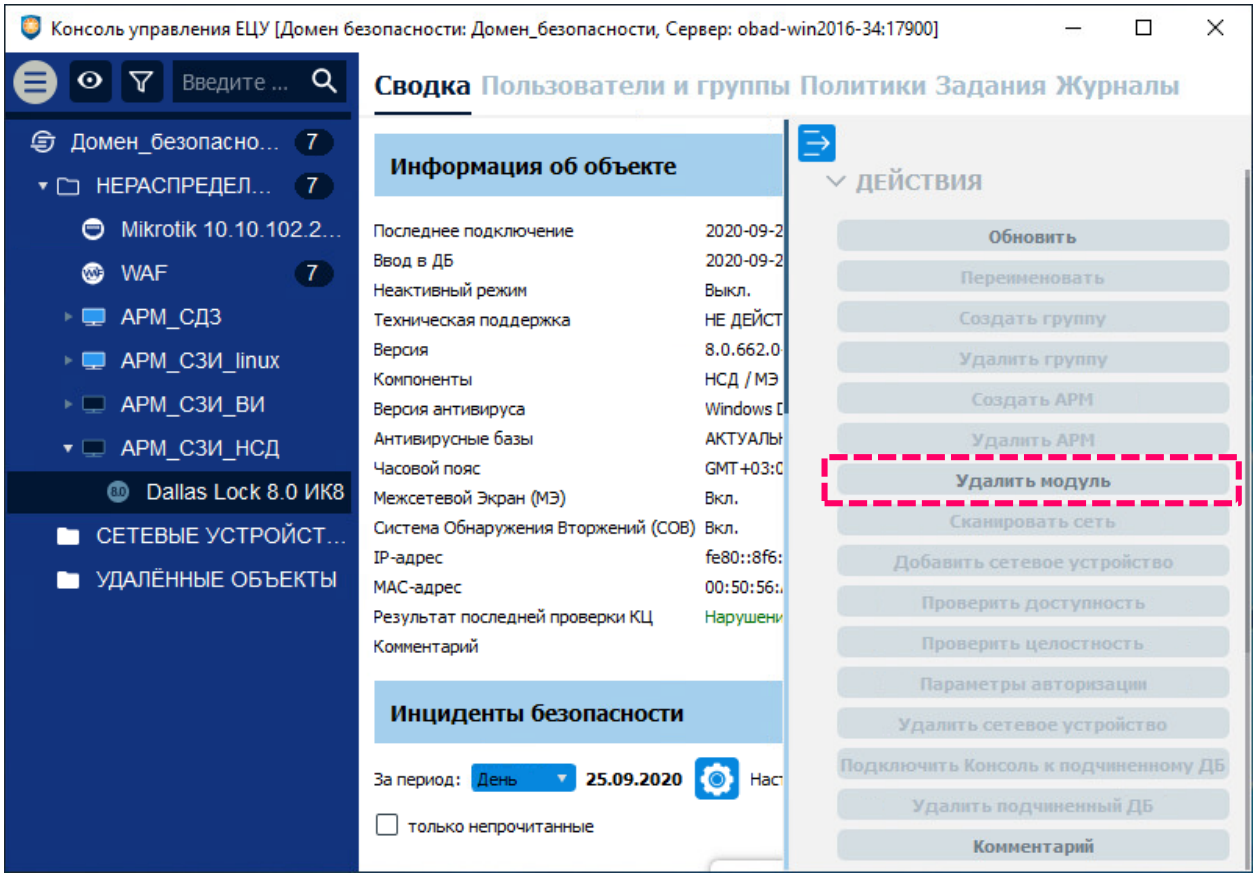

Рис. 92. Удаление посредством панели «Действия»

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.

8.1.1 Сводка модуля

Вкладка «Сводка» на уровне модуля отображает общее состояние модуля (рис. 93).

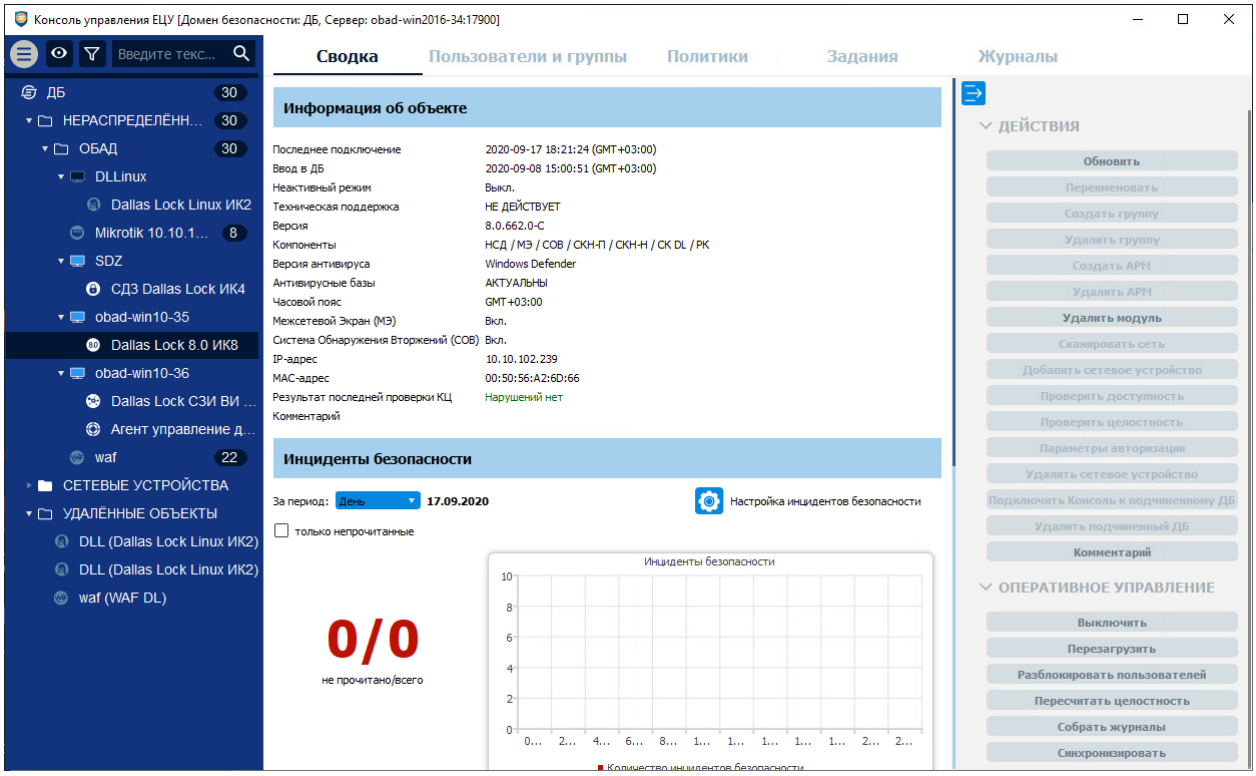

Рис. 93. Вкладка «Сводка» модуля

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.

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. 94).

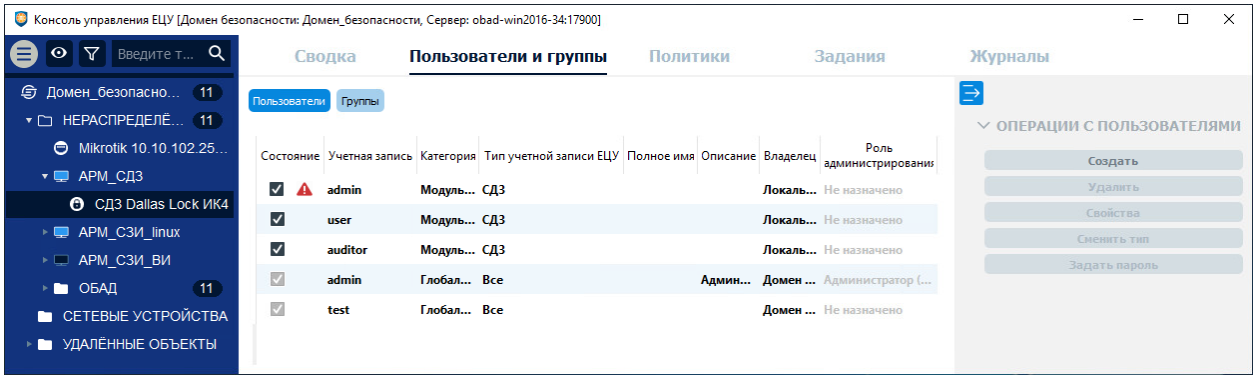

Рис. 94. Вкладка «Пользователи и групп» модуля

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. 95).

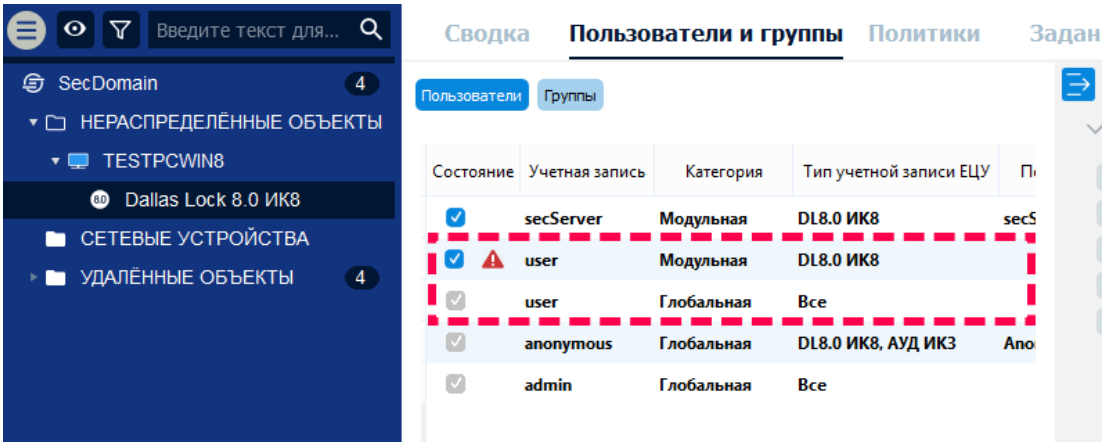

Рис. 95. Совпадение имен модульного и глобального пользователя

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. 96).

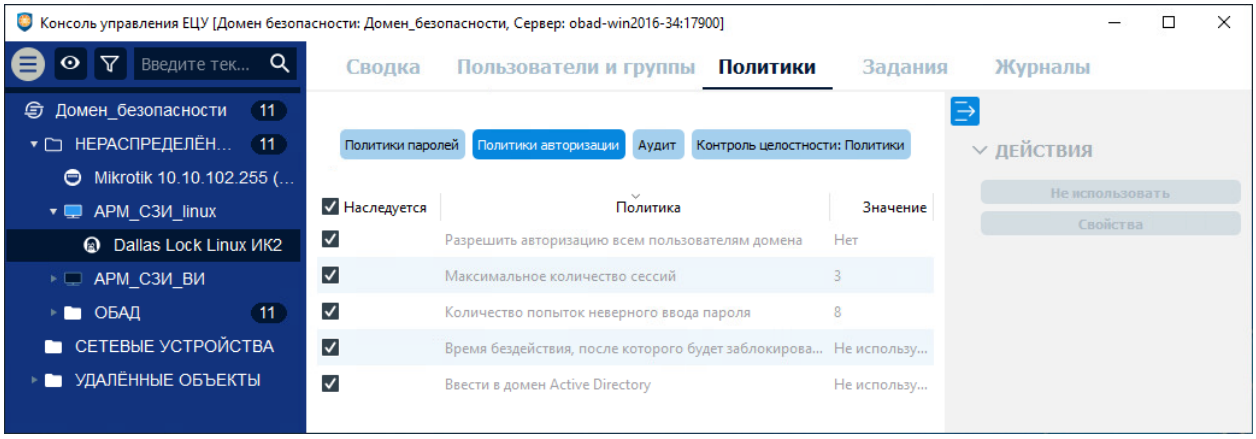

Рис. 96. Вкладка «Политики» модуля

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. 97).

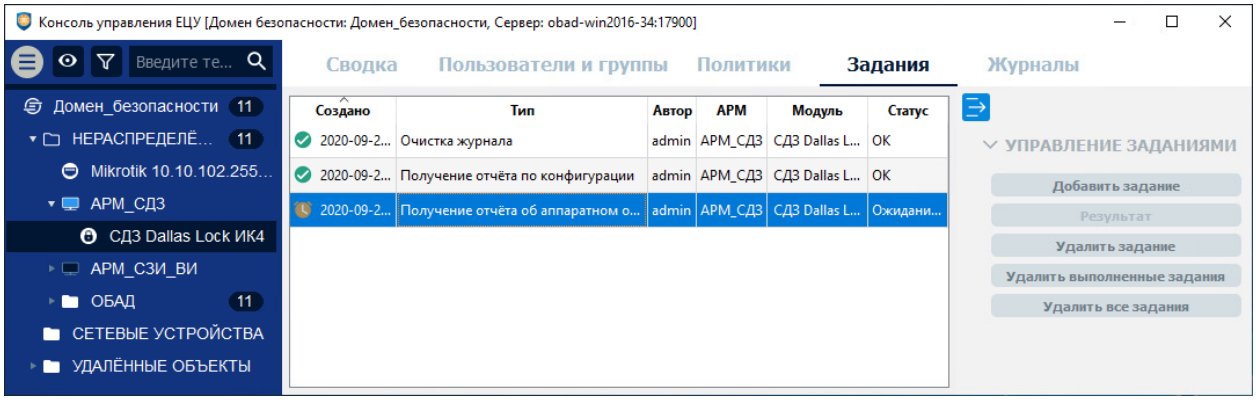

Рис. 97. Вкладка «Задания» модуля

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. 98).

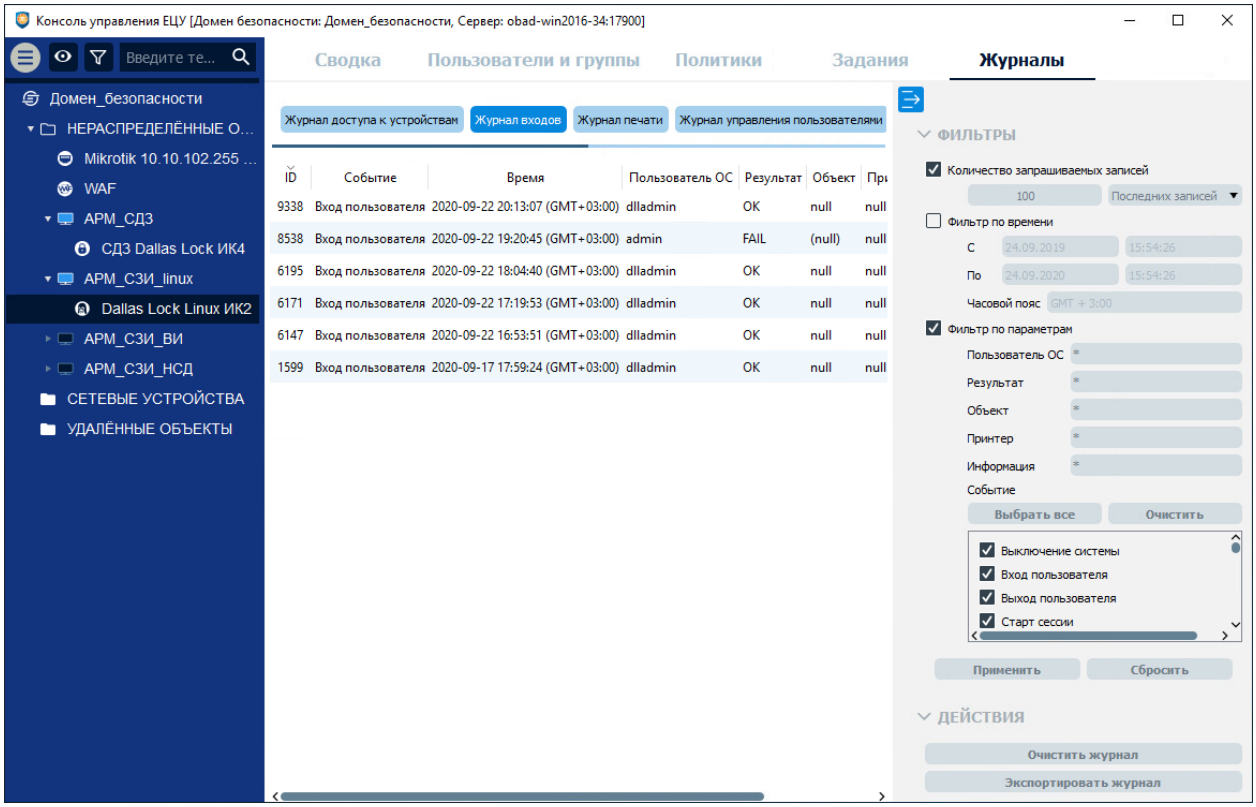

Рис. 98. Вкладка «Журналы» модуля

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 выбранном типе файла (TXT, CSV), воспользовавшись командой «Экспортировать журнал» на панели инструментов «Действия».

Для очистки выбранного 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. 99).

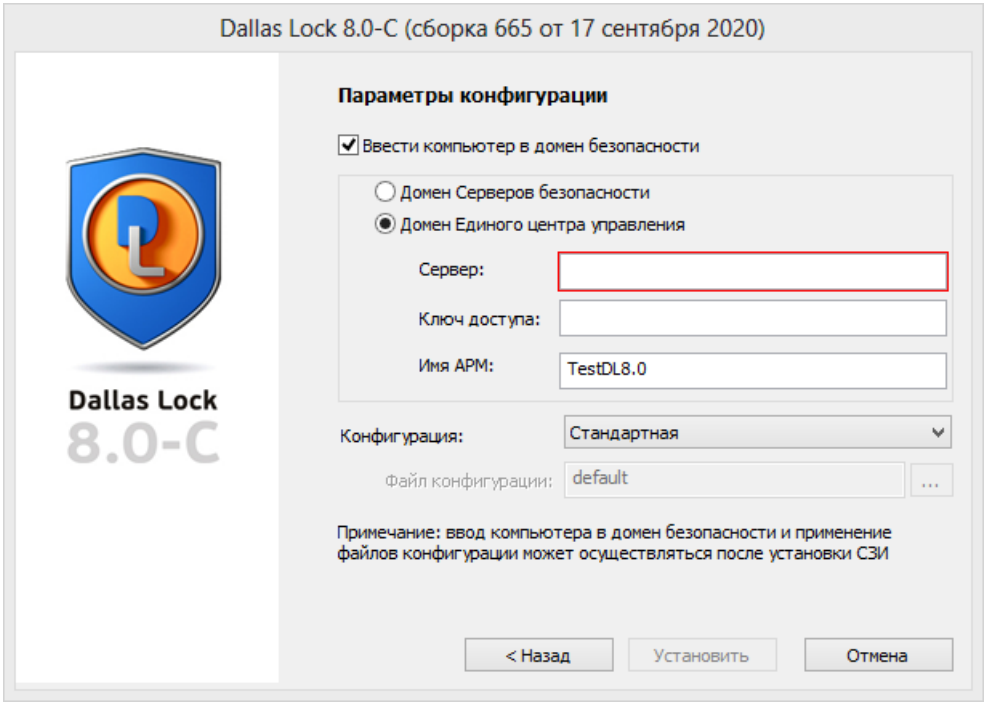

Рис. 99. Параметры установки системы защиты

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. 100).

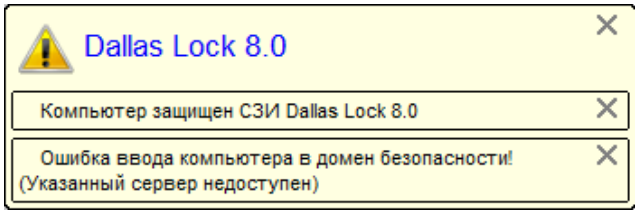

Рис. 100. Ошибка ввода компьютера в ДБ

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. 101).

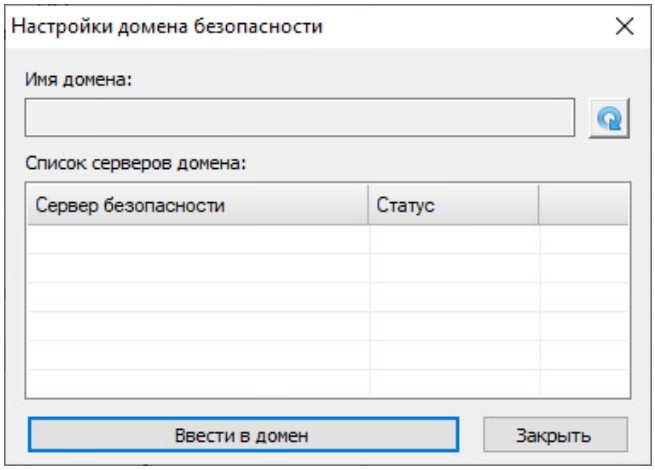

Рис. 101. Настройки ДБ

4. Нажать кнопку «Ввести в домен». Откроется окно ввода клиента в домен безопасности, где необходимо (рис. 102):
   - 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.

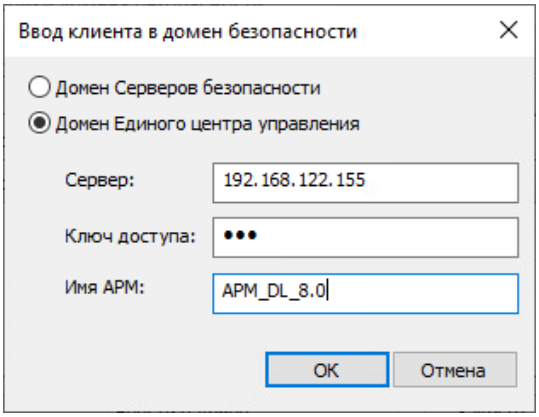

Рис. 102. Ввод компьютера в ДБ ЕЦУ

Далее необходимо нажать кнопку «ОК», и, в случае успеха, через некоторое время появится сообщение о том, что модуль успешно введен в ДБ (рис. 103).

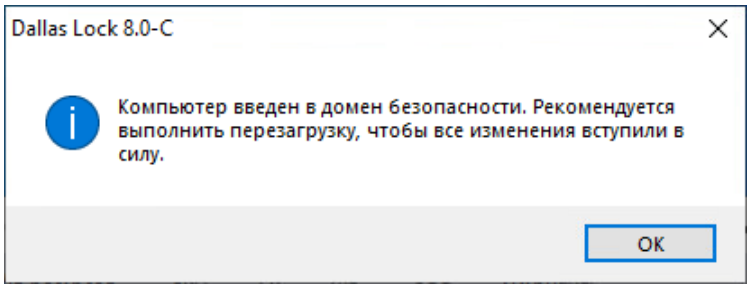

Рис. 103. Сообщение об успешном вводе модуля в ДБ

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. 104);

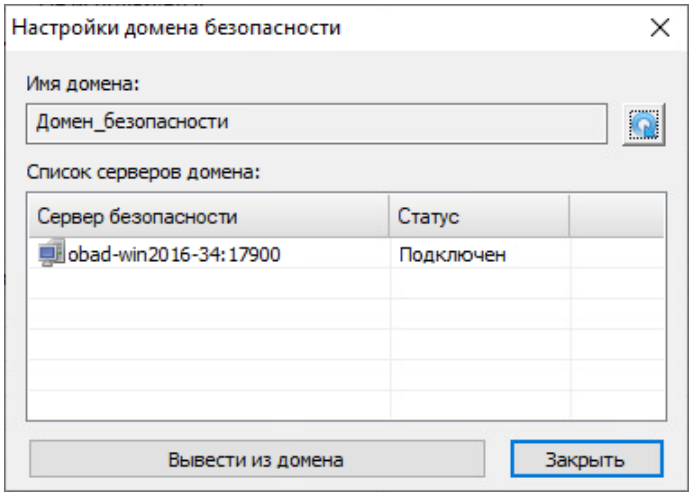

Рис. 104. Настройки ДБ

3. нажать кнопку «Вывести из домена». Откроется окно для подтверждения вывода модуля из ДБ (рис. 105);

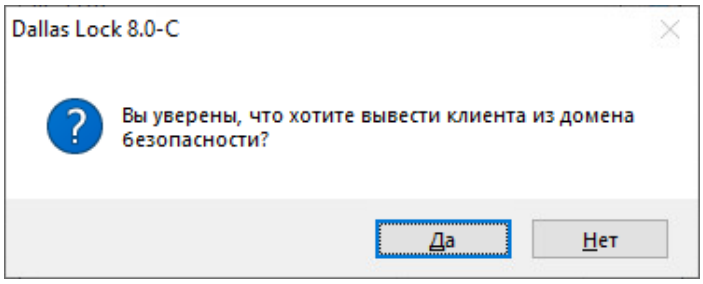

Рис. 105. Вывод модуля из ДБ

4. нажать кнопку «Да». Появится сообщение о том, что модуль успешно выведен из ДБ (рис. 106).

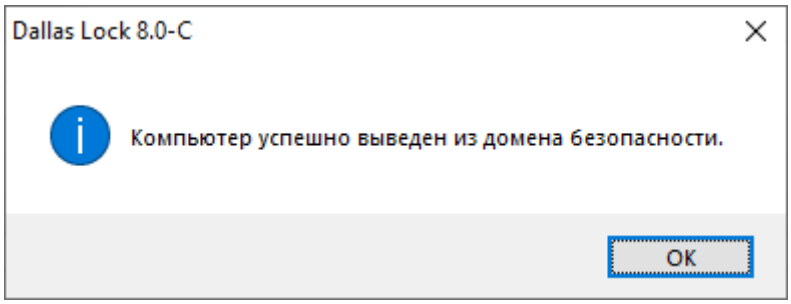

Рис. 106. Сообщение об успешном выводе модуля из ДБ

В консоли ЕЦУ удаленный модуль переместится в базовую группу «Удаленные объекты» дерева ДБ.

9.3 Централизованная установка СЗИ Dallas Lock 8.0 средствами AD

Средствами Microsoft Windows возможна централизованная установка СЗИ НСД Dallas Lock 8.0 на рабочие станции, входящие в состав контроллера домена AD.

Необходимые для этого действия включают в себя:

1. формирование файла установки на ЕЦУ;
2. создание точки распространения на контроллере домена AD;
3. создание объекта групповой политики для централизованной установки средствами AD;
4. конфигурация и применение групповой политики.

Примечание. Настройки параметров, производимые непосредственно на контроллере AD, будут рассмотрены на примере ОС Windows Server 2016.

9.3.1 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 → «Подготовить дистрибутив DL8.0 для AD». Появится окно «Мастер подготовки дистрибутива СЗИ для установки средствами AD» (рис. 107).

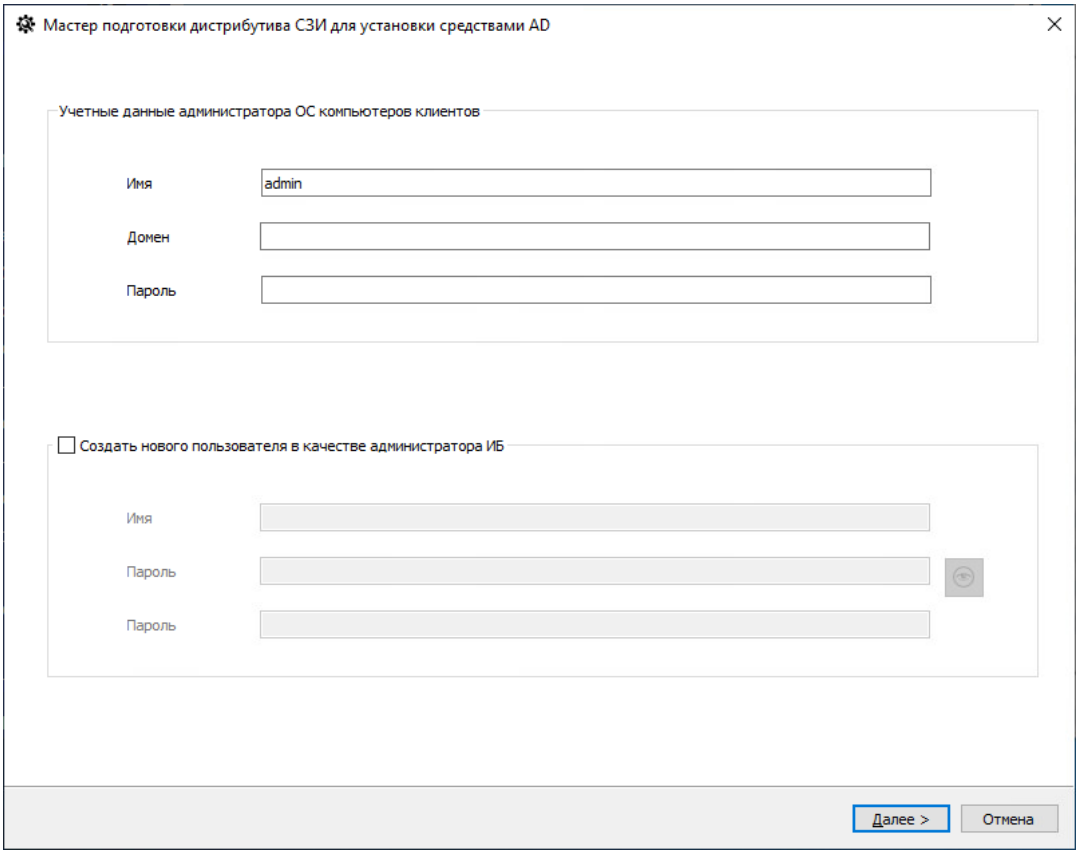

Рис. 107. Начало подготовки дистрибутива СЗИ Dallas Lock 8.0 для AD

В окне обязательно необходимо указать учетные данные администратора ОС компьютеров клиентов:

1. ввести логин и пароль будущего суперадминистратора СЗИ Dallas Lock 8.0 на целевых ТС;
2. имя домена Active Directory.

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.

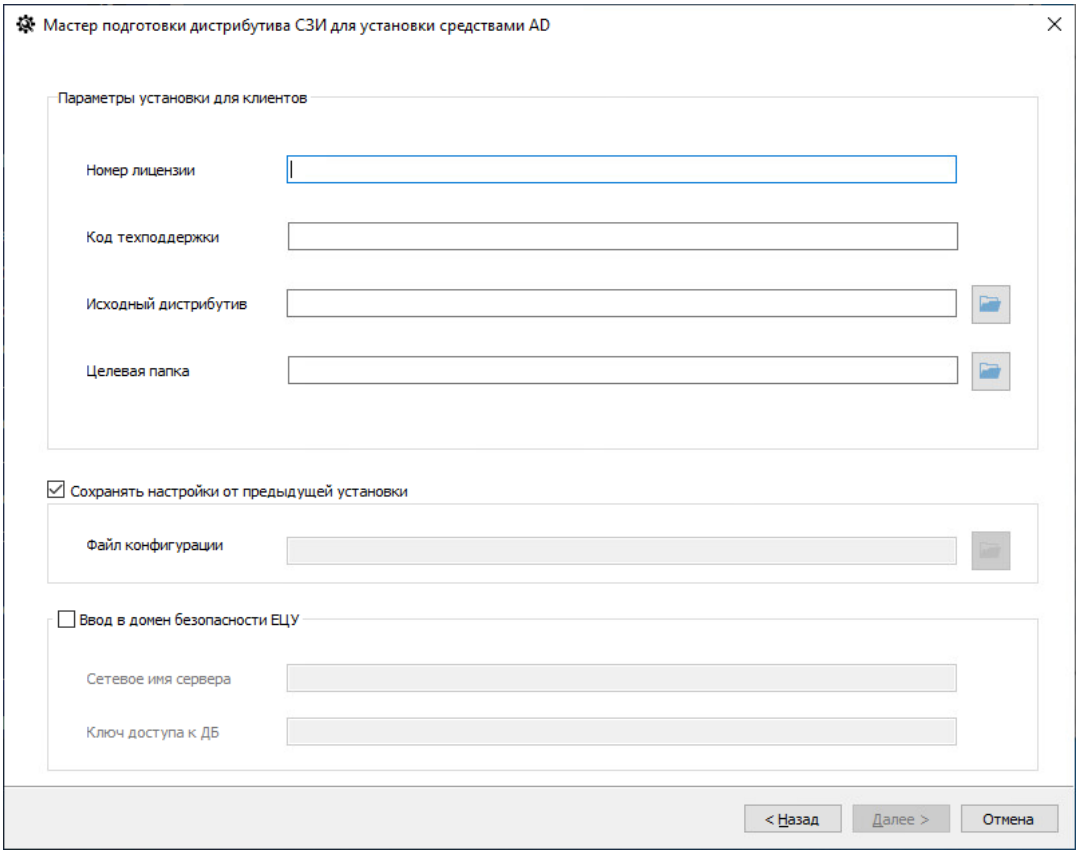

Рис. 108. Ввод параметров для дистрибутива

На втором шаге подготовки дистрибутива необходимо указать параметры удаленной установки, которые будут применены к целевым ТС после активации СЗИ Dallas Lock 8.0 (рис. 108):

1. номер лицензии;
2. код технической поддержки, который указан на обложке футляра;
3. путь к исходному дистрибутиву СЗИ Dallas Lock 8.0;
4. путь для создания дистрибутива на ПК, на котором запущена консоль ЕЦУ.

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 сетевое имя сервера ЕЦУ и ключ доступа к ДБ (по умолчанию ключ имеет пустое значение).

После заполнения всех обязательных полей в правом нижнем углу станет доступна кнопка «Далее» для перехода к следующему шагу подготовки дистрибутива.

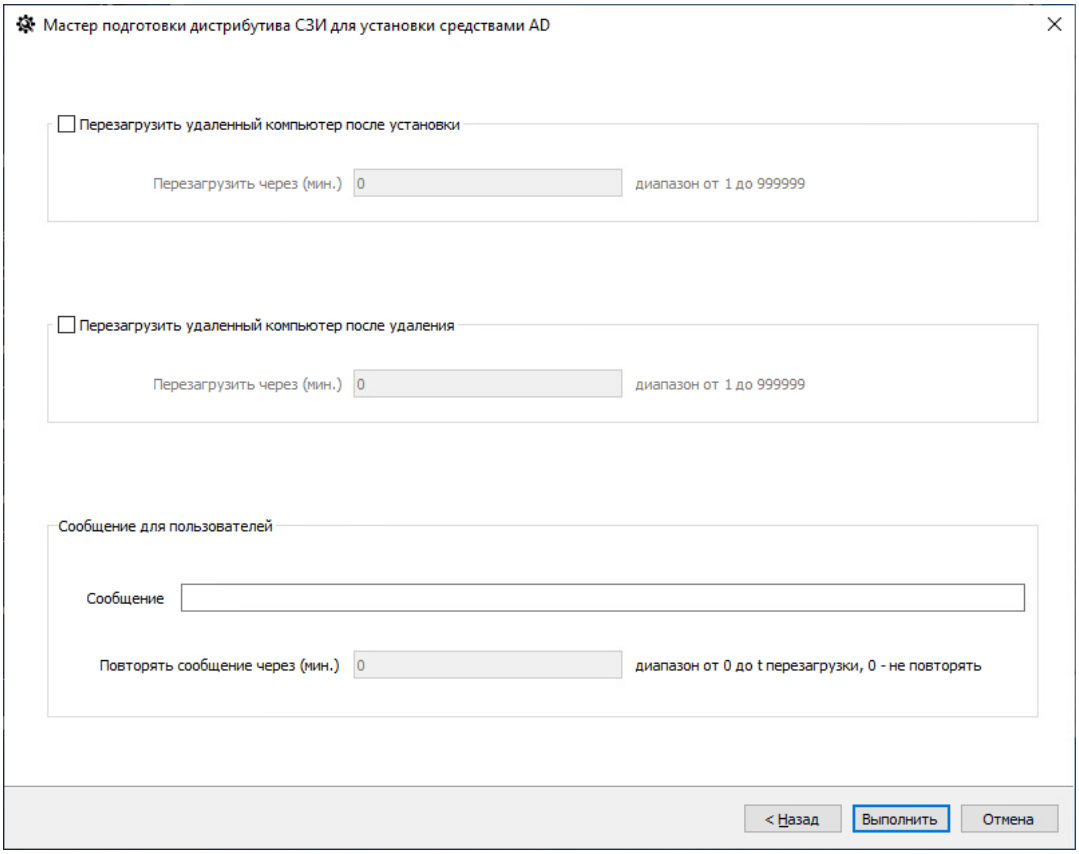

Рис. 109. Настройка параметров перезагрузки

На следующем шаге подготовки дистрибутива указываются параметры перезагрузки при инсталляции (рис. 109).

Поставленный в окне флаг «Перезагрузить удаленный компьютер после установки/удаления» позволяет автоматически перезагрузить компьютер после завершения установки/удаления 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/удаление СЗИ.

Для продолжения подготовки дистрибутива нажать кнопку «Выполнить».

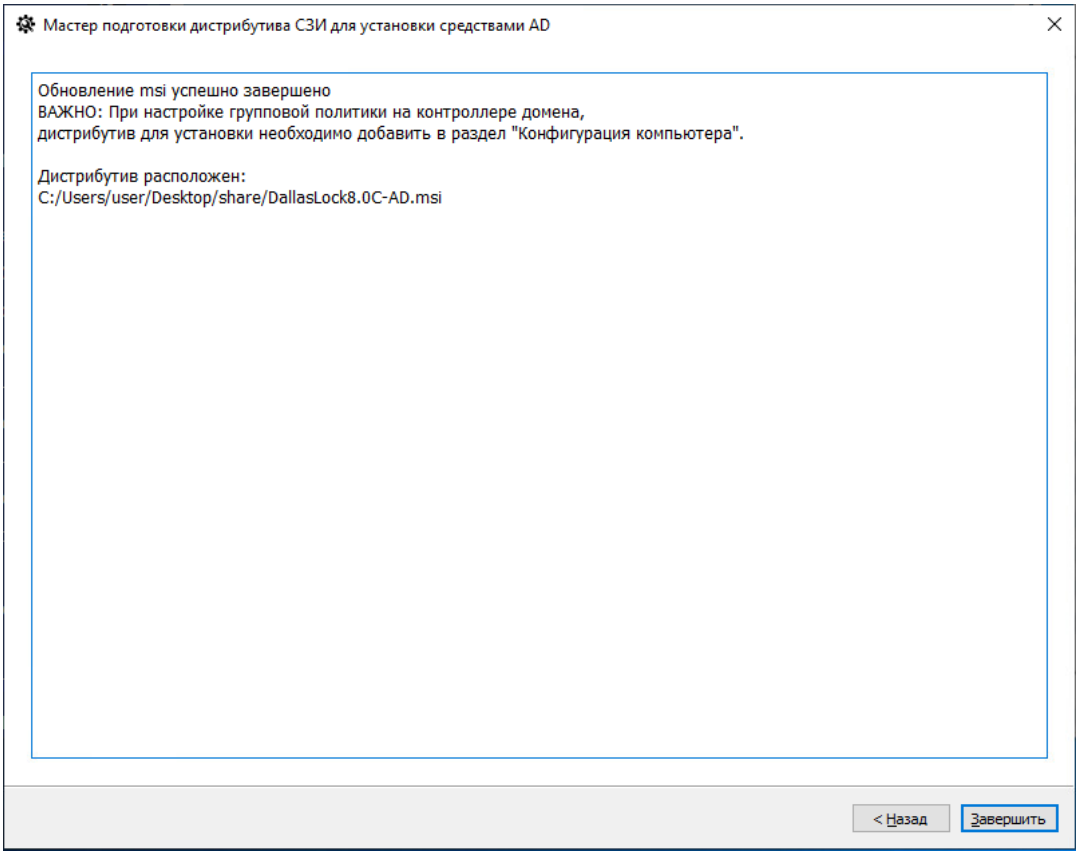

Рис. 110. Завершение подготовки дистрибутива

Появится окно с сообщением об успешном обновлении дистрибутива для установки AD. Дистрибутив будет расположен по пути, указанному в окне (рис. 110).

Подготовленный дистрибутив необходимо перенести на контроллер домена Windows Server, с которого будет производится удаленная установка.

Далее необходимо приступить к настройкам непосредственно на контроллере домена в службах AD.

9.3.2 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. 111, рис. 112).

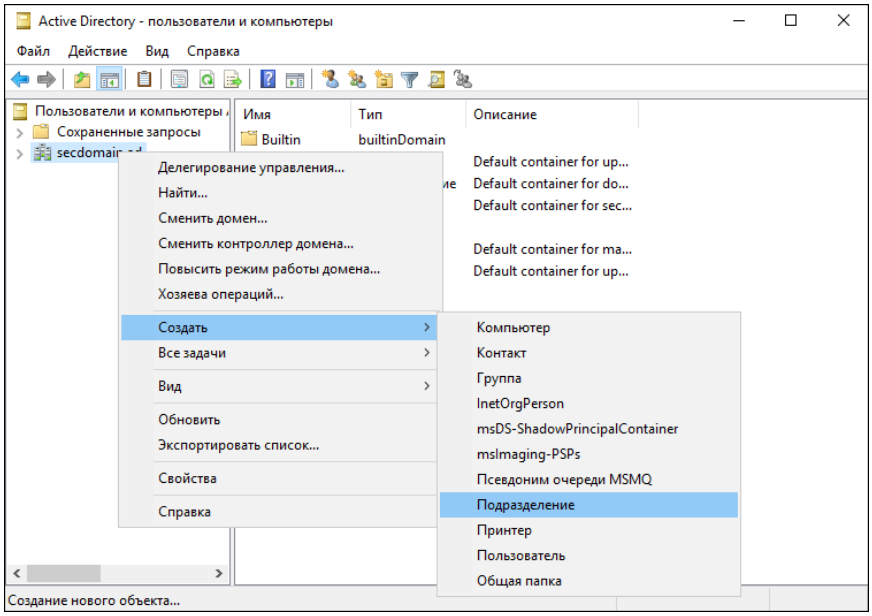

Рис. 111. Создание подразделения в AD

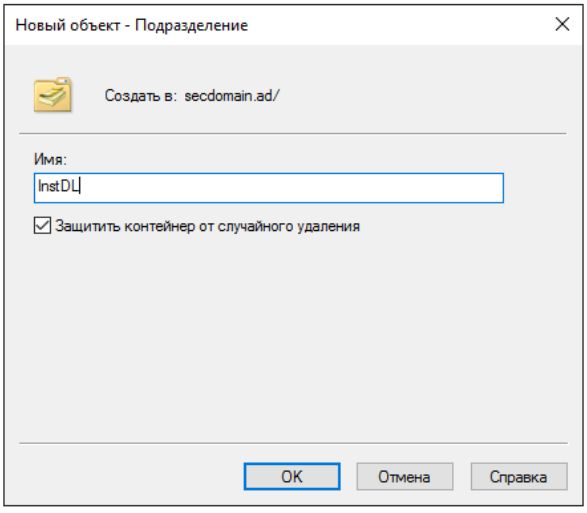

Рис. 112. Имя нового подразделения в AD

2. В это подразделение перенести необходимые компьютеры с помощью функции из контекстного меню «Переместить» (рис. 113, рис. 114).

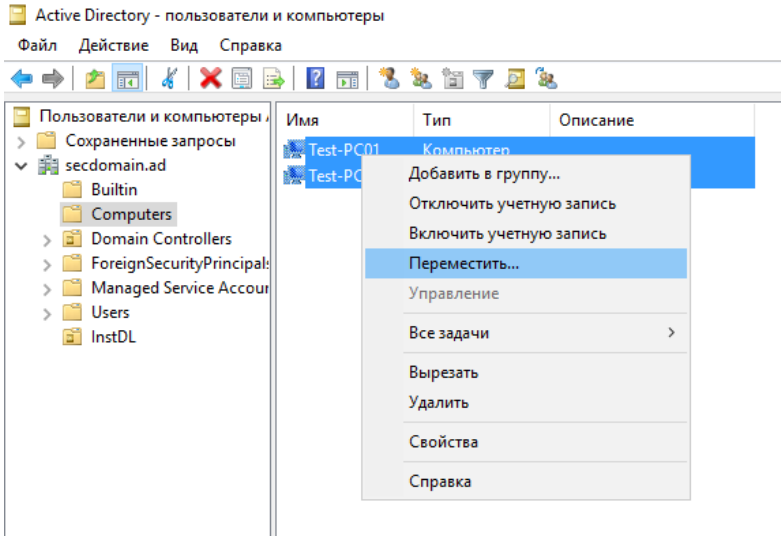

Рис. 113. Пункт контекстного меню «Переместить…»

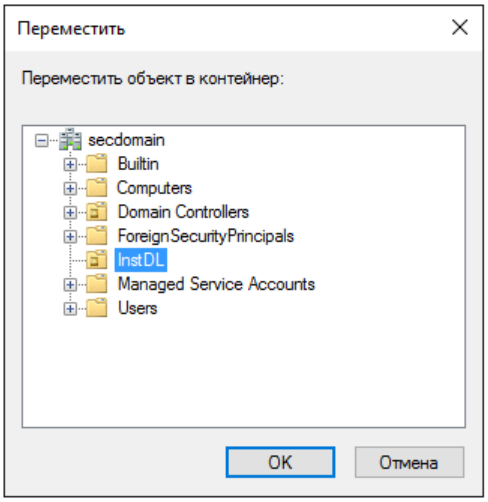

Рис. 114. Перенос рабочих станций в подразделение

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.

9.3.3 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. 115).

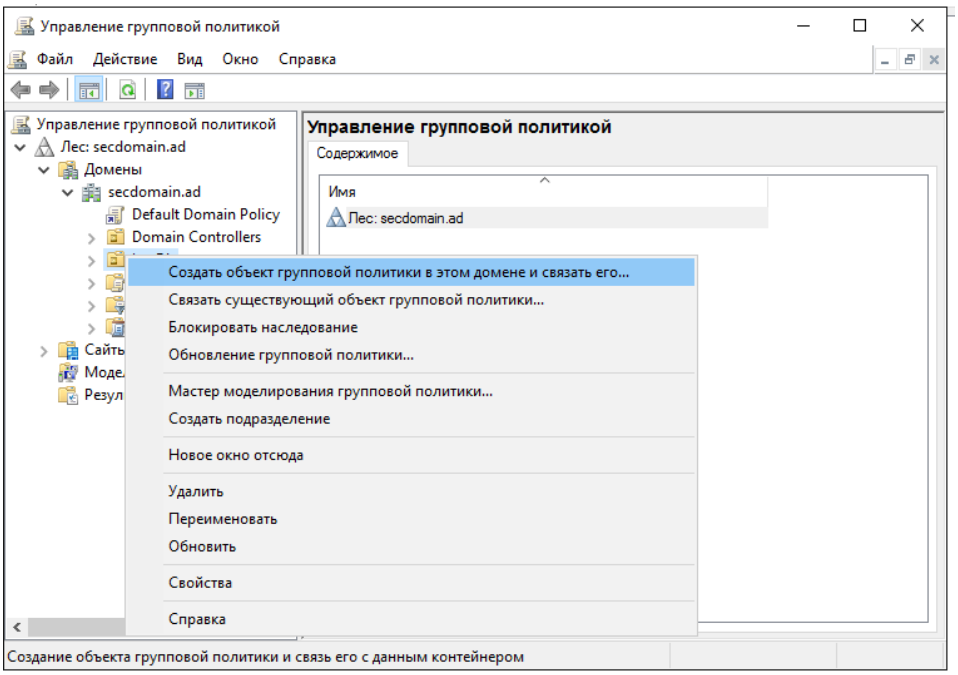

Рис. 115. Консоль управления групповой политикой на Windows Server

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. 116).

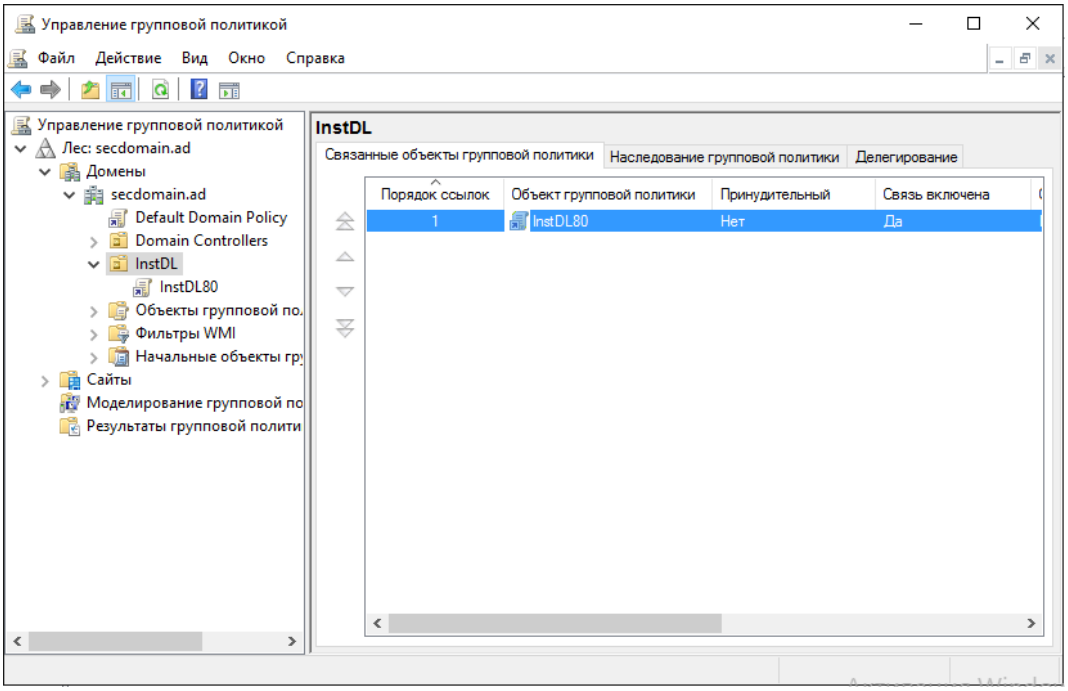

Рис. 116. Новый объект групповой политики, связанный с подразделением

3. Таким образом создана групповая политика для подразделения компьютеров в ОС Windows Server.

9.3.4 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. 117).

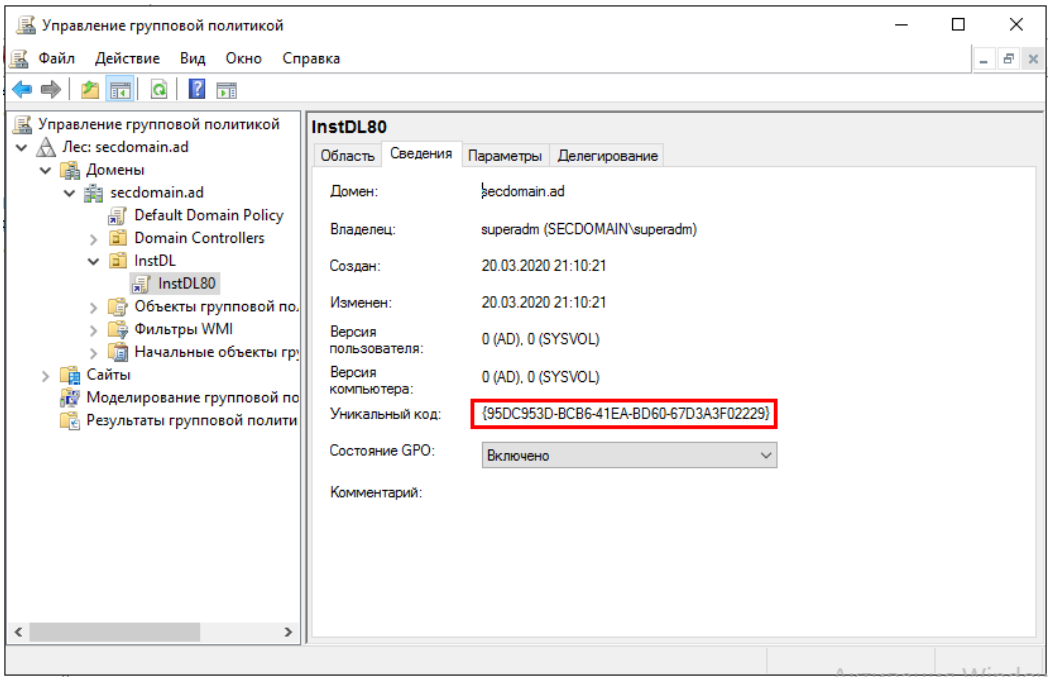

Рис. 117. Новый объект групповой политики, связанный с подразделением

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. 118).

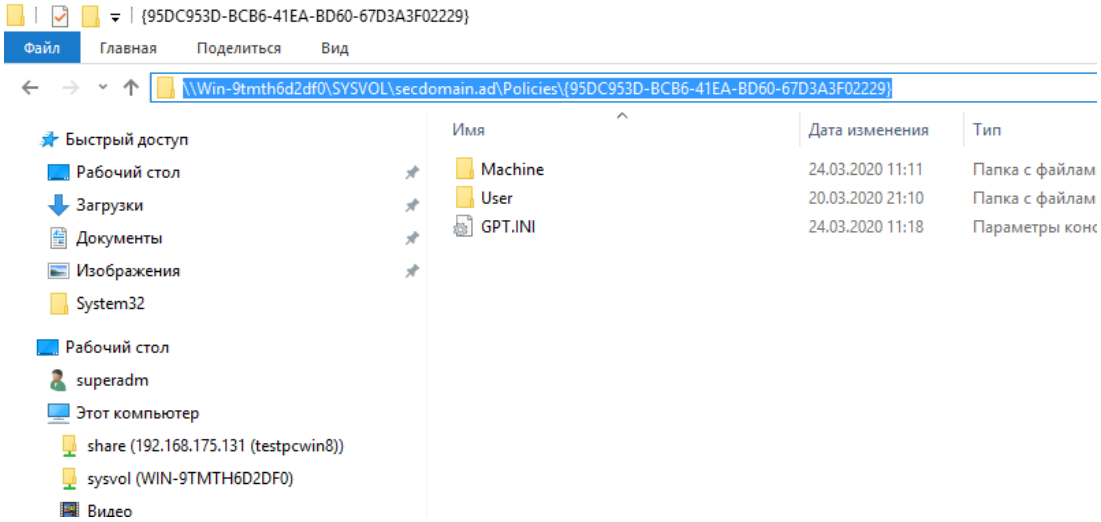

Рис. 118. Расположение папки-контейнера групповой политики

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. 119).

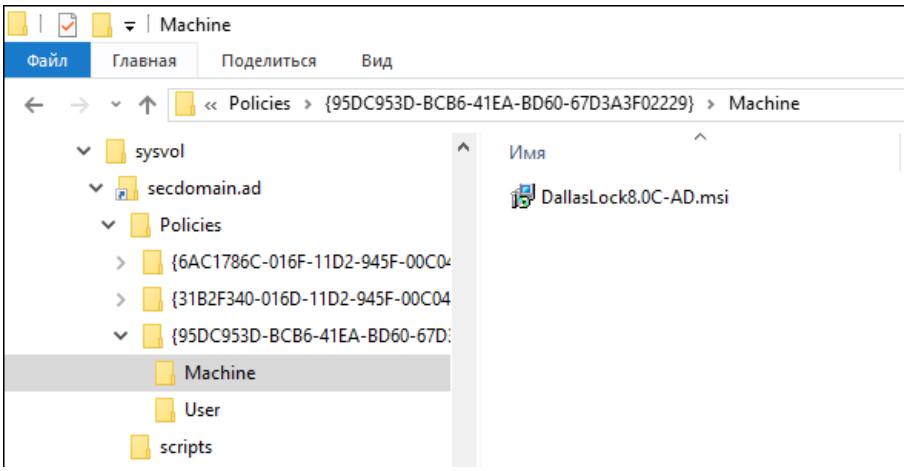

Рис. 119. Перенос msi-дистрибутива в папку групповой политики

Таким образом, был создан источник удаленной установки системы защиты Dallas Lock 8.0, который в контексте Microsoft имеет название «Точка распространения».

9.3.5 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. 120).

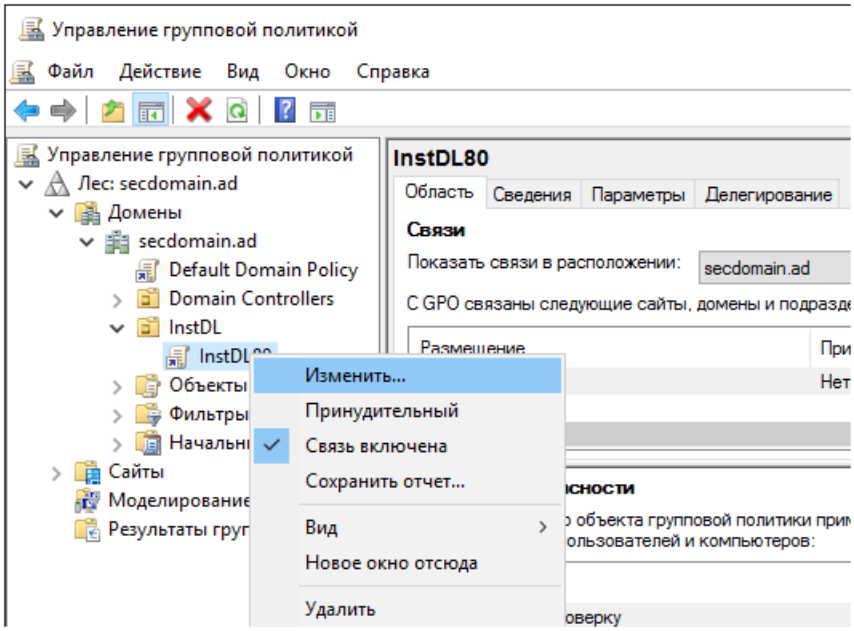

Рис. 120. Вызов контекстного меню в Консоли управления групповой политикой

Откроется необходимое окно редактора. В данном окне в дереве параметров требуется выбрать установку программ (рис. 121).

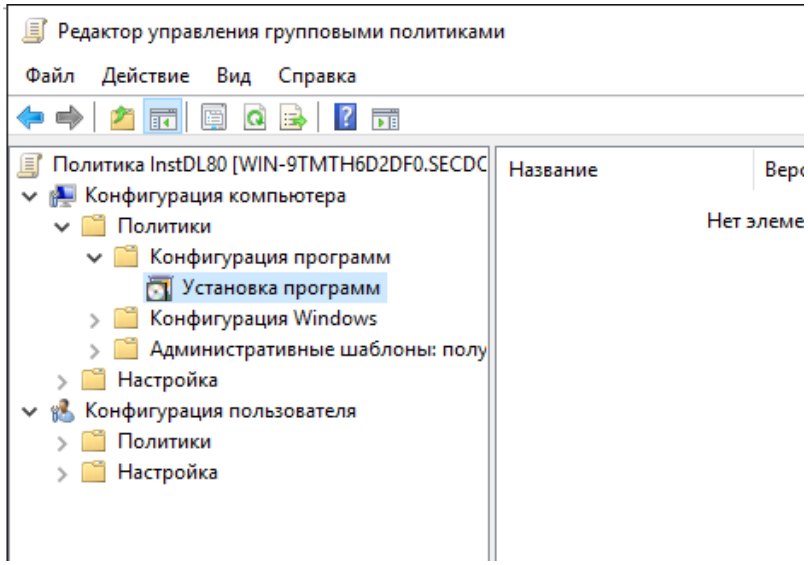

Рис. 121. Окно редактора групповой политики

2. Далее в правом поле окна установки программ с помощью контекстного меню создать пакет установки: нажать последовательно «Создать», «Пакет...» (рис. 122).

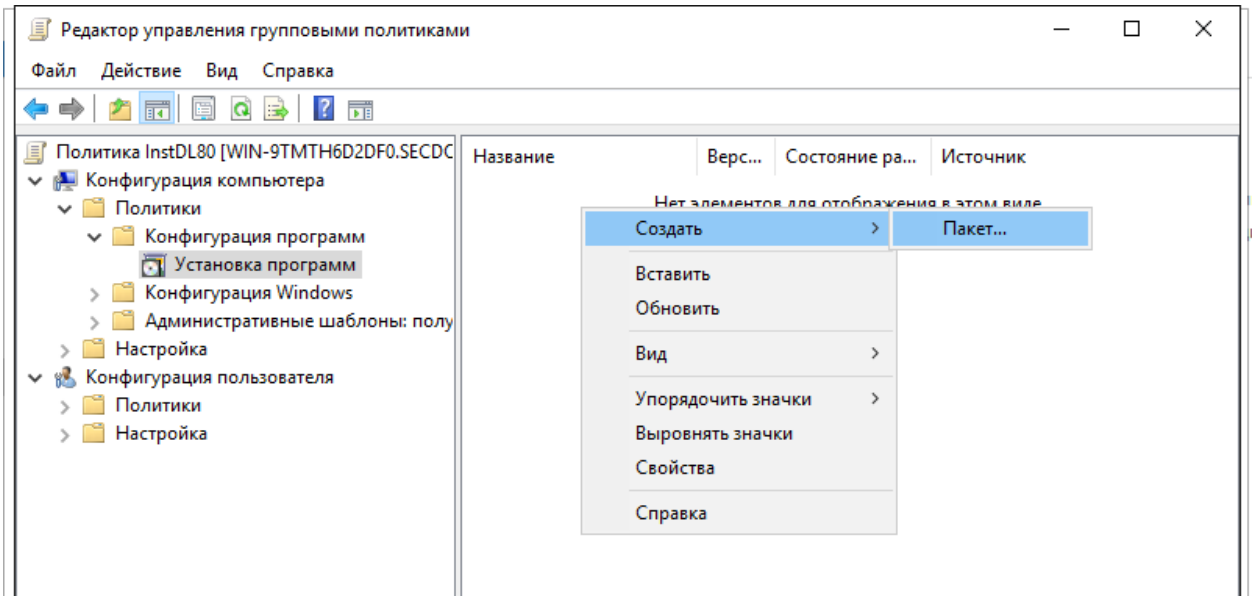

Рис. 122. Создание пакета конфигурации

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. 123).

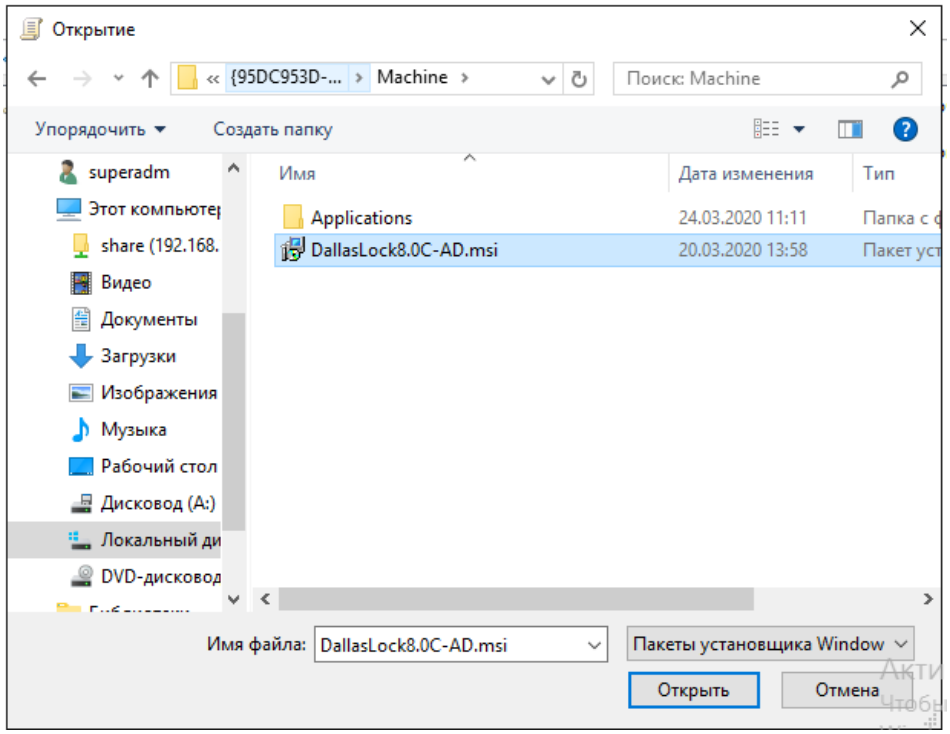

Рис. 123. Выбор расположения пакета установки

4. Выбрать msi-пакет и нажать кнопку «Открыть».
5. В диалоговом окне выбора метода развертывания программ необходимо выбрать вариант «назначенный» и нажать «OK» (рис. 124).

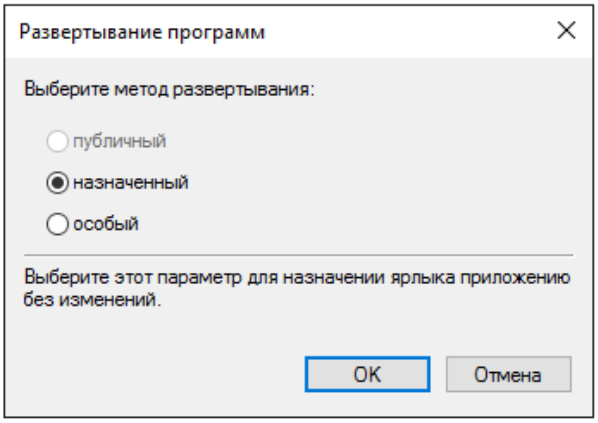

Рис. 124. Выбор метода развертывания программ

Система развернет сформированный файл установки. Выбранный общий установочный пакет появится на правой панели редактора объектов групповой политики (рис. 125).

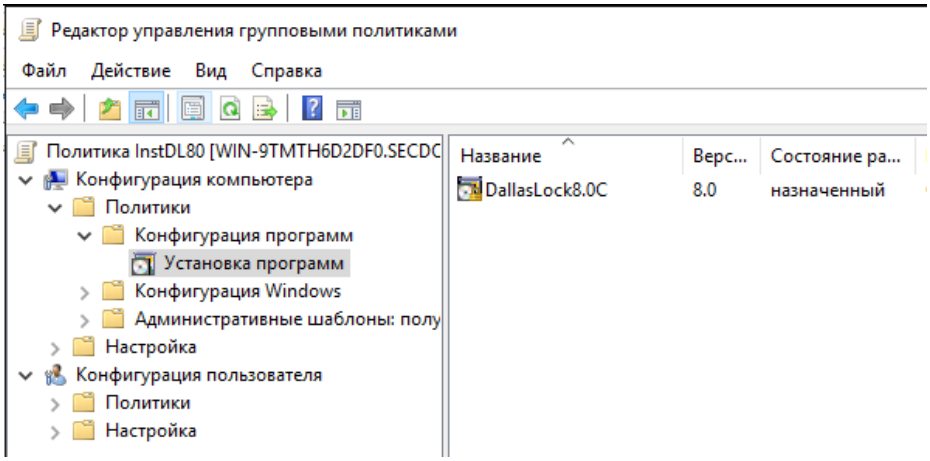

Рис. 125. Появление назначенного пакета установки в окне конфигурации

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;
- по расписанию (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. 126).

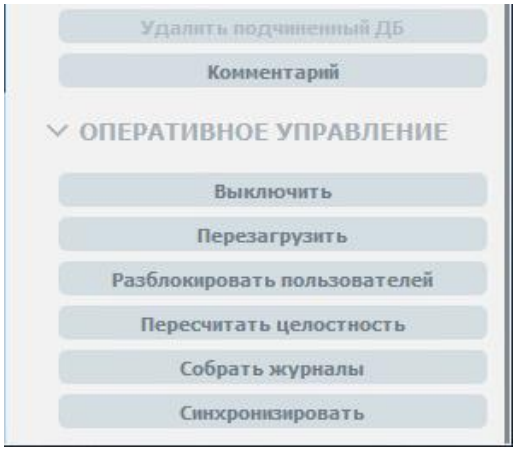

Рис. 126. Кнопка «Синхронизировать»

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;
- по расписанию (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. 127).

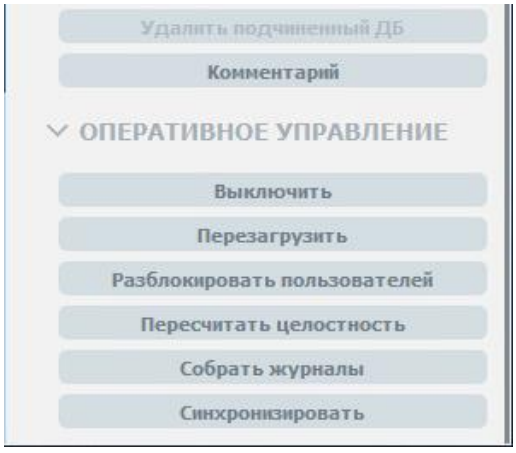

Рис. 127. Кнопка «Собрать журналы»

Отправка журналов по команде из оболочки администрирования DL8.0

Для отправки журналов в 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 «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. 128).

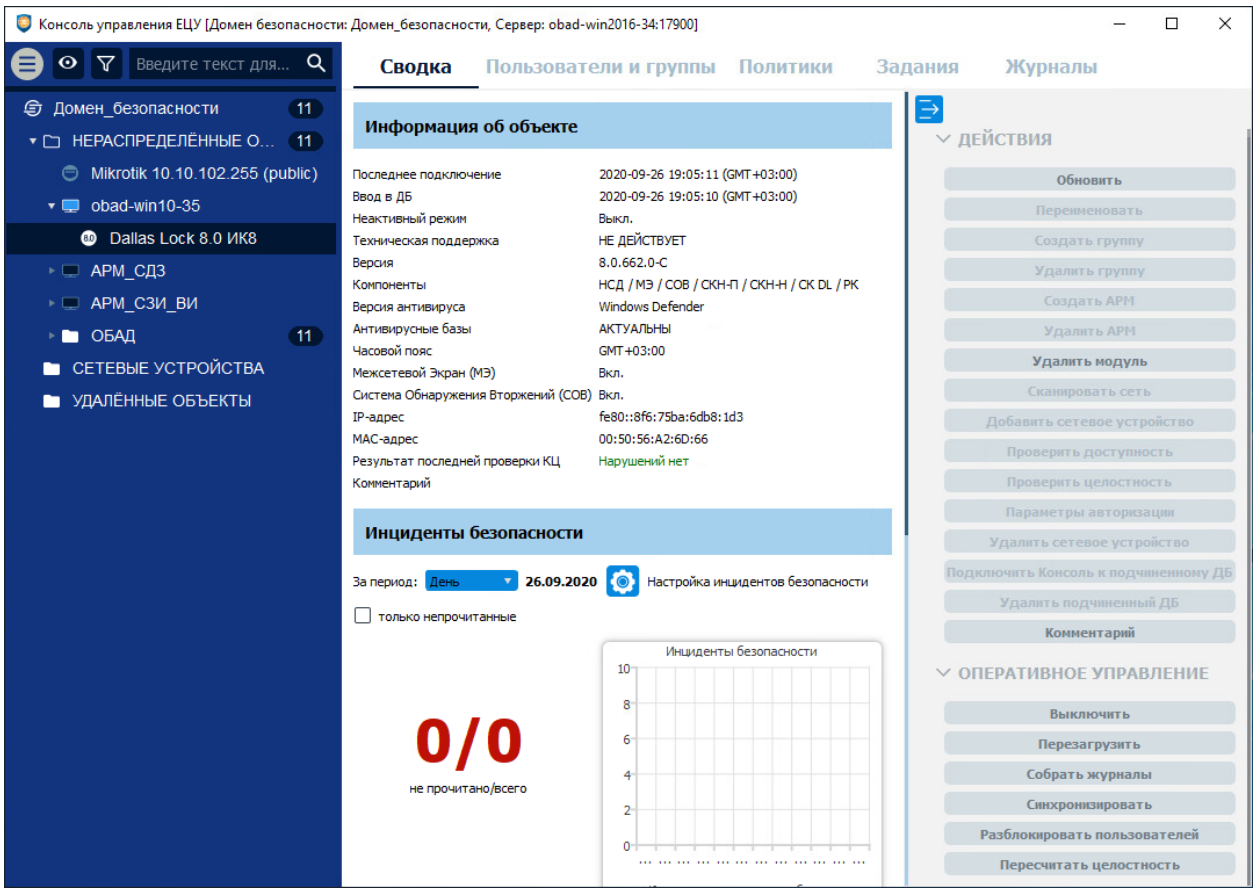

Рис. 128. Вкладка «Сводка»

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.
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;
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. 129):

- изменение параметров лицензии;
- получение конфигурации;
- применение конфигурации;
- проверка целостности.

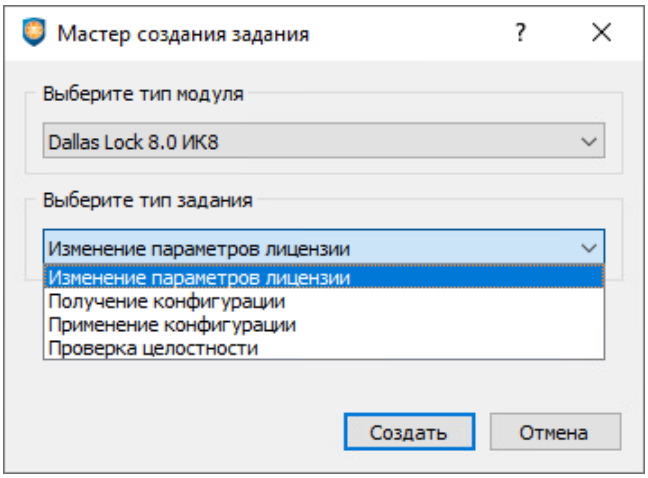

Рис. 129. Мастер создания задания для модуля СЗИ Dallas Lock 8.0

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. 130).

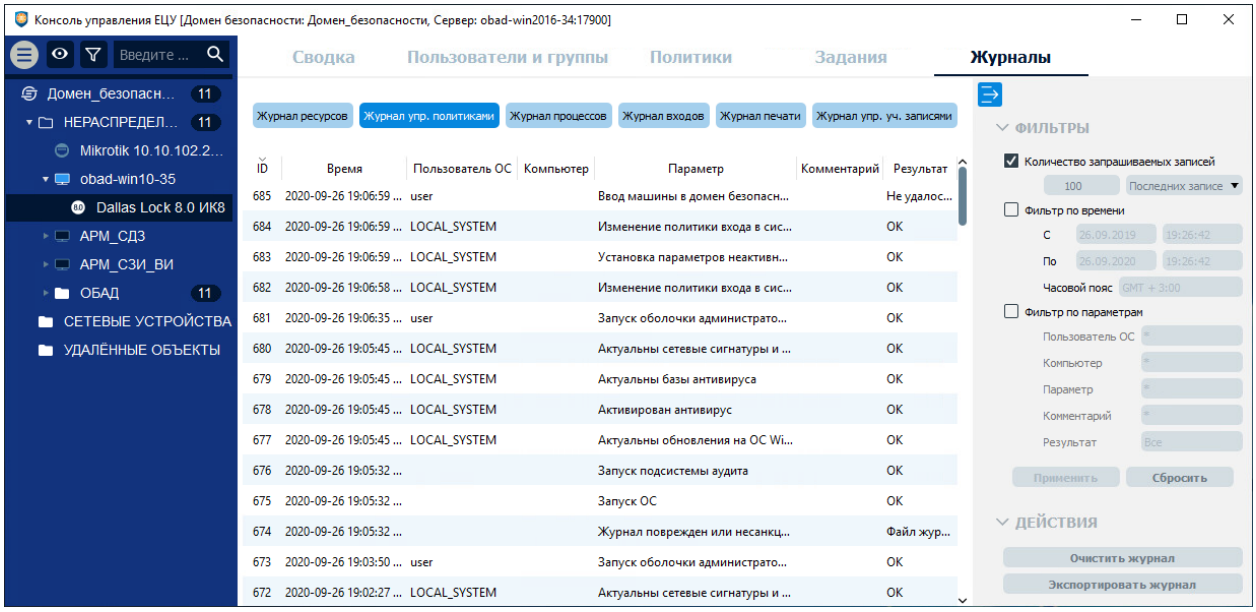

Рис. 130. Вкладка «Журналы»

Для модуля СЗИ Dallas Lock 8.0 доступны:

- «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:

1. в ЛВС должен быть работающий сервер ЕЦУ;
2. между модулем и сервером ЕЦУ должен быть свободный обмен пакетами по TCP/IP порту 17900.

Внимание! После ввода модуля СЗИ 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 «Централизованное управление» (рис. 131), где необходимо указать:
   - имя АРМ, в составе которого необходимо ввести модуль;
   - адрес сервера ЕЦУ;
   - ключ доступа к ДБ.

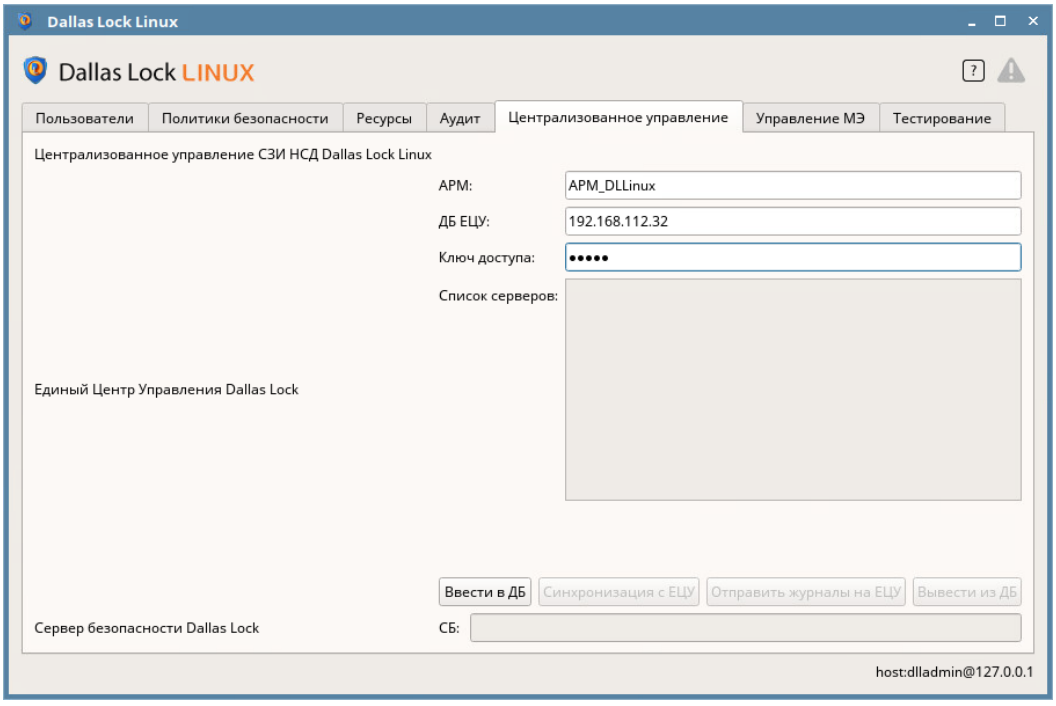

Рис. 131. Вкладка «Централизованное управление»

4. Далее необходимо нажать кнопку «Ввести в ДБ».

Если процесс ввода модуля в ДБ прошел успешно, то через некоторое время поля с информацией о Домене безопасности станут недоступными для редактирования.

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 раздел централизованного управления «*mngdll*»;
4. перейти в подменю ввода в домен безопасности, выполнив команду *connect-domain*». После ввода команды система перейдет в раздел ввода в домен безопасности «*connect-domain*»;
5. в данном разделе необходимо задать последовательно следующие атрибуты подключения:
   - *net-name <IP-адрес или сетевое имя сервера ЕЦУ>*;
   - *name <имя АРМ>*;
   - *key <ключ доступа к ДБ>*;
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.

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. открыть вкладку «Централизованное управление»;
3. нажать кнопку «Вывести из ДБ» (рис. 132).

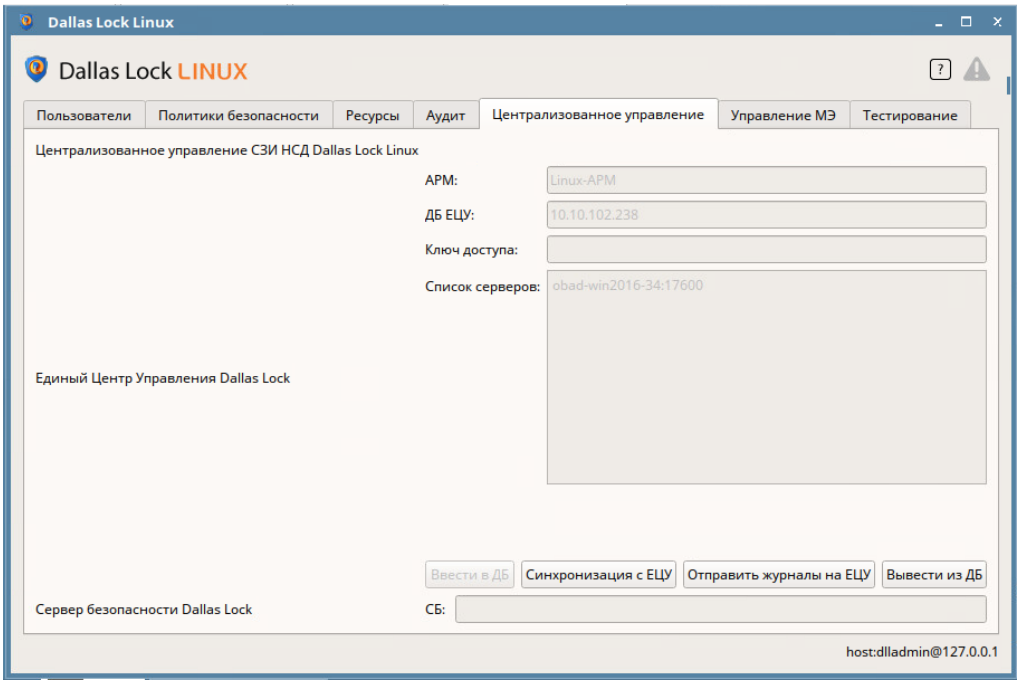

Рис. 132. Вывод модуля из ДБ

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 «*mngdll*»;
3. перейти в подменю вывода из домена безопасности, выполнив команду «*disconnect-domain*». После ввода команды система перейдет в раздел вывода из домена безопасности «*disconnect-domain*»;
4. выполнить команду «*execute*»;

Примечание. При условии отсутствия связи с Доменом безопасности перед выполнением команды «*execute*» необходимо изменить атрибут, предназначенный для принудительного вывода модуля из ДБ.
Пример:
force yes <enter>
execute <enter>

5. в результате успешного выполнения появится сообщение:
   «C*ommand 'disconnect-domain' executed successfully*» — модуль успешно выведен из ДБ.

В консоли ЕЦУ удаленный модуль переместится в базовую группу «Удаленные объекты» дерева ДБ.

10.3 Централизованная установка СЗИ НСД Dallas Lock Linux

Существует возможность централизованно выполнить установку или удаление СЗИ Dallas Lock Linux для одного или нескольких компьютеров, расположенных в одной ЛВС.

Внимание! В процессе удаленной установки СЗИ 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:

1. для компьютеров следует использовать имя и пароль администратора ОС и выполнять удаленную установку для группы компьютеров, имеющих одинаковые пароли администратора ОС;
2. 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 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 Dallas Lock Linux необходимо отключить SSH-сервер на целевых ТС.

Для удаленной установки 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»[1]. Сохранить файл после внесенных изменений.

[1] В ряде ОС символ «+» может не восприниматься, и строка будет считаться некорректной.

Примечание. ЕЦУ Dallas Lock для связи с модулем СЗИ 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 «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 и выбрать пункт «Удаленное развертывание DL Linux».
4. В открывшемся окне добавить целевые ТС в список для удаленных операций. Для этого заполнить поля «Port» и «Введите IP адрес или сетевое имя компьютера» и далее нажать кнопку «Добавить адрес» (рис. 133).

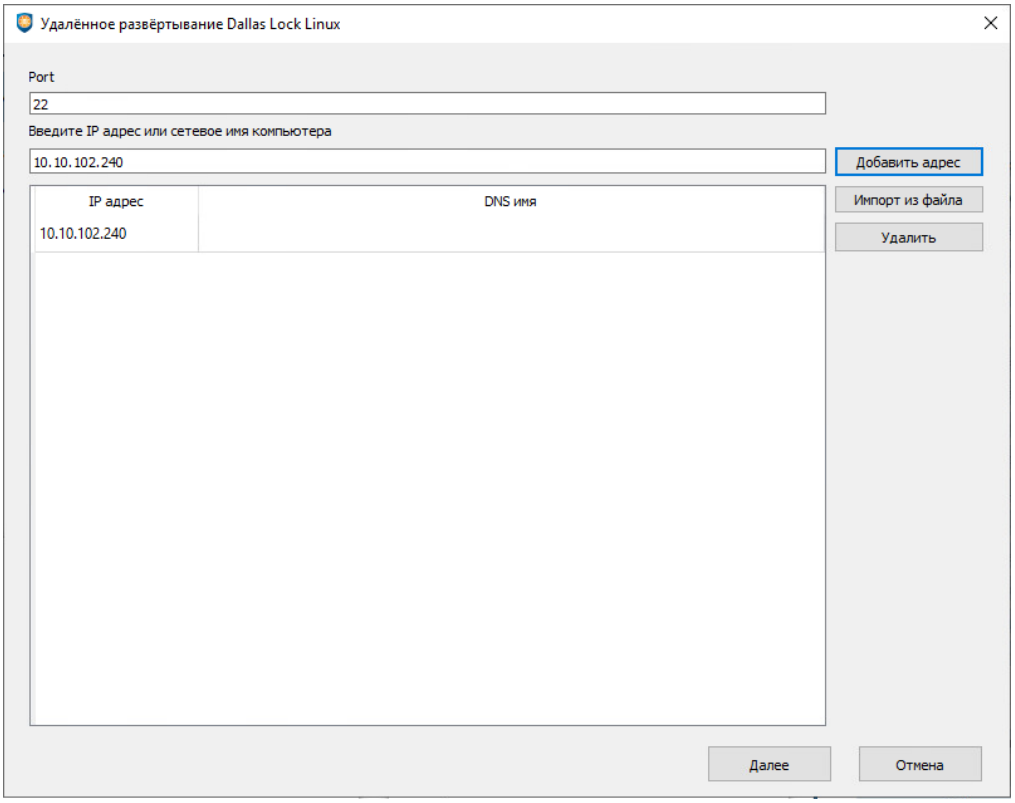

Рис. 133. Список целевых ТС для удаленного развертывания СЗИ НСД Dallas Lock Linux

После добавления целевых ТС в список необходимо нажать кнопку «Далее».

5. Заполнить параметры установки, которые будут применены к модулям в процессе активации СЗИ НСД Dallas Lock Linux (рис. 134):
   - путь к установочному файлу СЗИ НСД Dallas Lock Linux;
   - номер лицензии, который указан на обложке футляра;
   - параметры для ввода модулей в Домен безопасности ЕЦУ после установки (опционально);
   - логин и пароль администратора ОС на целевых ТС;
   - логин и пароль суперпользователя (опционально).

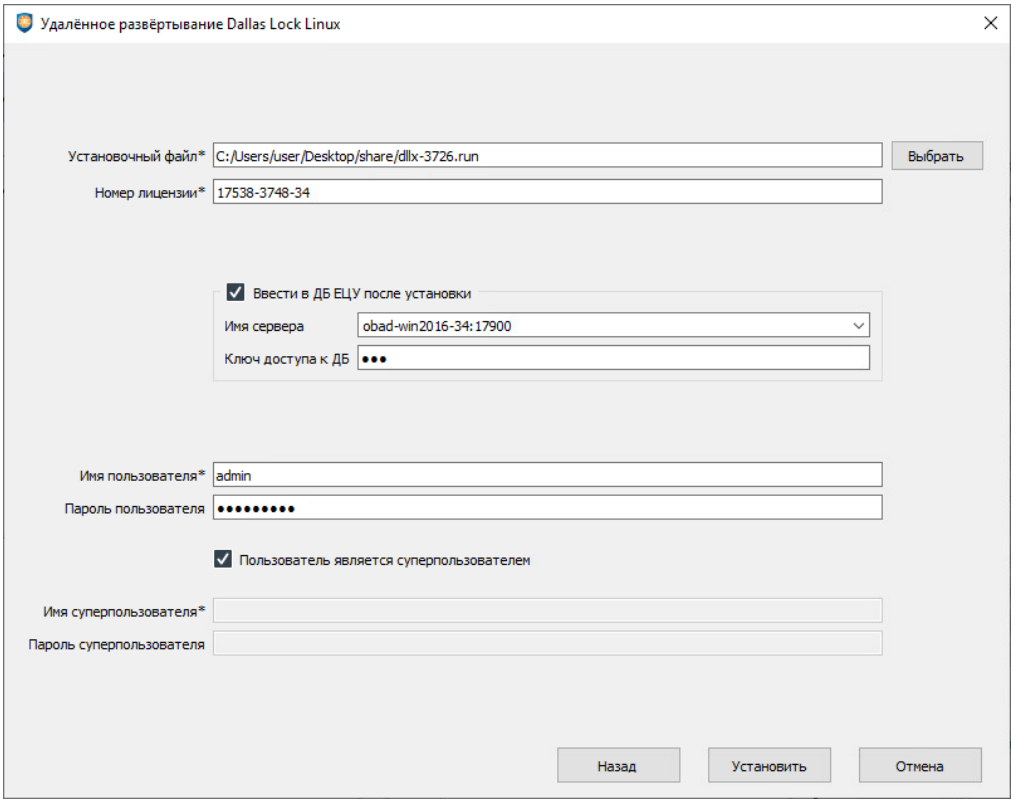

Рис. 134. Параметры установки СЗИ НСД Dallas Lock Linux

После заполнения всех необходимых полей нужно нажать кнопку «Установить».

6. Далее можно просматривать состояние процесса установки для каждого клиента (рис. 135).

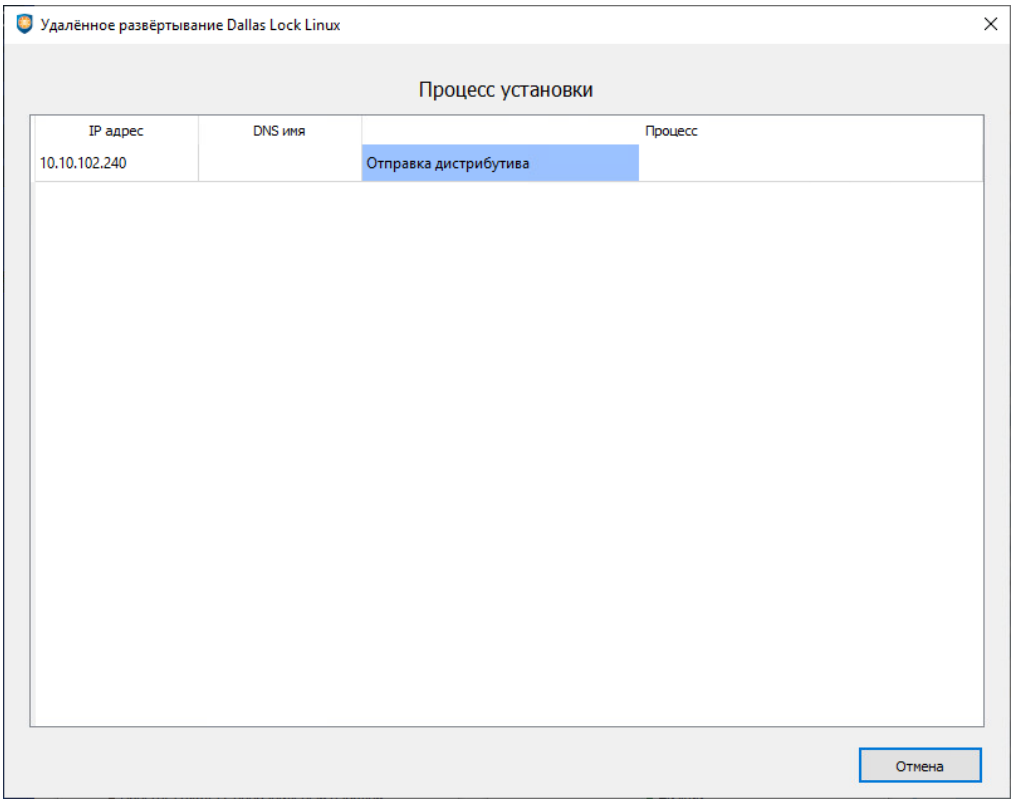

Рис. 135. Информация о ходе централизованной установки средствами ЕЦУ

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 Dallas Lock Linux

В дереве Домена безопасности ЕЦУ присутствуют зарегистрированные в ДБ модули СЗИ Dallas Lock Linux в составе АРМ.

Значки объектов, обозначающих модули СЗИ 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, на модуле СЗИ Dallas Lock Linux необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между ЕЦУ и модулем:

- при включении модуля;
- по расписанию (см. «Параметры работы модулей»);
- по команде пользователя:
  - из консоли ЕЦУ;
  - из графической оболочки модуля СЗИ Dallas Lock Linux.

Синхронизация по команде из консоли ЕЦУ

Команда «Синхронизировать» в консоли ЕЦУ для модуля СЗИ Dallas Lock Linux доступна на вкладке «Сводка» на уровне модуля в дереве Домена безопасности на панели инструментов «Оперативное управление» (рис. 136).

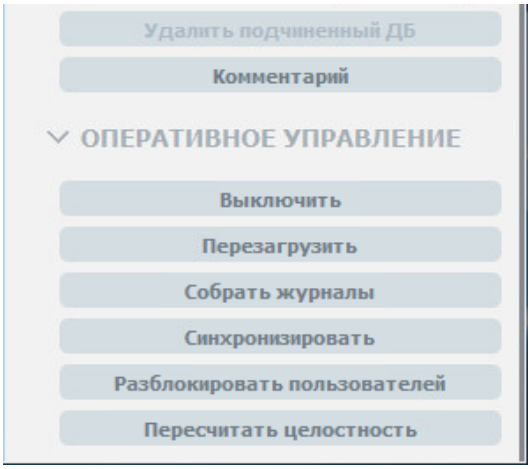

Рис. 136. Кнопка «Синхронизировать»

Синхронизация по команде из графической оболочки СЗИ Dallas Lock Linux

Для проведения синхронизации с Доменом безопасности ЕЦУ по команде из графической оболочки модуля СЗИ Dallas Lock Linux на клиентском ПК необходимо выполнить следующие шаги:

1. запустить графическую оболочку СЗИ Dallas Lock Linux и авторизоваться;
2. перейти на вкладку «Централизованное управление»;
3. нажать кнопку «Синхронизация с ЕЦУ» (рис. 137).

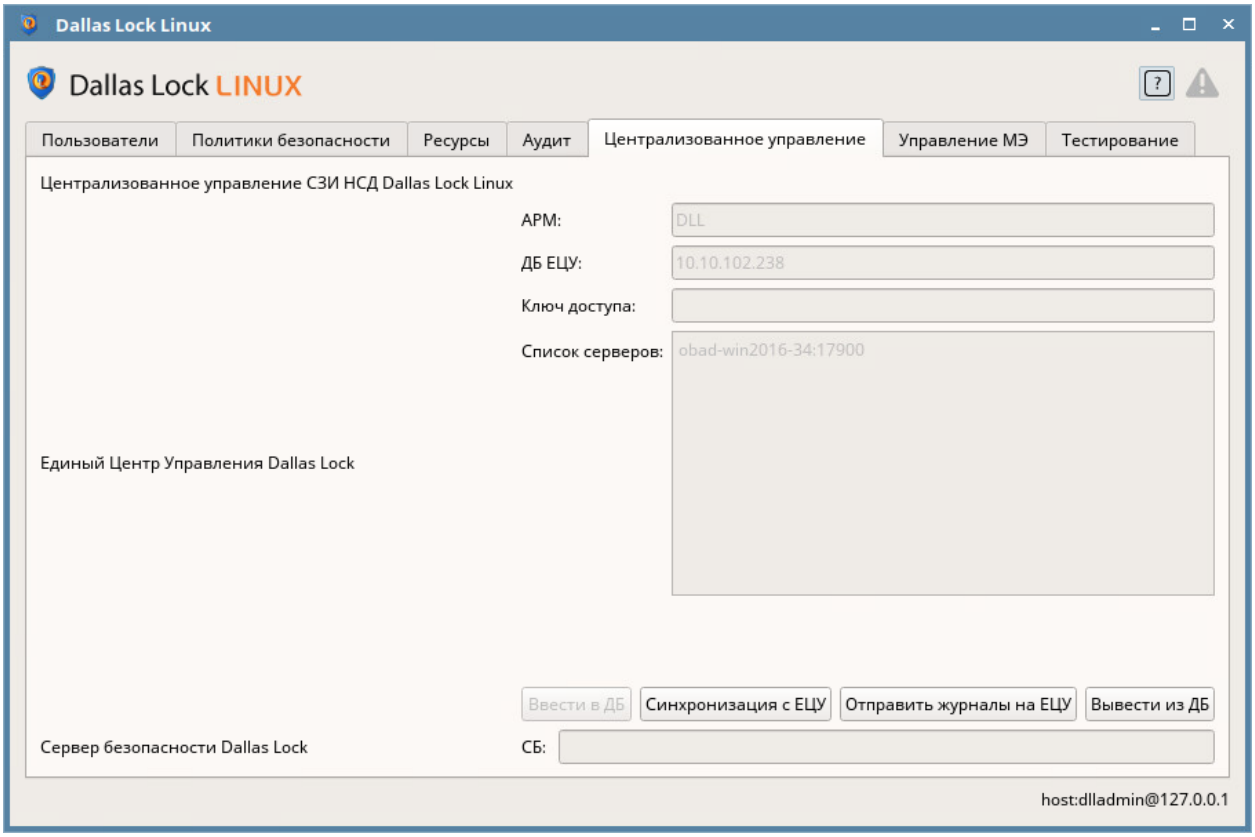

Рис. 137. Кнопка «Синхронизация с ЕЦУ»

10.4.2 Сбор журналов

Для получения в ЕЦУ записей журналов, ведущихся на модуле СЗИ Dallas Lock Linux, необходимо проведение сбора журналов. Сбор журналов может быть проведен при условии наличия сетевого подключения между ЕЦУ и модулем:

- при включении модуля;
- по расписанию (см. «Параметры работы модулей»);
- по команде пользователя:
  - из консоли ЕЦУ;
  - из графической оболочки модуля СЗИ Dallas Lock Linux.

Сбор журналов по команде из консоли ЕЦУ

Команда «Собрать журналы» в консоли ЕЦУ для модуля СЗИ Dallas Lock Linux доступна на вкладке «Сводка» на уровне модуля в дереве Домена безопасности на панели инструментов «Оперативное управление» (рис. 138).

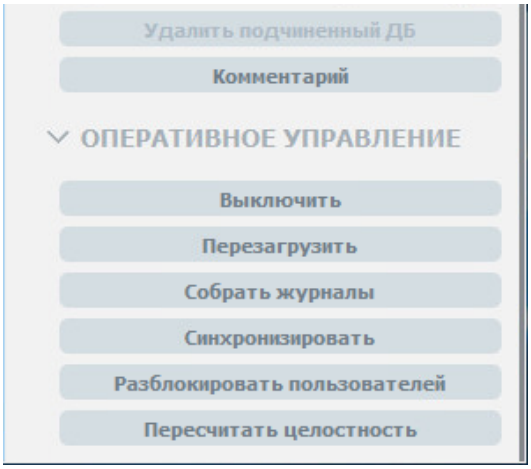

Рис. 138. Кнопка «Собрать журналы»

Отправка журналов по команде из графической оболочки администратора

Для отправки журналов в Доменом безопасности ЕЦУ по команде из графической оболочки модуля СЗИ Dallas Lock Linux на клиентском ПК необходимо выполнить следующие шаги:

1. запустить графическую оболочку СЗИ Dallas Lock Linux и авторизоваться;
2. перейти на вкладку «Централизованное управление»;
3. нажать кнопку «Отправить журналы на ЕЦУ» (рис. 139).

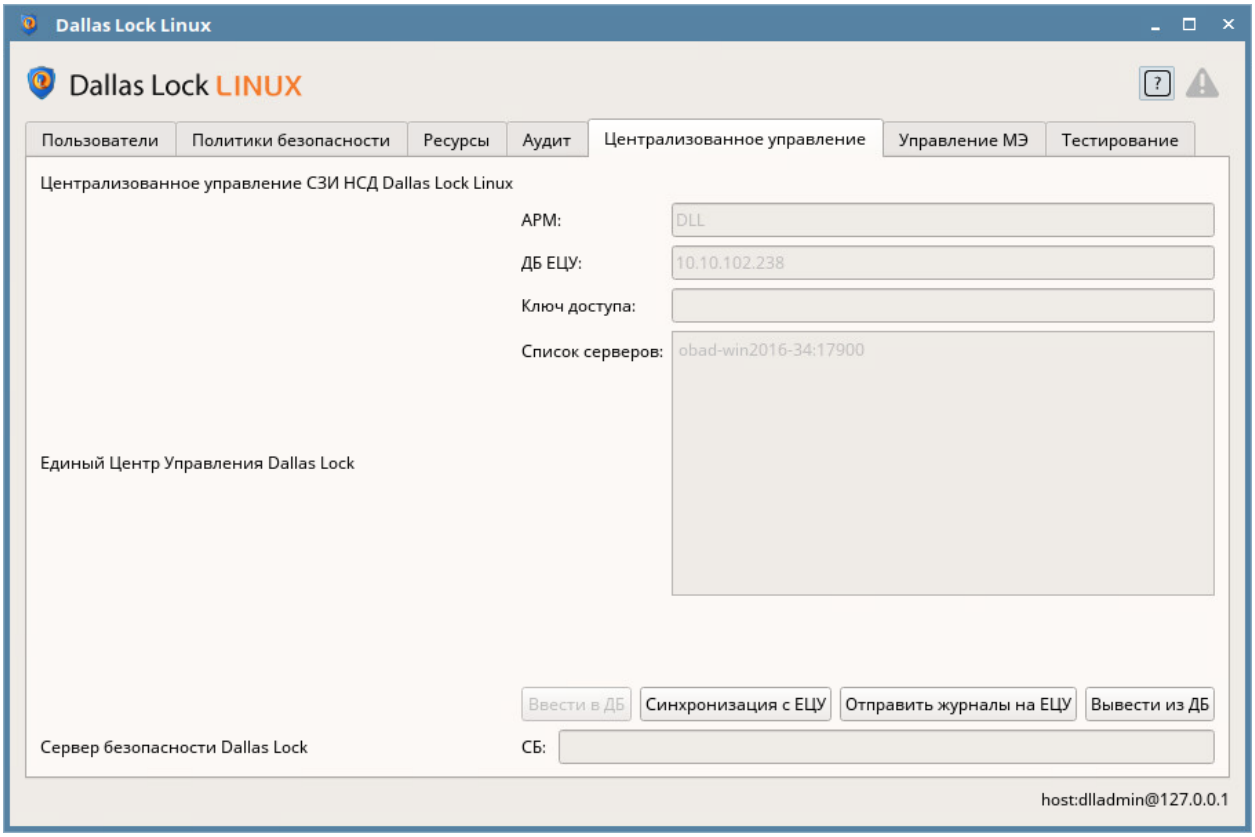

Рис. 139. Кнопка «Отправить журналы на ЕЦУ»

10.4.3 Сводка модуля СЗИ Dallas Lock Linux

Вкладка «Сводка» на уровне модуля СЗИ Dallas Lock Linux отображает общее состояние модуля (рис. 140).

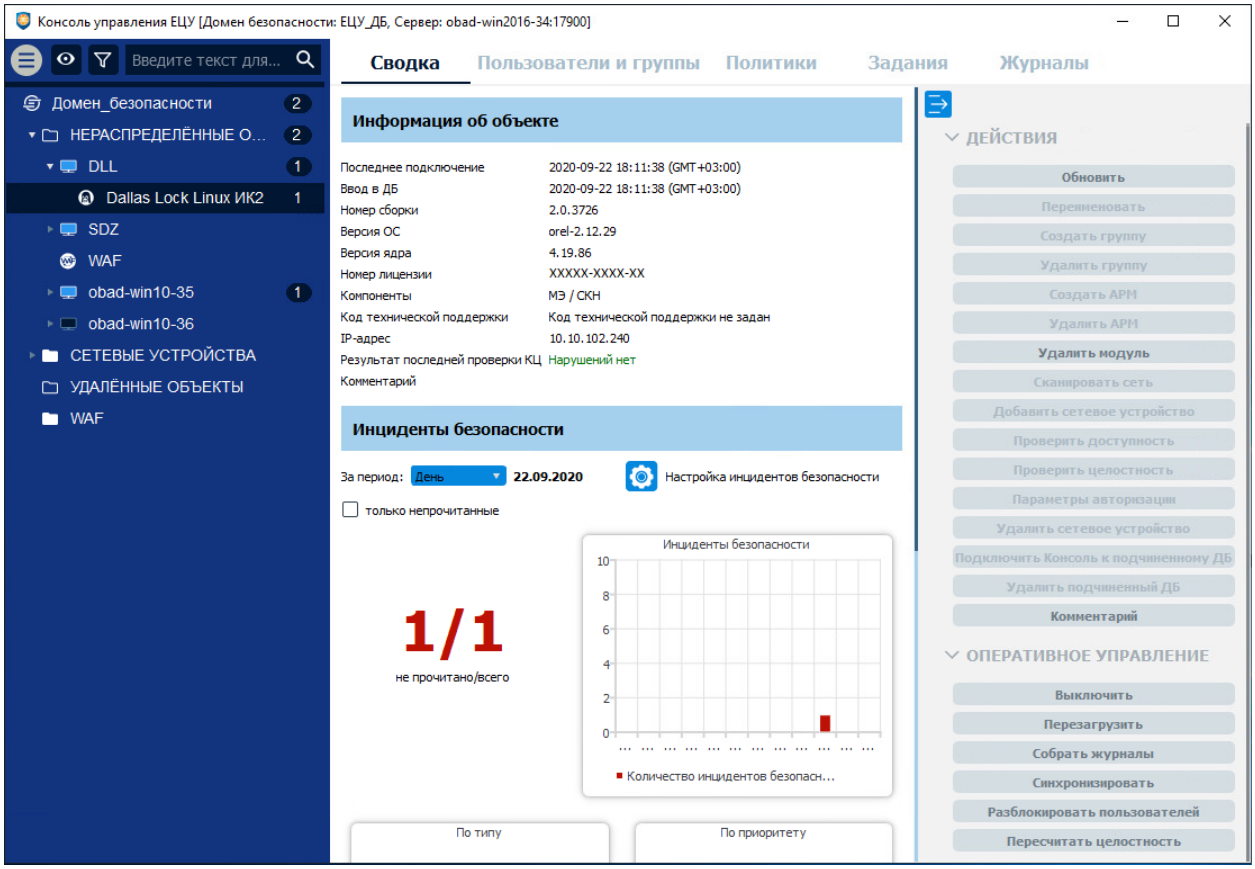

Рис. 140. Вкладка «Сводка»

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; • номер лицензии; • компоненты; • код технической поддержки; • IP-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;
5. собрать журналы;
6. синхронизировать.

10.4.4 Пользователи и группы модуля СЗИ Dallas Lock Linux

Вкладка «Пользователи и группы» на уровне модуля СЗИ 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 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 Dallas Lock Linux

На уровне модуля СЗИ Dallas Lock Linux в списке на вкладе «Политики» доступны только политики, актуальные для СЗИ 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 Dallas Lock Linux

На уровне модуля СЗИ Dallas Lock Linux в списке на вкладе «Задания» доступны для создания только задания, актуальные для СЗИ Dallas Lock Linux (рис. 141):

- изменение параметров лицензии (изменяет номер лицензии и код технической поддержки).

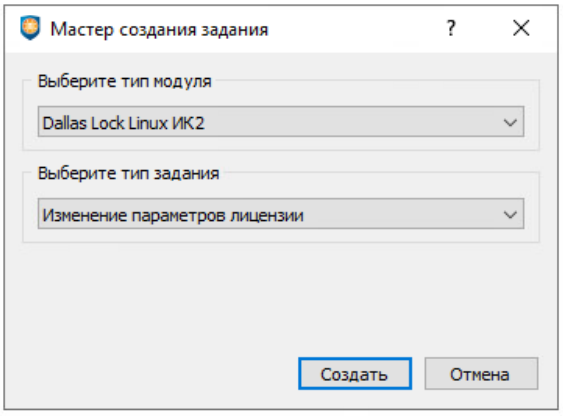

Рис. 141. Мастер создания задания для модуля СЗИ Dallas Lock Linux

Работа с заданиями для модуля СЗИ 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 Dallas Lock Linux

Вкладка «Журналы» для модуля СЗИ Dallas Lock Linux позволяет просматривать журналы безопасности модуля (рис. 142).

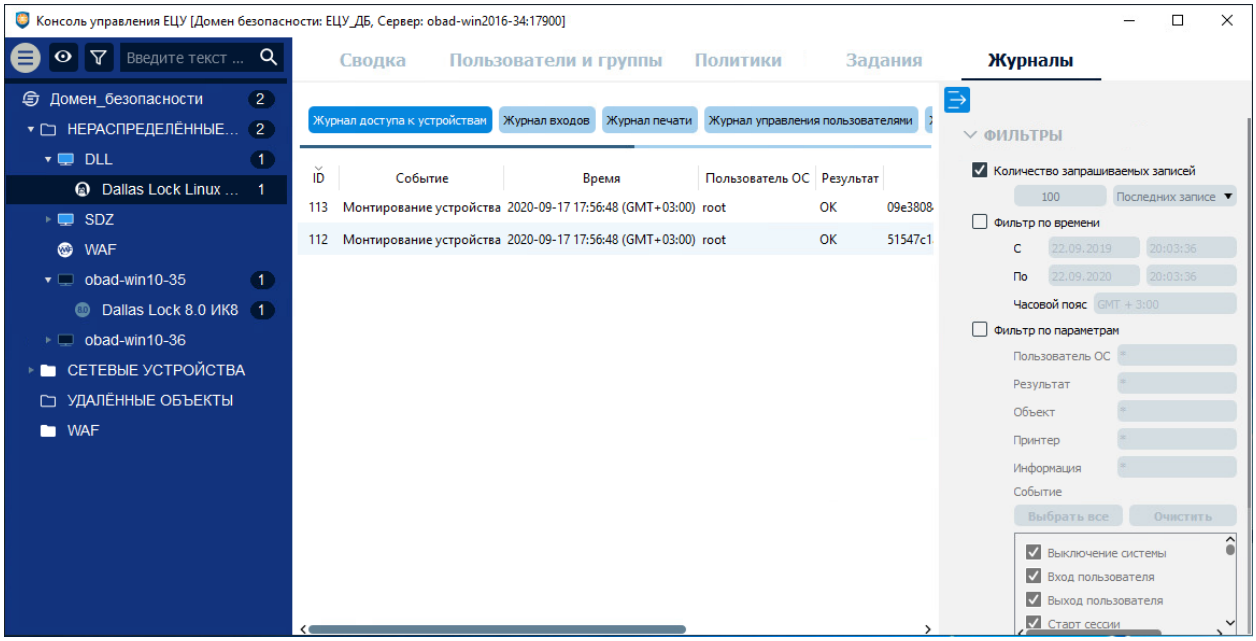

Рис. 142. Вкладка «Журналы»

Для модуля СЗИ Dallas Lock Linux доступны:

- «Журнал доступа к устройствам»;
- «Журнал входов»;
- «Журнал печати»;
- «Журнал управления пользователями»;
- «Журнал управления политиками безопасности»;
- «Системный журнал»;
- «Журнал доступа к ресурсам».

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:

1. в ЛВС должен быть работающий сервер ЕЦУ;
2. 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 значения параметров безопасности подлежат синхронизации со значениями политик ЕЦУ 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, подключиться к Центру управления СЗИ ВИ;
3. выбрать в дереве объектов вкладку «Агенты ВИ»;
4. перейти в категорию «Состояние» и нажать кнопку «Ввод в ЕЦУ» (рис. 143);

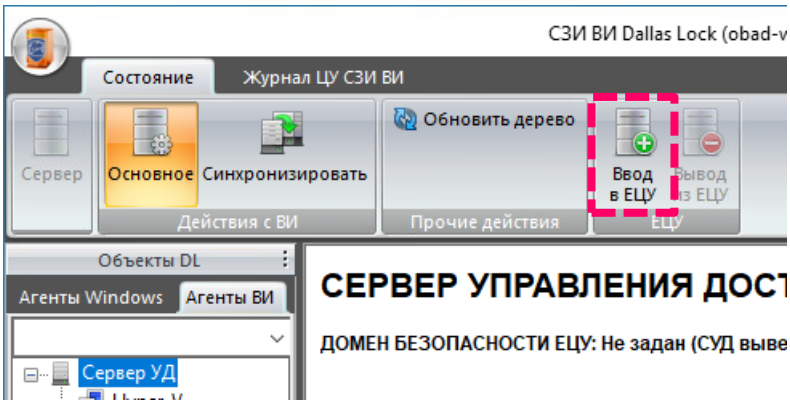

Рис. 143. Ввод в ЕЦУ

5. указать в появившемся окне «Ввод в ЕЦУ» следующие данные (рис. 144):
   - DNS-имя или IP-адрес сервера ЕЦУ;
   - имя АРМ, в составе которого необходимо ввести модуль;
   - ключ доступа к ДБ;

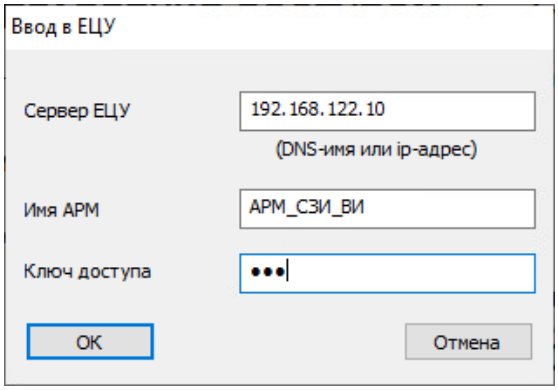

Рис. 144. Окно «Ввод в ЕЦУ»

6. нажать кнопку «ОК», и будет инициировано создание АРМ и регистрация модуля в его составе (рис. 145).

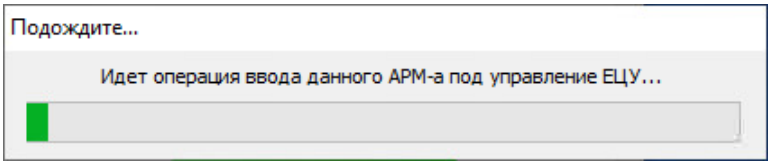

Рис. 145. Операция ввода АРМ под управление ЕЦУ

Если процесс ввода модуля в ДБ прошел успешно, то через некоторое время появится соответствующее сообщение (рис. 146).

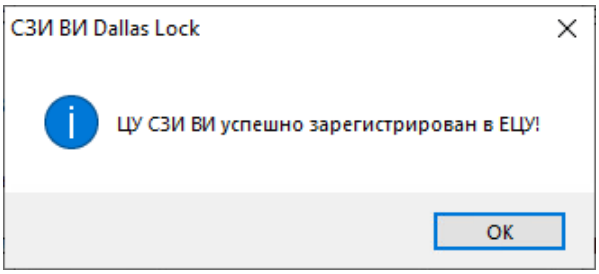

Рис. 146. Модуль зарегистрирован в ЕЦУ

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 (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. выбрать в дереве объектов вкладку «Агенты ВИ»;
3. перейти в категорию «Состояние»;
4. нажать кнопку «Вывод из ЕЦУ» (рис. 147);

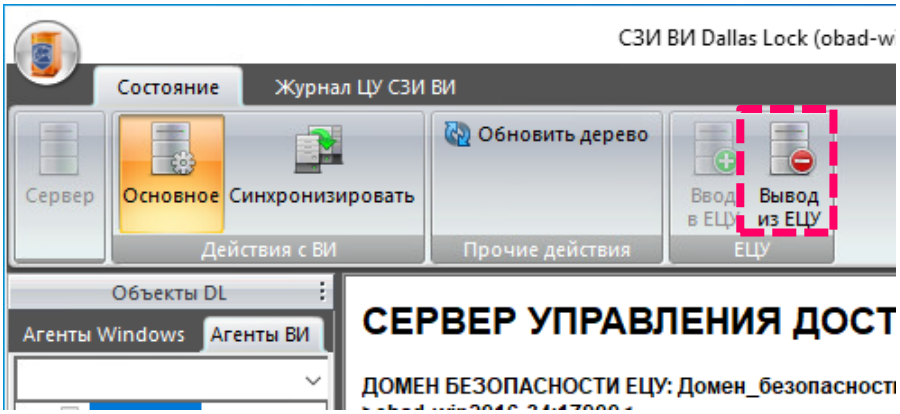

Рис. 147. Вывод из ЕЦУ

5. в появившемся диалоговом окне нажать кнопку «Да» (рис. 148).

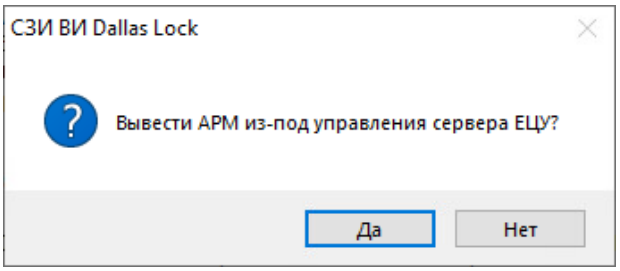

Рис. 148. Вывод АРМ из-под управления сервера ЕЦУ

Если процесс вывода модуля из ДБ прошел успешно, то через некоторое время появится сообщение о том, что АРМ (модули Dallas Lock СЗИ ВИ и Агент управления доступом) выведен из ДБ (рис. 149).

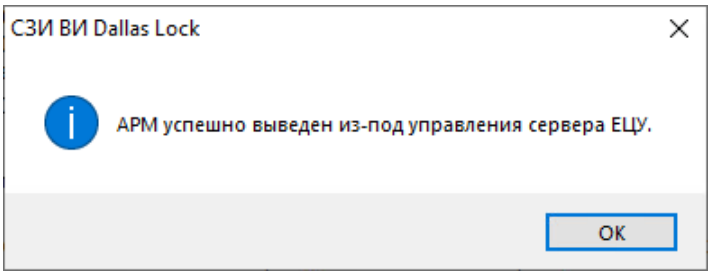

Рис. 149. Модули СЗИ ВИ выведены из ДБ ЕЦУ

В консоли ЕЦУ удаленный модуль переместится в базовую группу «Удаленные объекты» дерева ДБ.

11.3 Настройка СЗИ ВИ Dallas Lock

В дереве Домена безопасности ЕЦУ присутствуют зарегистрированные в ДБ модули СЗИ ВИ Dallas Lock, которые отображаются в качестве двух отдельных модулей в составе АРМ:

- Dallas Lock СЗИ ВИ — компонент Центра управления СЗИ ВИ Dallas Lock, обеспечивающий централизованное управление объектами виртуальной инфраструктуры и защиту серверов виртуализации;
- Агент управления доступом — компонент СЗИ ВИ Dallas Lock, обеспечивающий защиту технических средств, на которые установлен.

Значки объектов, обозначающих модули СЗИ ВИ Dallas Lock, зависят от состояния модуля и могут принимать следующий вид:

Dallas Lock СЗИ ВИ	**Агент управления доступом**	
		— 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, на модуле СЗИ ВИ Dallas Lock необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между ЕЦУ и модулем:

- при включении модуля;
- по расписанию (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. 149).

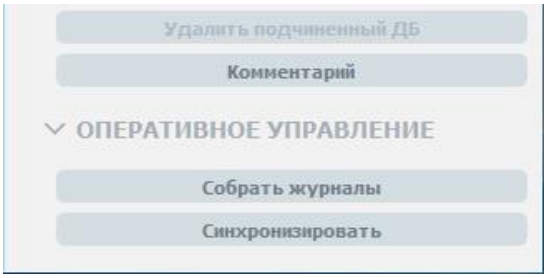

Рис. 150. Кнопка «Синхронизировать»

Синхронизация по команде из Консоли Центра управления СЗИ ВИ Dallas Lock

Для проведения синхронизации с Доменом безопасности ЕЦУ 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. 151).

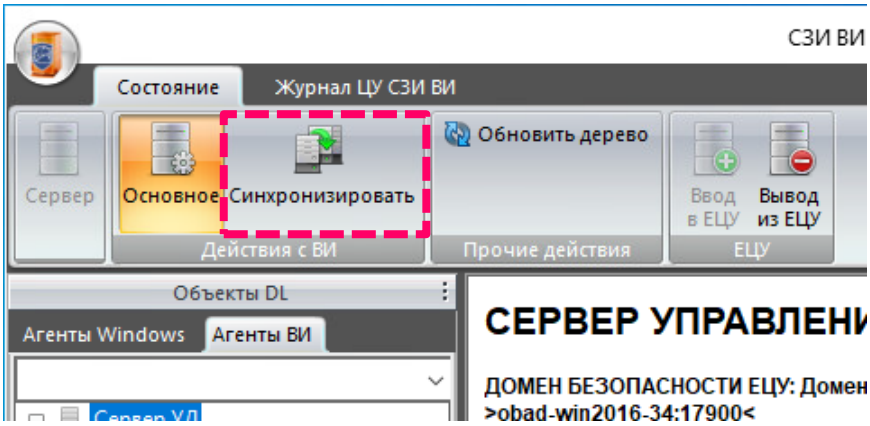

Рис. 151. Кнопка «Синхронизировать»

11.3.2 Сбор журналов

Для получения в ЕЦУ 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;
- по расписанию (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 и Агент управления доступом доступна на вкладке «Сводка» на уровне модуля в дереве ДБ на панели инструментов «Оперативное управление» (рис. 152).

Рис. 152. Кнопка «Собрать журналы»

11.3.3 Сводка модуля Dallas Lock СЗИ ВИ

Вкладка «Сводка» на уровне модуля Dallas Lock СЗИ ВИ отображает общее состояние модуля (рис. 153).

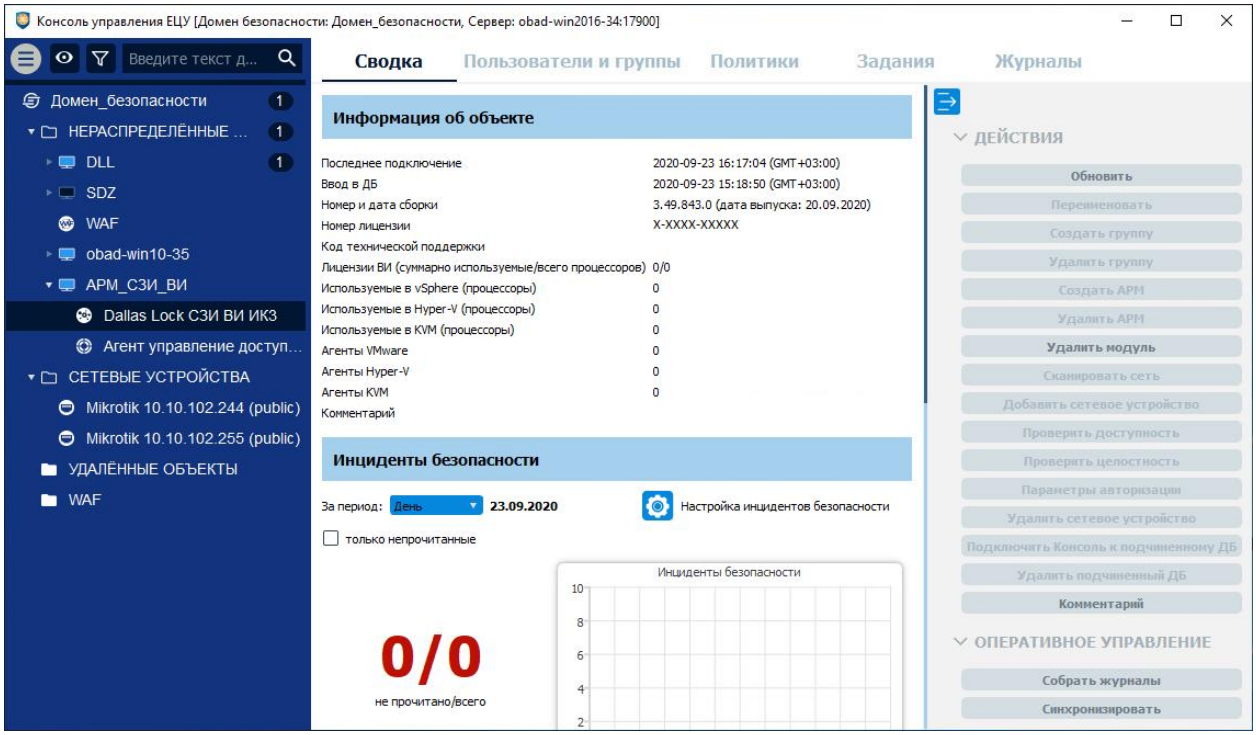

Рис. 153. Вкладка «Сводка»

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;
• 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; • 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» доступны только политики, актуальные для Dallas Lock СЗИ ВИ (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.

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. 154):

- изменение параметров лицензии;
- получение конфигурации;
- получение отчета о конфигурации;
- применение конфигурации;
- проверка обновлений.

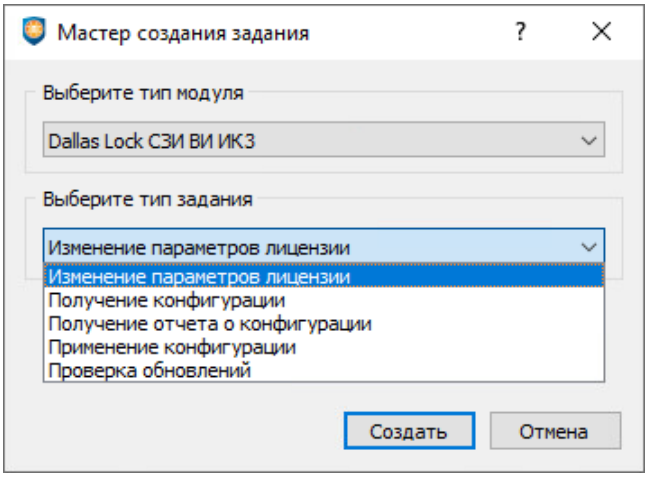

Рис. 154. Мастер создания задания для модуля Dallas Lock СЗИ ВИ

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. 155).

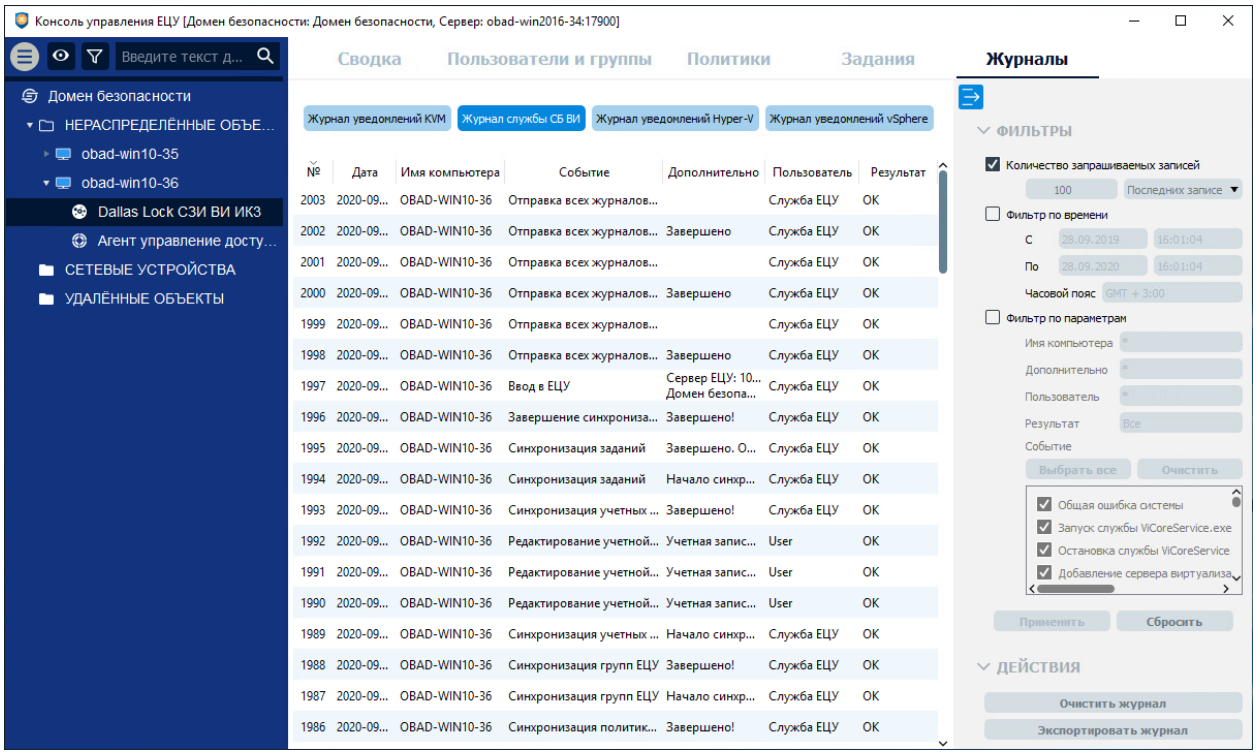

Рис. 155. Вкладка «Журналы»

Для модуля Dallas Lock СЗИ ВИ доступны:

- «Журнал уведомлений KVM»;
- «Журнал службы СБ 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.

11.3.8 Сводка модуля Агент управления доступом

Вкладка «Сводка» на уровне модуля Агент управления доступом отображает общее состояние модуля (рис. 156).

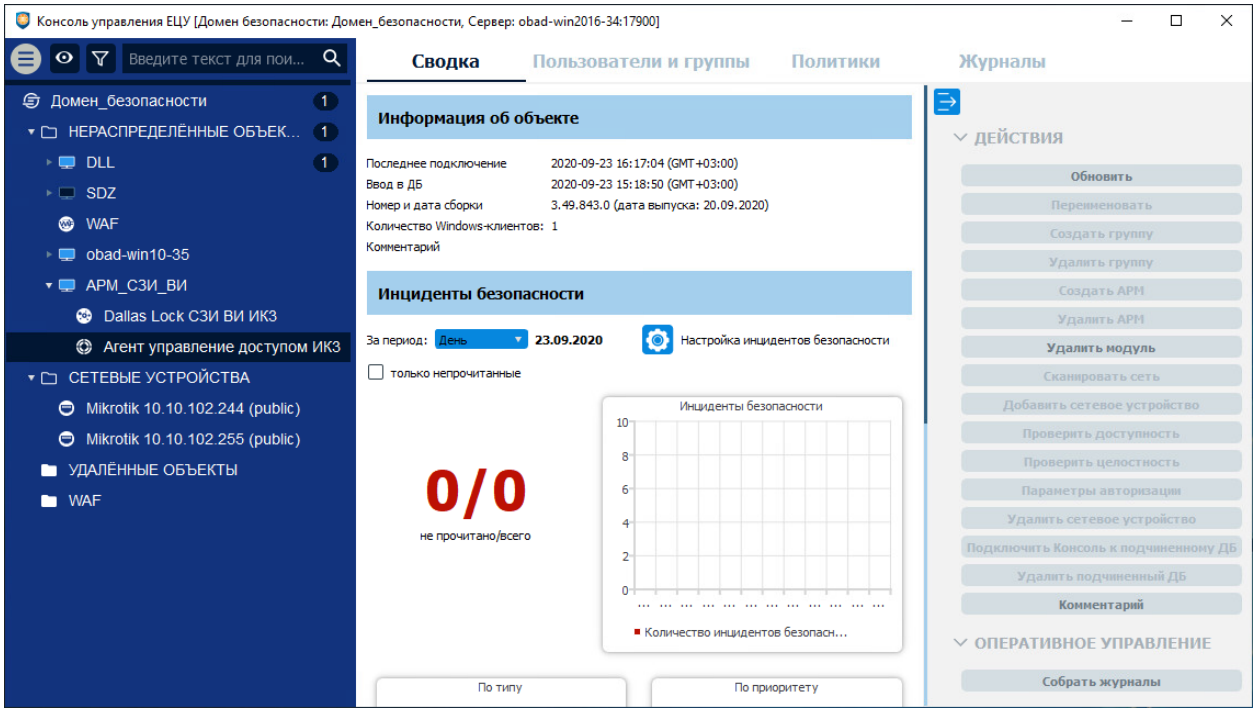

Рис. 156. Вкладка «Сводка»

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; • информация о дате и времени ввода модуля в ДБ; • номер и дата сборки; • количество Windows-клиентов; • 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. собрать журналы.

11.3.9 Пользователи и группы модуля Агент управления доступом

Вкладка «Пользователи и группы» на уровне модуля Агент управления доступом 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 Агент управления доступом производится аналогично описанному управлению пользователями и группами в разделе «Пользователи и группы модуля». Для применения изменений на модулях необходима синхронизация.

11.3.10 Политики модуля Агент управления доступом

На уровне модуля Агент управления доступом в списке на вкладе «Политики» доступны только политики, актуальные для Агента управления доступом (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.

11.3.11 Журналы модуля Агент управления доступом

Вкладка «Журналы» для модуля Агент управления доступом позволяет просматривать журналы безопасности модуля (рис. 157).

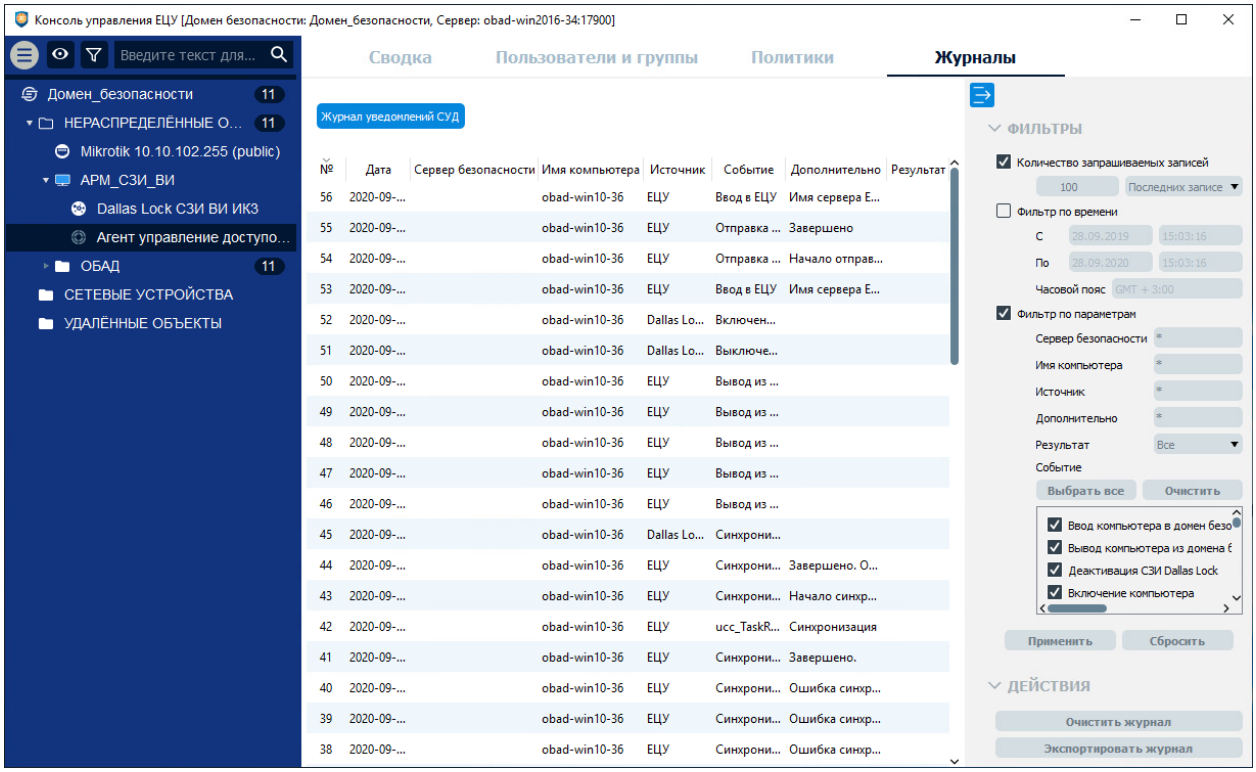

Рис. 157. Вкладка «Журналы»

Для модуля Агент управления доступом доступен «Журнал уведомлений СУД».
Работа с журналами модулей описана в разделе «Журналы модуля».
Для получения записей журнала 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:

1. в ЛВС должен быть работающий сервер ЕЦУ;
2. 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 значения политик безопасности подлежат синхронизации со значениями политик ЕЦУ 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. 158).

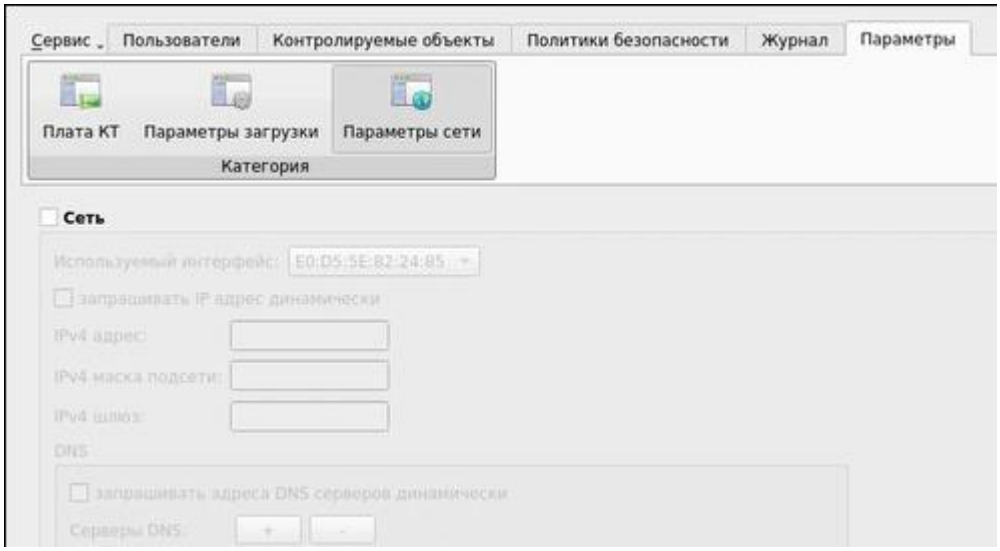

Рис. 158. Вкладка «Параметры сети» модуля СДЗ Dallas Lock

5. Поставить чекбокс в поле «Сеть», после чего станут доступны для редактирования другие поля страницы.
6. Заполнить вручную необходимые сетевые параметры или же поставить чекбокс в поле «запрашивать IP адрес динамически» для автоматического назначения сетевых параметров DHCP-сервером (рис. 159). Нажать кнопку «Применить».

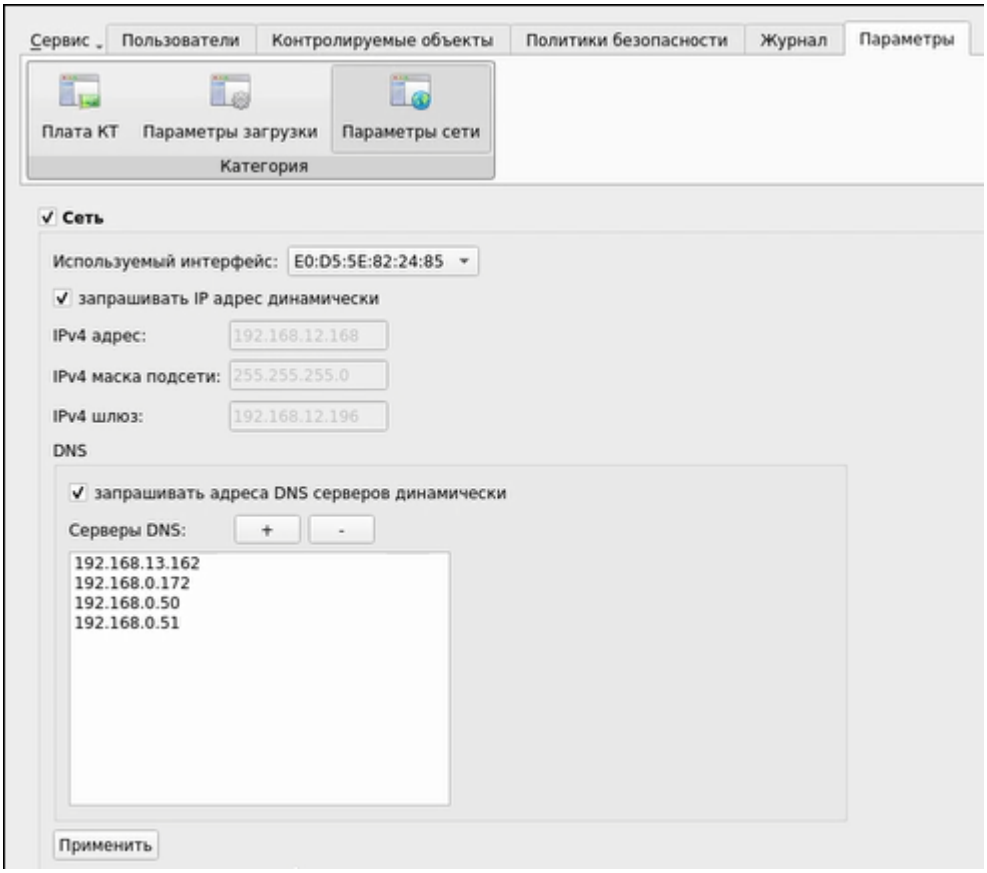

Рис. 159. Заполненные сетевые параметры

7. Заполнить параметры ввода в ДБ на панели «Централизованное управление» (рис. 160):
   - выбрать «Единый Центр Управления»;
   - указать имя АРМ, в составе которого необходимо ввести модуль;
   - указать сетевой адрес сервера ЕЦУ;
   - ввести ключ доступа к ДБ.

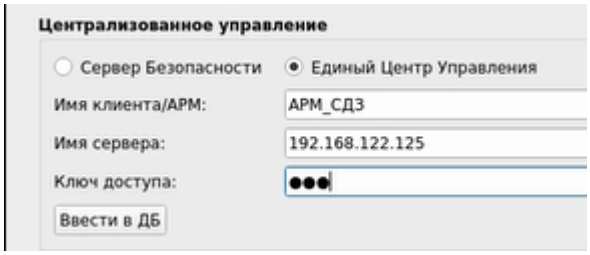

Рис. 160. Централизованное управление

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. 161).

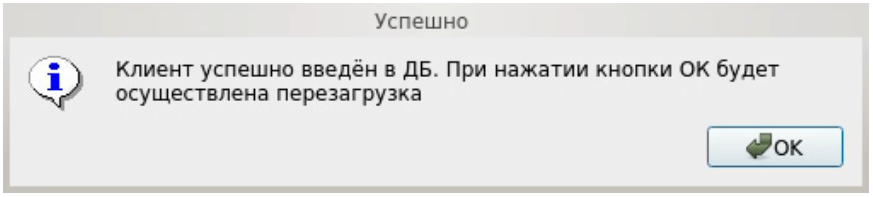

Рис. 161. Сообщение об успешном вводе модуля в ДБ

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. 162).

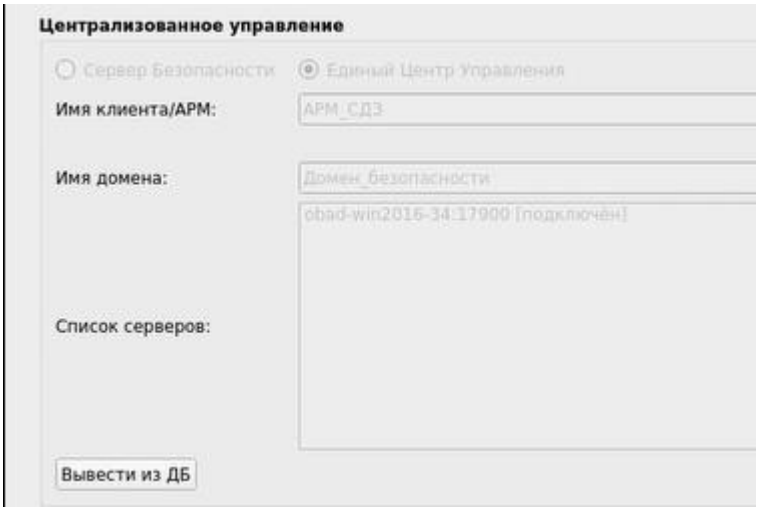

Рис. 162. Вывод модуля СДЗ посредством оболочки администратора

5. Если процесс вывода модуля из ДБ прошел успешно, то через некоторое время появится соответствующее сообщение (рис. 163).

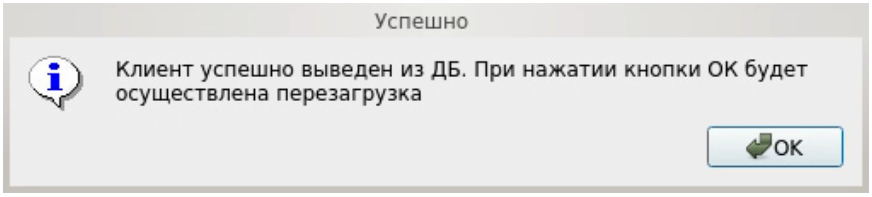

Рис. 163. Сообщение об успешном выводе модуля из ДБ

В консоли ЕЦУ удаленный модуль переместится в базовую группу «Удаленные объекты» при условии наличия связи с ЕЦУ. При отсутствии сетевого подключения к ЕЦУ модуль может быть выведен из Домена безопасности принудительно, при этом в консоли ЕЦУ такой модуль не будет перемещен в группу «Удаленные объекты».

12.3 Настройка модуля СДЗ Dallas Lock

В дереве Домена безопасности ЕЦУ 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 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, на модуле СДЗ Dallas Lock необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между ЕЦУ и модулем при включении модуля.

12.3.2 Сбор журналов

Для получения в ЕЦУ 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. 164).

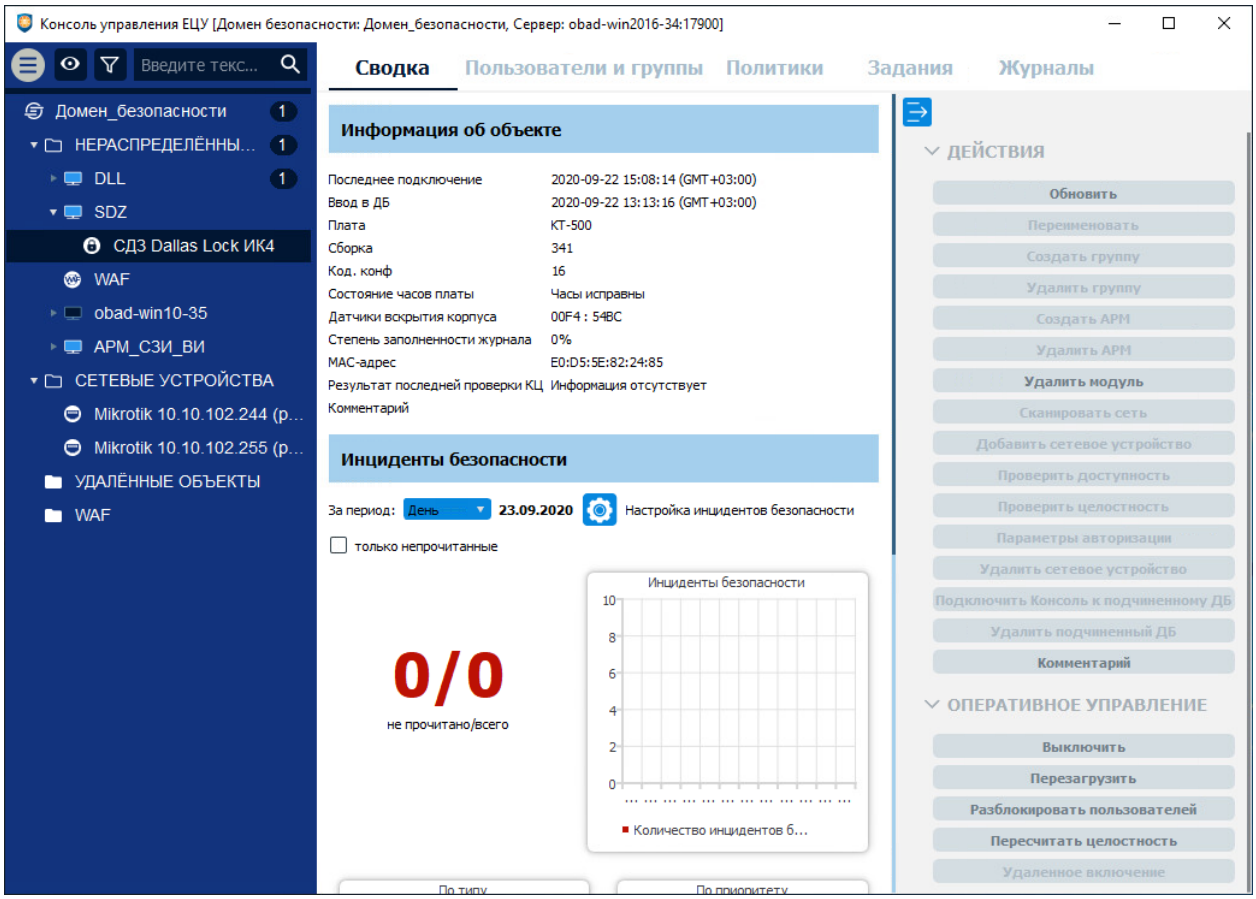

Рис. 164. Вкладка «Сводка»

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. удаленно включить;
4. разблокировать пользователей;
5. 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. 165):

- очистка журнала;
- получение конфигурации;
- получение отчета об аппаратном обеспечении;
- получение отчета по конфигурации;
- применение конфигурации.

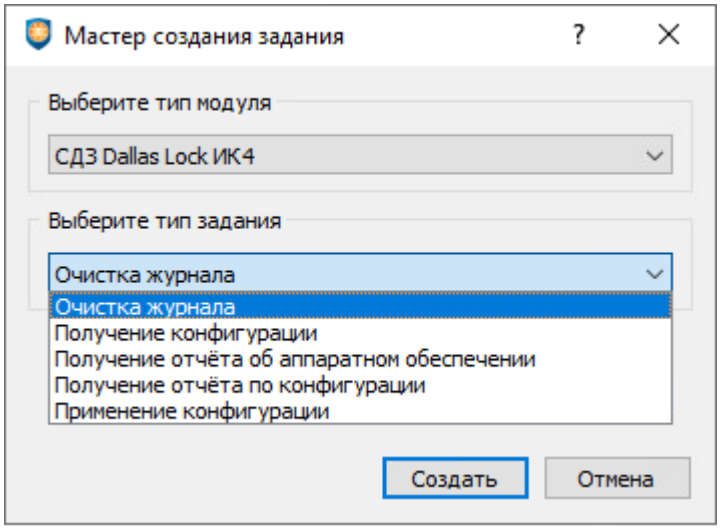

Рис. 165. Мастер создания задания для модуля СДЗ

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. 166).

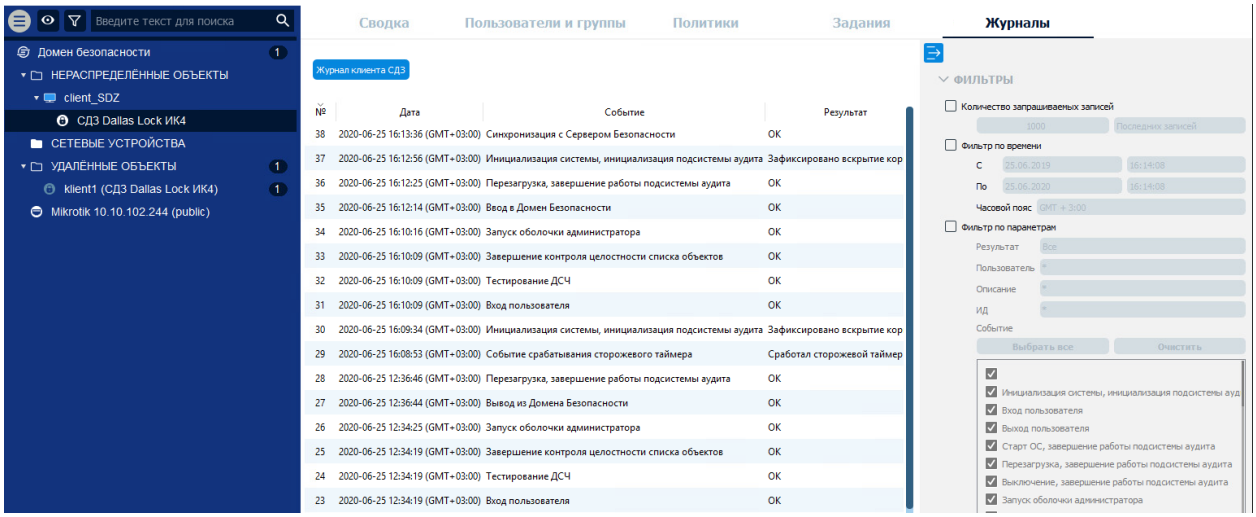

Рис. 166. Вкладка «Журналы»

Для модуля СДЗ доступен «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:

1. в ЛВС должен быть работающий сервер ЕЦУ;
2. 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. 167);

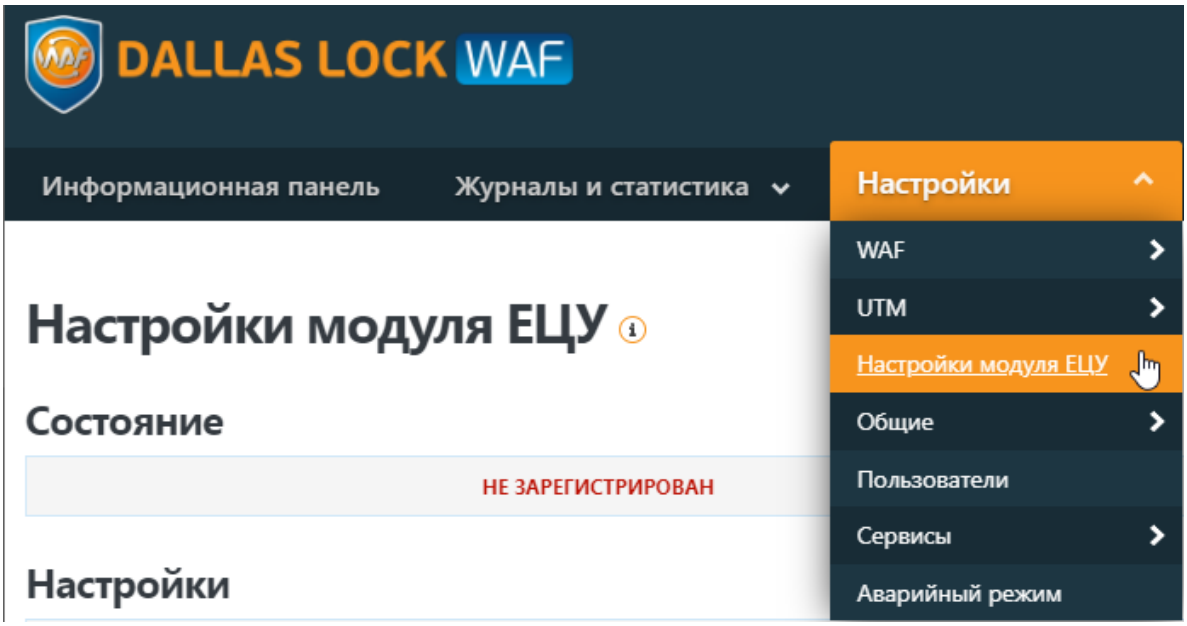

Рис. 167. Вкладка «Настройки»

4. в разделе «Настройки» заполнить параметры ввода в ДБ (рис. 168):
   - имя модуля;
   - сетевой адрес сервера ЕЦУ;
   - ключ доступа к ДБ;

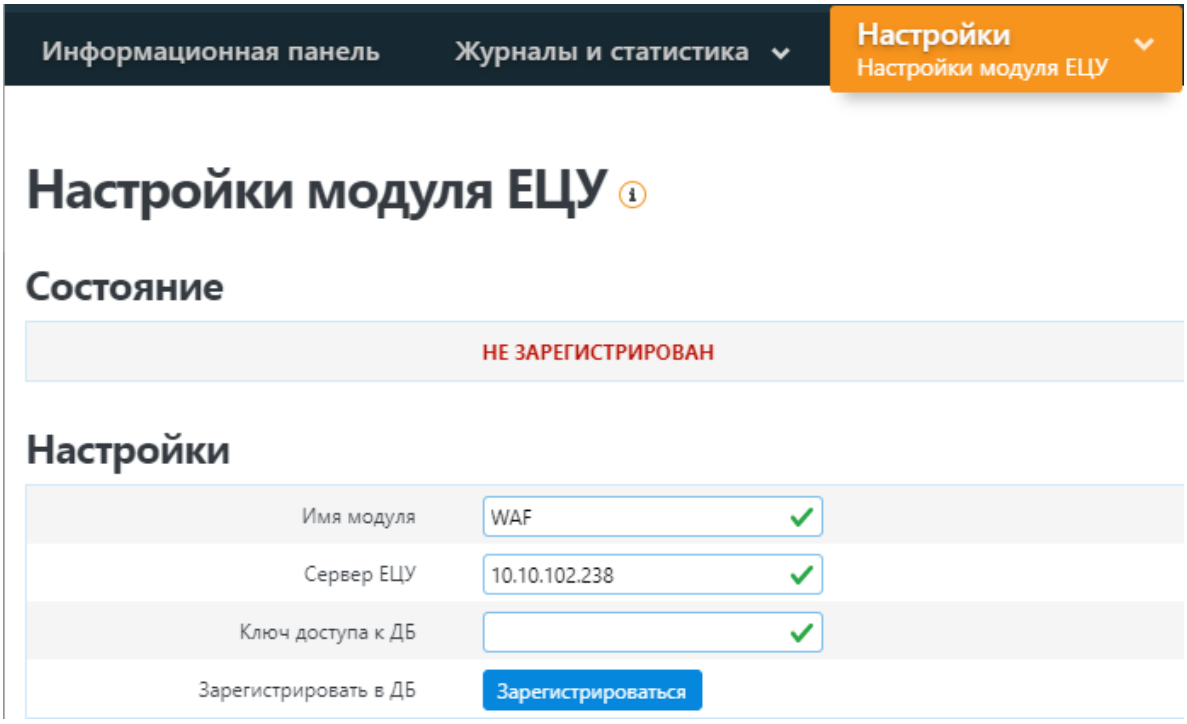

Рис. 168. Настройки модуля ЕЦУ

6. 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 (рис. 169).

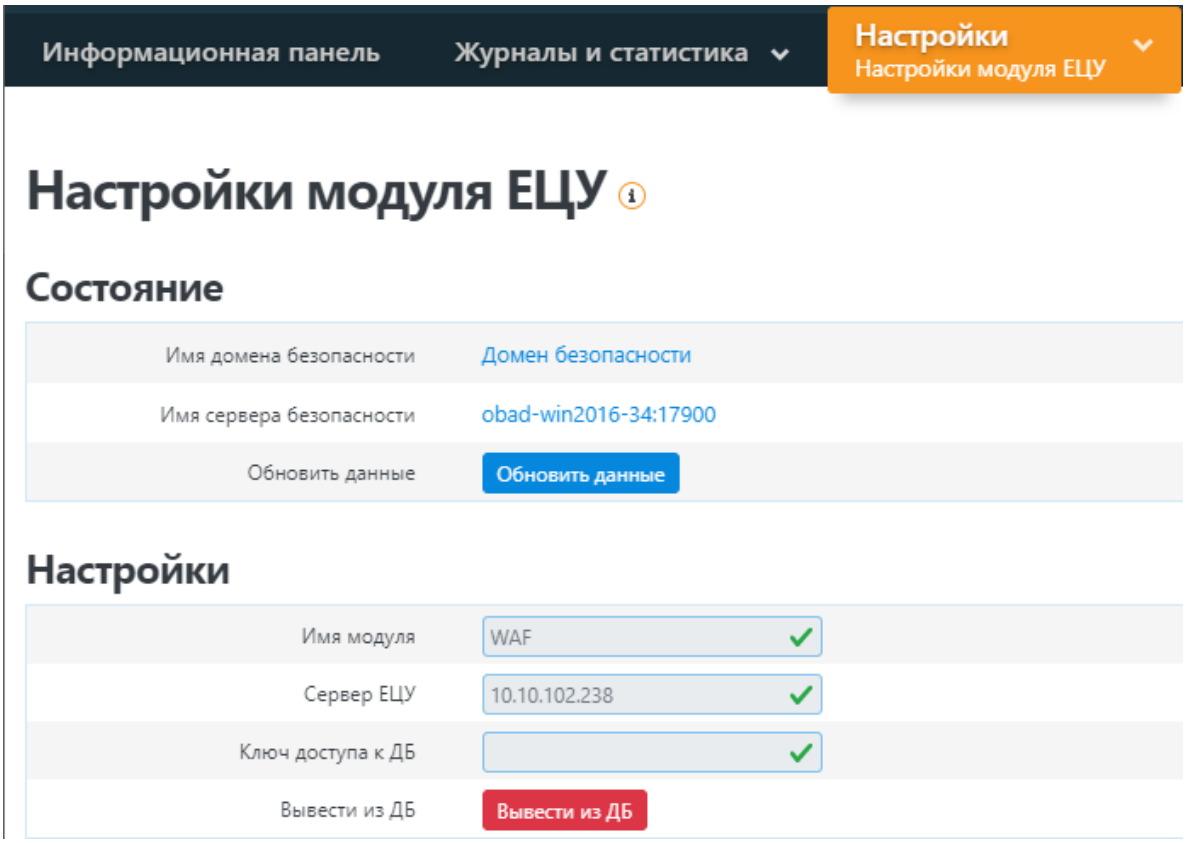

Рис. 169. Состояние

В консоли ЕЦУ в дереве ДБ в группе «Нераспределенные объекты» появится модуль WAF (без АРМ) с соответствующим именем (рис. 170).

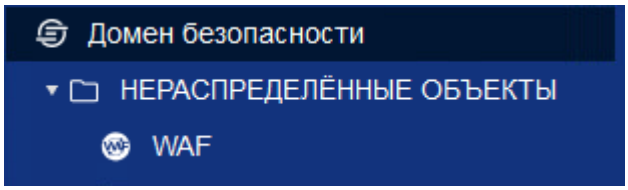

Рис. 170. Иконка модуля в дереве ДБ

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. 171);

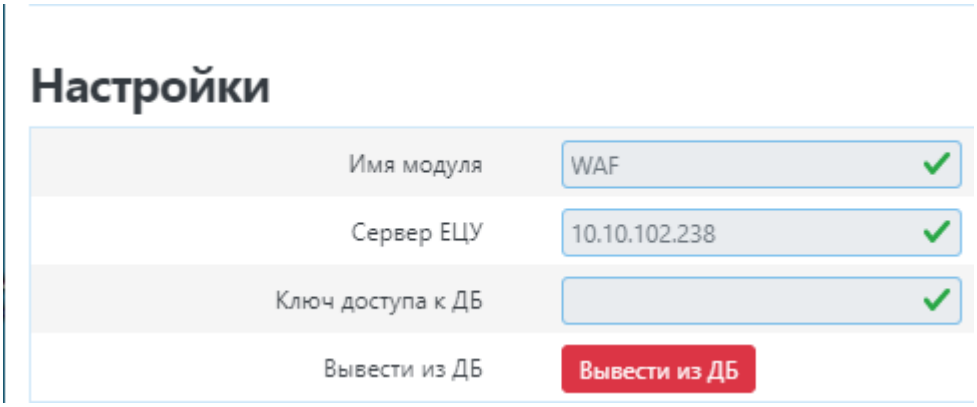

Рис. 171. Вывод из ДБ

Если процесс вывода модуля из ДБ прошел успешно, то через некоторое время поля с настройками модуля ЕЦУ станут доступными для редактирования, в разделе «Состояние» отобразится статус «НЕ ЗАРЕГИСТРИРОВАН».
В консоли ЕЦУ удаленный модуль переместится в базовую группу «Удаленные объекты» дерева ДБ.

13.3 Настройка модуля WAF Dallas Lock

В дереве Домена безопасности ЕЦУ 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.

13.3.1 Синхронизация

Для отправки на ЕЦУ 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 и модулем:

- при включении модуля;
- по расписанию (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. 172).

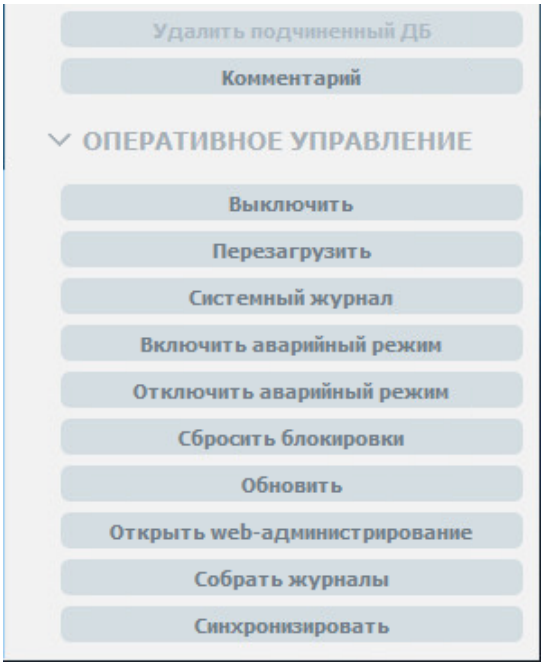

Рис. 172. Кнопка «Синхронизировать»

Синхронизация по команде из веб-интерфейса модуля WAF Dallas Lock

Для проведения синхронизации с Доменом безопасности ЕЦУ 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 данные» (рис. 173).

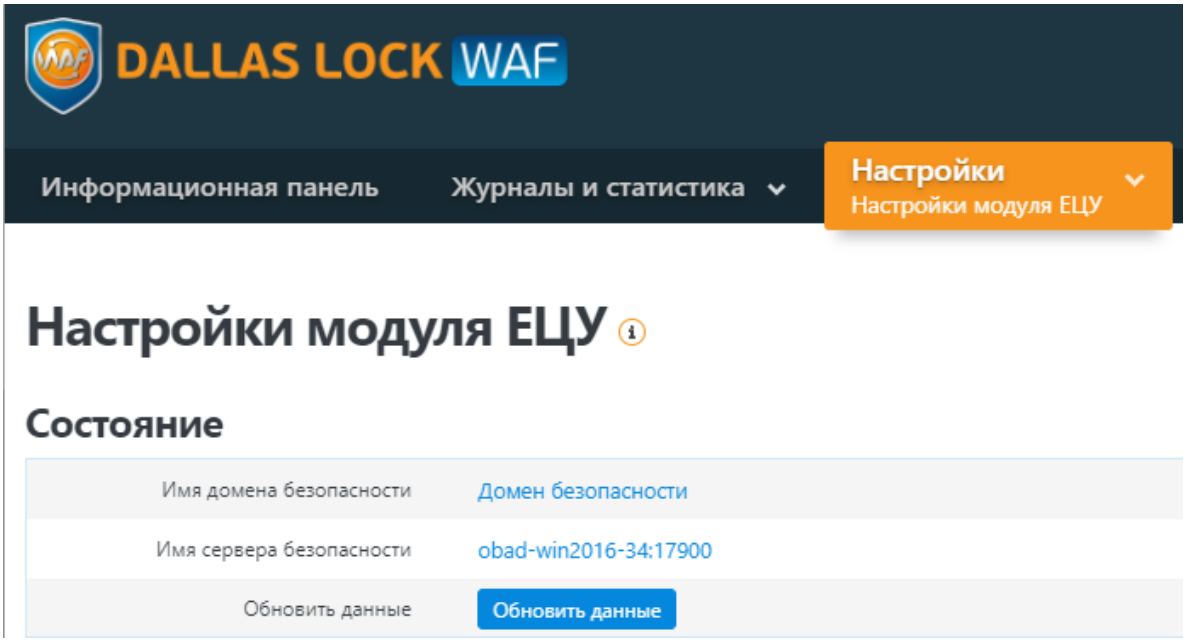

Рис. 173. Кнопка «Обновить данные»

13.3.2 Сбор журналов

Для получения в ЕЦУ записей журналов, ведущихся на модуле, необходимо проведение сбора журналов. Сбор журналов может быть проведен при условии наличия сетевого подключения между ЕЦУ и модулем:

- при включении модуля;
- по расписанию (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. 174).

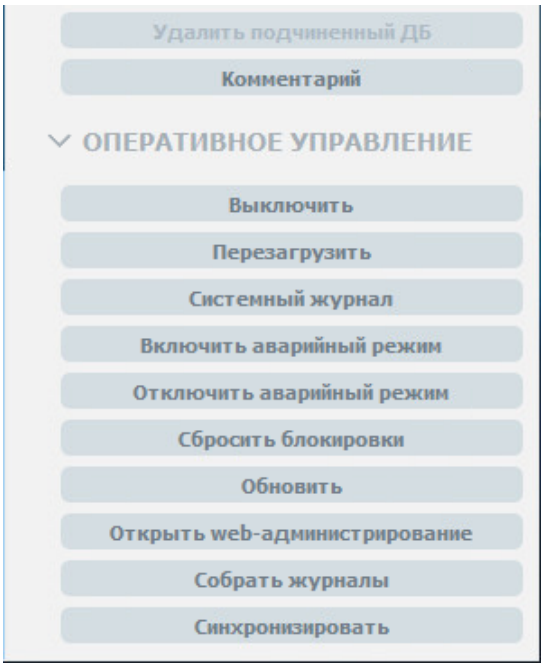

Рис. 174. Кнопка «Собрать журналы»

13.3.3 Сводка модуля WAF Dallas Lock

Вкладка «Сводка» на уровне модуля WAF Dallas Lock отображает общее состояние модуля (рис. 175).

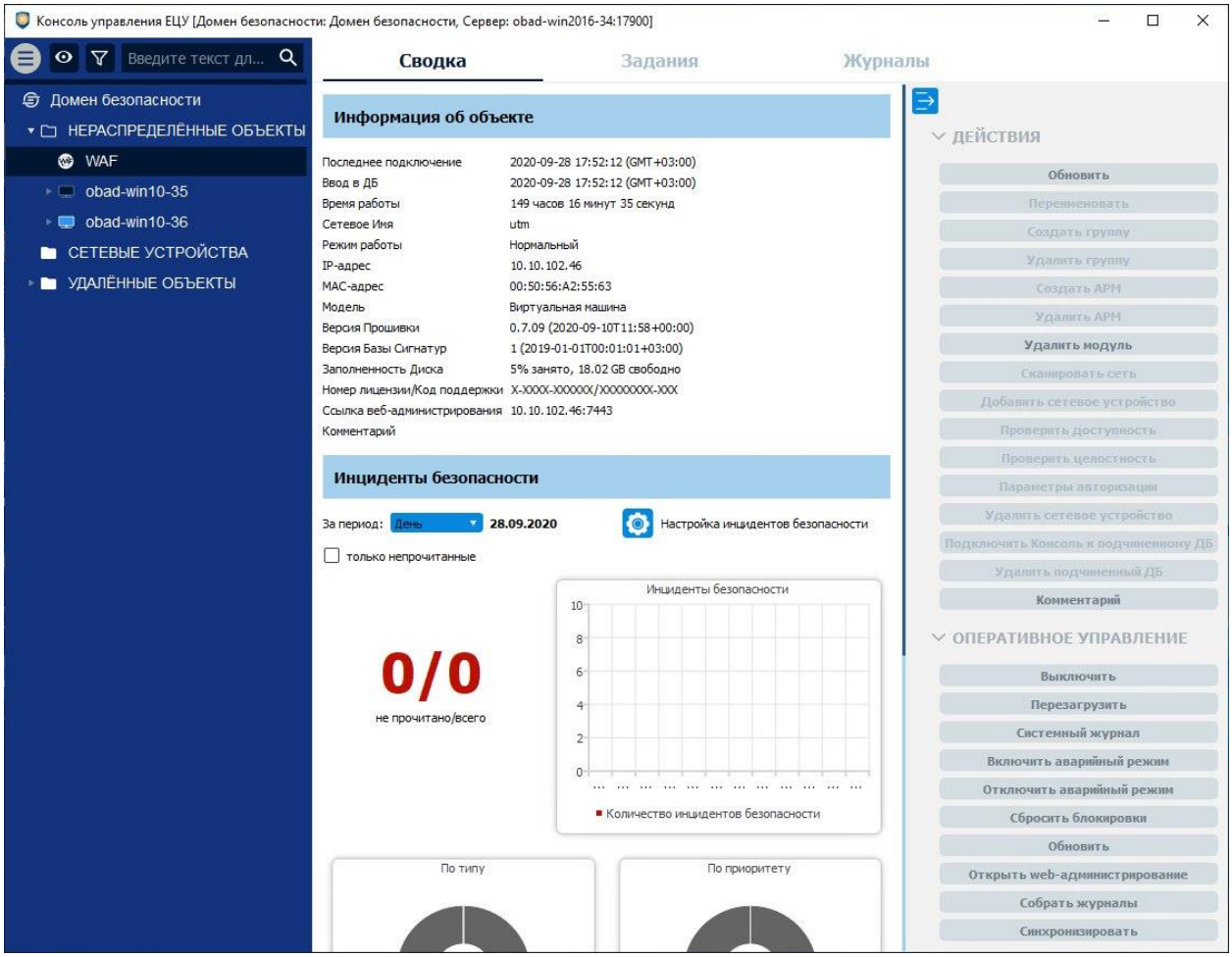

Рис. 175. Вкладка «Сводка»

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 модуль;
3. комментарий.

Доступны следующие команды оперативного управления на панели инструментов:

1. выключить;
2. перезагрузить;
3. системный журнал;
4. включить аварийный режим;
5. отключить аварийный режим;
6. сбросить блокировки;
7. обновить;
8. открыть web-администрирование;
9. собрать журналы;
10. синхронизировать.

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. 176):

- восстановить резервную копию;
- обновление базы разрешающих правил;
- сбор журналов;
- сброс к заводским настройкам;
- создать резервную копию.

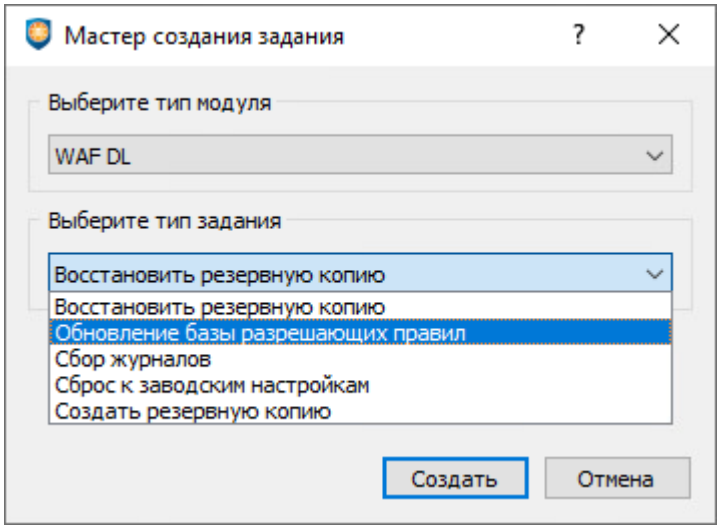

Рис. 176. Мастер создания задания для модуля WAF Dallas Lock

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. 177).

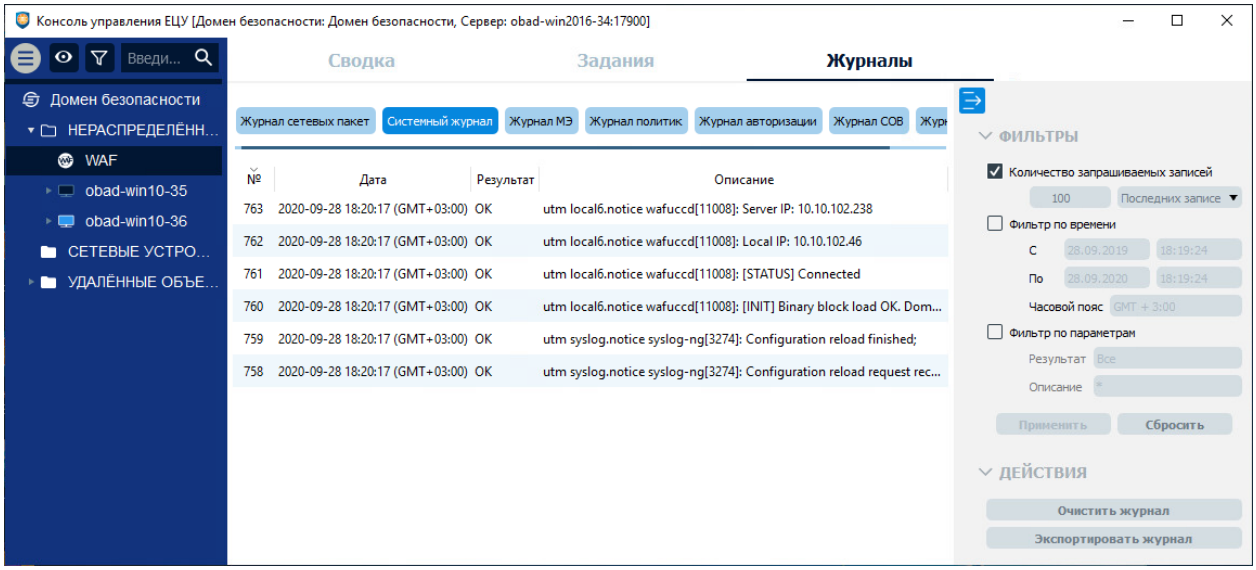

Рис. 177. Вкладка «Журналы»

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 СЕТЕВОЕ ОБОРУДОВАНИЕ

14.1 Регистрация сетевого устройства в ДБ

Зарегистрировать сетевое устройство в Домене безопасности можно следующими способами:

- путем добавления по IP-адресу;
- путем сканирования сети.

14.1.1 Добавление сетевого устройства по IP

Для регистрации сетевого устройства в Домене безопасности ЕЦУ по IP-адресу необходимо выполнить следующие шаги:

1. Убедиться, что сетевое устройство поддерживает протокол SNMP 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. 178).

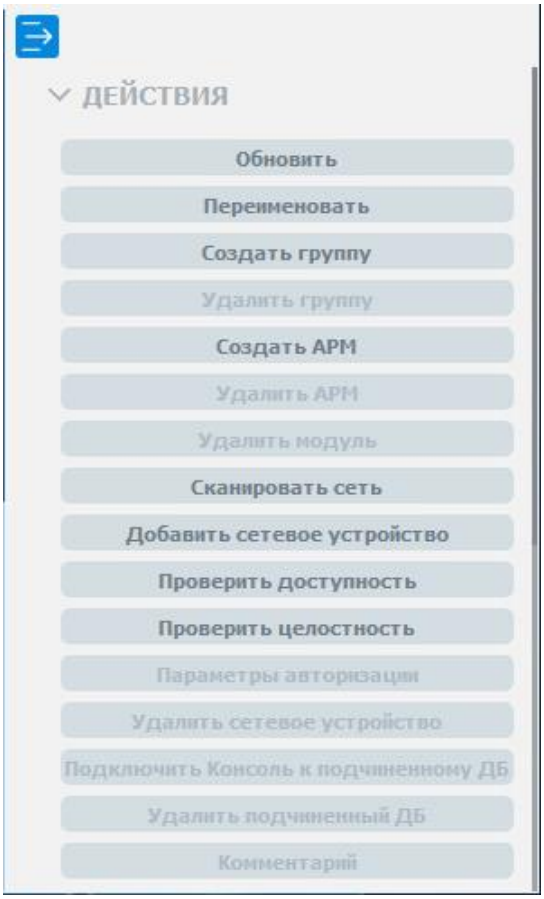

Рис. 178. Добавить сетевое устройство

4. Появится окно «Добавление устройства», в котором необходимо указать следующие параметры (рис. 179):
   - IPv4-адрес сетевого устройства;
   - версию протокола SNMP;
   - порт;
   - таймаут;
   - сообщество (пароль).

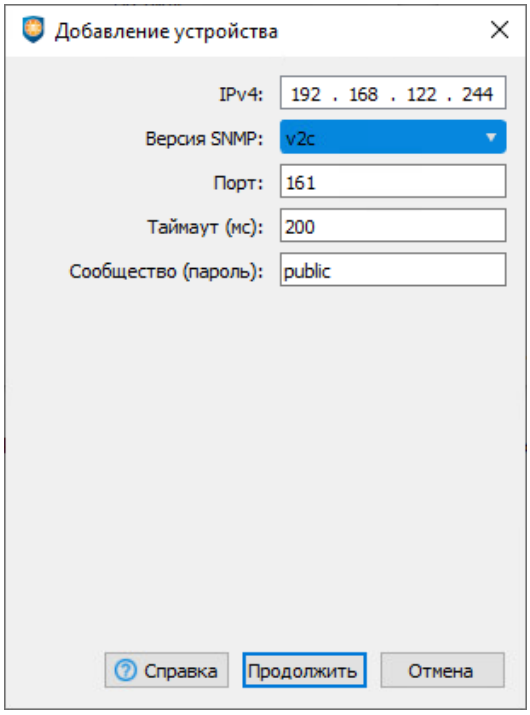

Рис. 179. Окно добавления сетевого устройства

5. После заполнения всех полей нажать кнопку «Продолжить».

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 устройства», появится иконка зарегистрированного сетевого устройства (рис. 180).

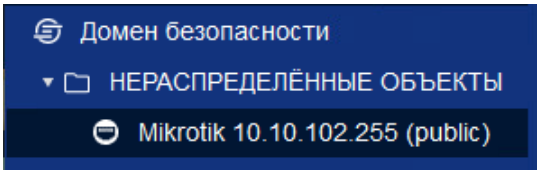

Рис. 180. Иконка зарегистрированного сетевого устройства в дереве ДБ

14.1.2 Сканирование диапазона сетевых адресов

Для регистрации сетевого устройства в Домене безопасности ЕЦУ путем сканирования диапазона сетевых адресов необходимо выполнить следующие шаги:

1. Убедиться, что сетевое устройство поддерживает протокол SNMP 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. 181).

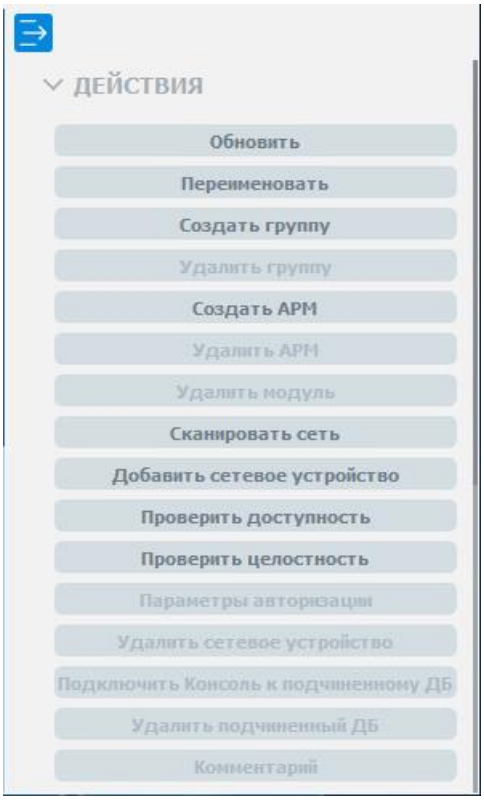

Рис. 181. Сканировать сеть

4. Появится окно «Сканирование сети», в котором перейти на вкладку «Сетевое устройство» и далее указать следующие параметры (рис. 182):

- диапазон IPv4-адресов для сканирования;
- версию протокола SNMP;
- порт;
- таймаут;
- сообщество (пароль).

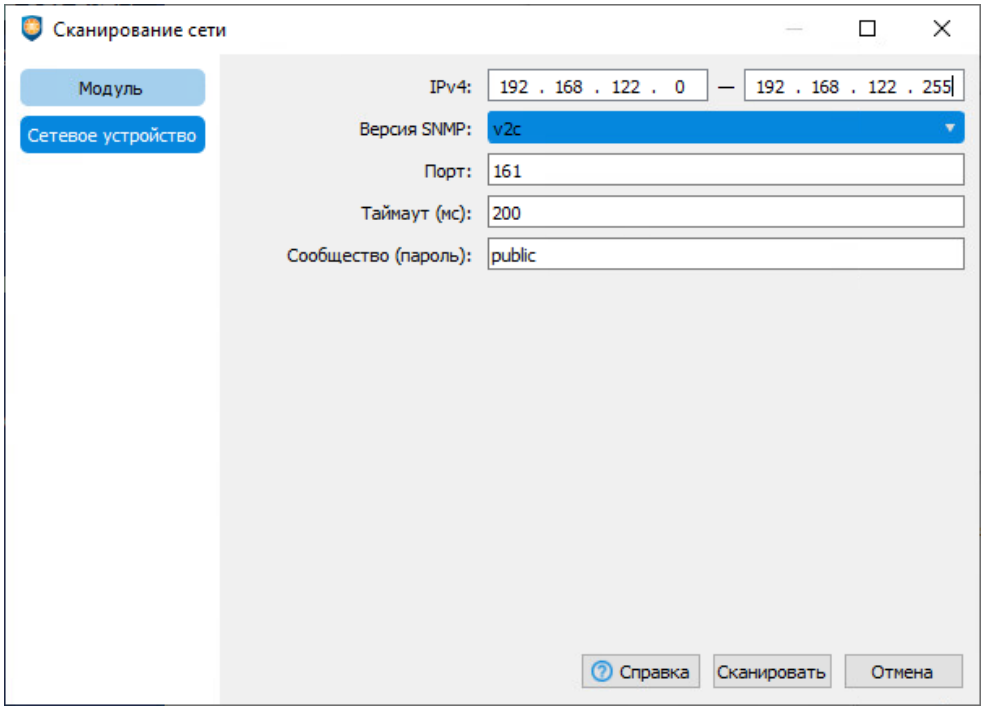

Рис. 182. Окно сканирование сети

5. После заполнения всех полей нажать кнопку «Сканировать» и далее можно просматривать состояние процесса сканирования для каждого диапазона сетевых адресов.
6. По завершении процесса сканирования из списка обнаруженных объектов можно выбрать те объекты, которые необходимо зарегистрировать в ДБ (рис. 183).

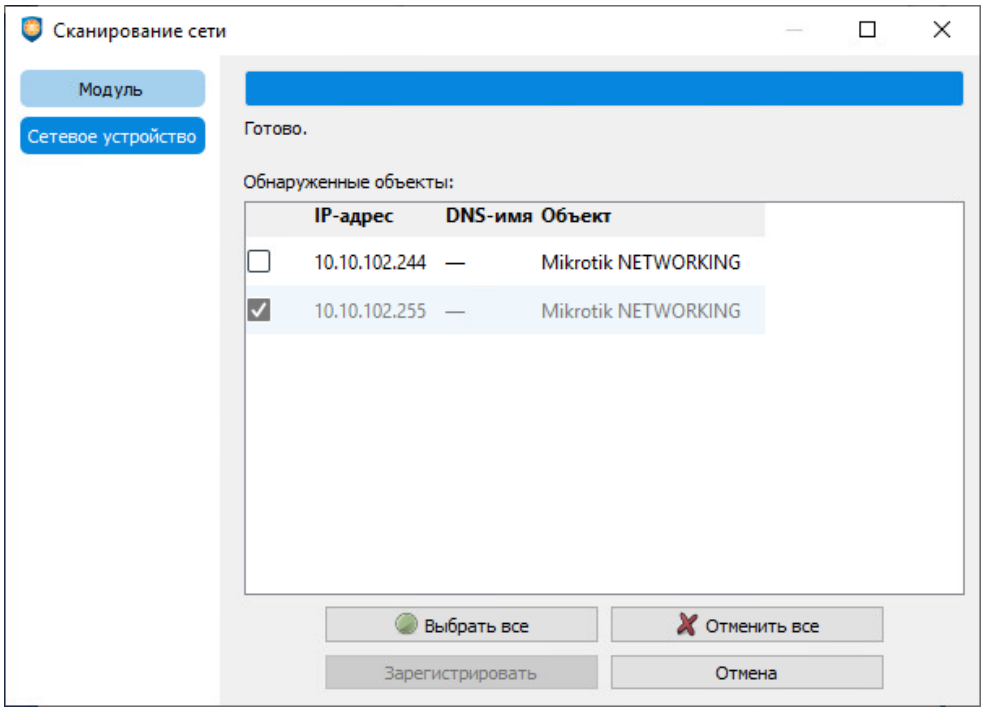

Рис. 183. Выбор объектов для регистрации в ДБ

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. 184).

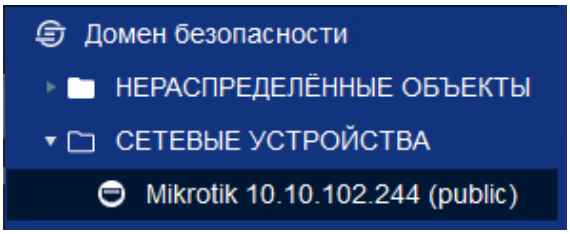

Рис. 184. Иконка зарегистрированного сетевого устройства в дереве ДБ

14.2 Удаление сетевого устройства из ДБ

Для удаления сетевого устройства из Домена безопасности ЕЦУ необходимо:

1. Выбрать пункт «Удалить сетевое устройство» из контекстного меню, нажав правой кнопкой мыши на нужное устройство в дереве ДБ (рис. 185), или воспользоваться командой «Удалить сетевое устройство» на панели инструментов «Действия» вкладки «Сводка» на уровне устройства в дереве ДБ (рис. 186).

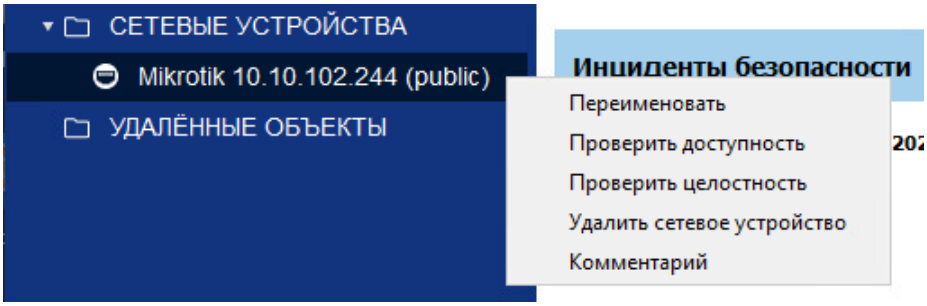

Рис. 185. Удаление устройства посредством контекстного меню

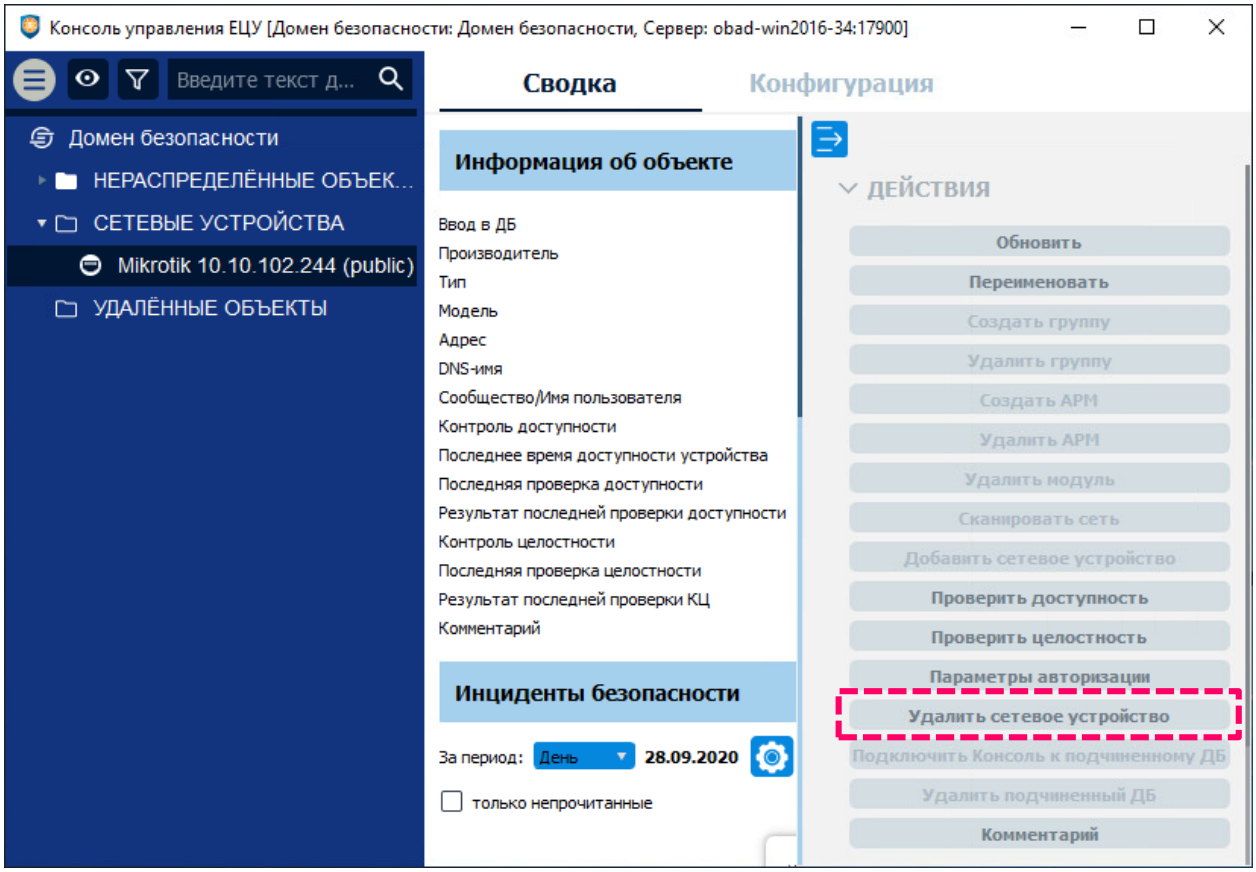

Рис. 186. Удаление посредством панели «Действия»

2. Удаленное сетевое устройство переместится в базовую группу «Удаленные объекты» дерева ДБ.

14.3 Настройка сетевого устройства

В дереве Домена безопасности ЕЦУ 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 времени, которое определяется параметром «Оповещения при отсутствии связи с объектом» (при условии, что настроено оповещение об отсутствии связи с объектом).

Настройки на уровне сетевого устройства отображаются на нескольких основных вкладках.

14.3.1 Сводка сетевого устройства

Вкладка «Сводка» на уровне сетевого устройства отображает общее состояние сетевого устройства (рис. 187).

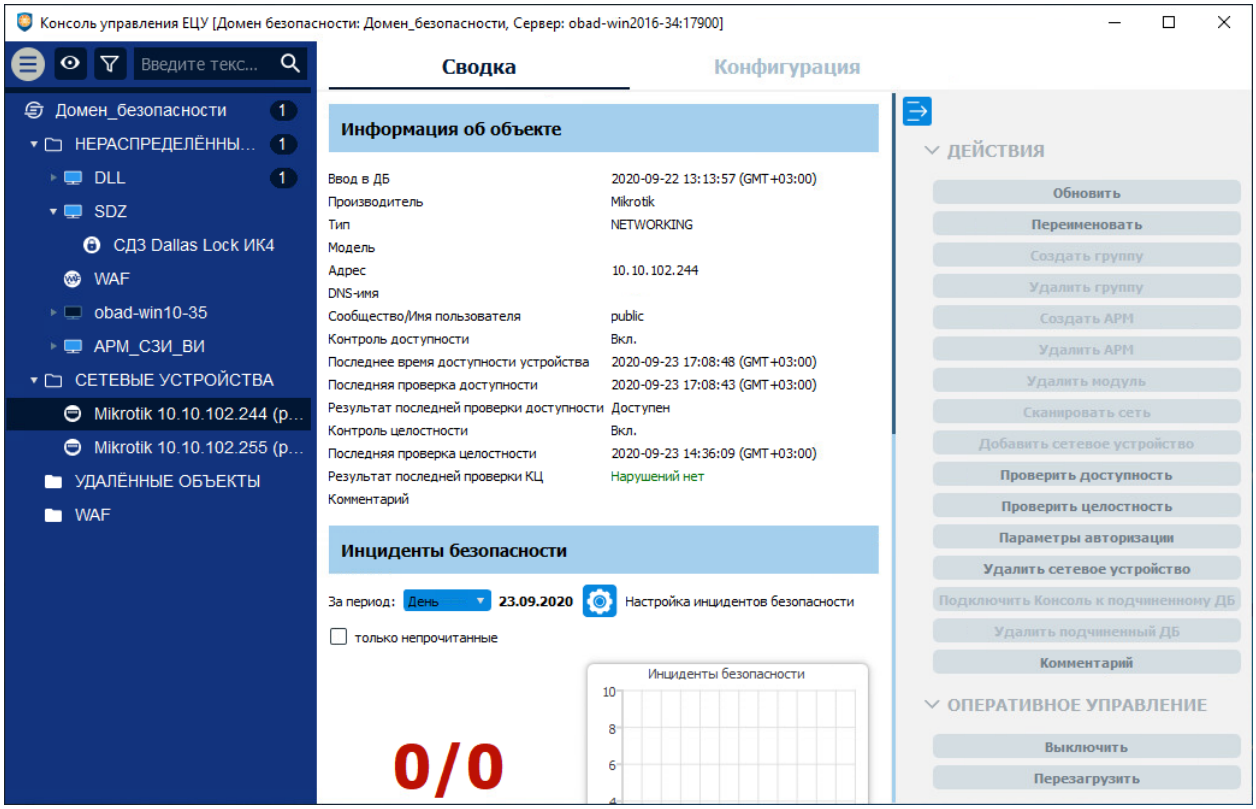

Рис. 187. Сводка сетевого устройства

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; • информация о производителе, типе и модели сетевого устройства; • сетевой адрес устройства; • DNS-имя устройства; • сообщество/имя пользователя, под которым зарегистрировано устройство; • состояние контроля доступности; • дата и время последней доступности устройства; • дата и время последней проверки доступности; • информация о результатах проверки доступности устройства; • состояние контроля целостности; • дата и время последней проверки целостности; • информация о результатах проверки целостности; • 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. переименовать;
3. проверить доступность;
4. проверить целостность;
5. параметры авторизации;
6. удалить сетевое устройство;
7. комментарий.

Доступны следующие команды оперативного управления на панели инструментов:

1. выключить;
2. перезагрузить.

14.3.2 Конфигурация сетевого устройства

Вкладка «Конфигурация» на уровне сетевого устройства отображает параметры сетевого устройства (рис. 188).

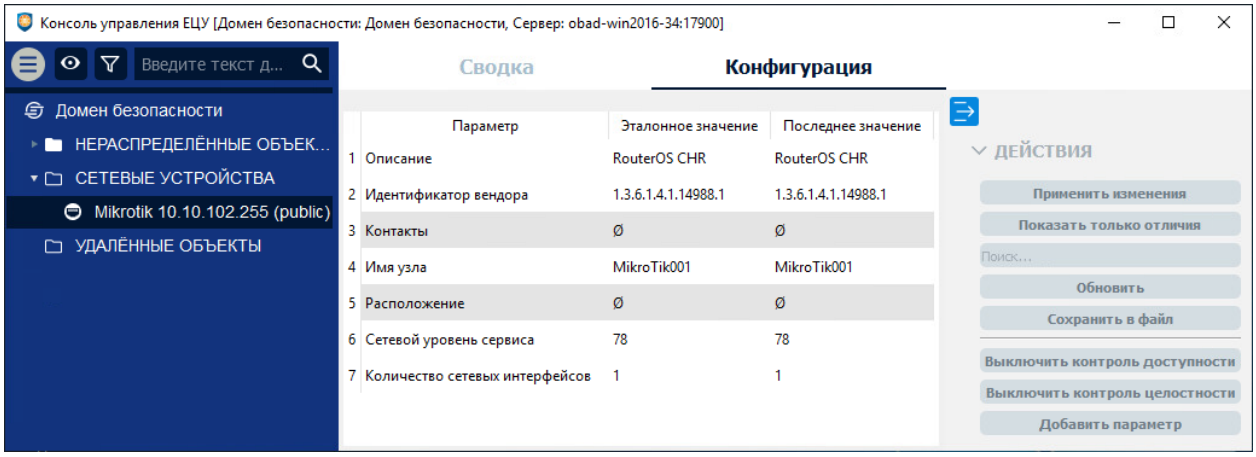

Рис. 188. Конфигурация сетевого устройства

В таблице на вкладке «Конфигурация» содержатся параметры и их значения, полученные от сетевого устройства по протоколу SNMP.
Список параметров сетевого устройства представляется собой таблицу с полями:

- Параметр;
- Эталонное значение;
- Последнее значение.

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 осуществляется поиск конфигурации для данного устройства. Если в базе не обнаружена конфигурация для производителя, используется конфигурация по умолчанию.

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 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. 189).

Примечание. События нарушения целостности сетевого оборудования могут возникать, если ЕЦУ при работе не успевает получить значения параметров OID с устройств. Для решения данной проблемы сетевое устройство необходимо вывести из-под контроля ЕЦУ и зарегистрировать заново, увеличив при добавлении время таймаута.

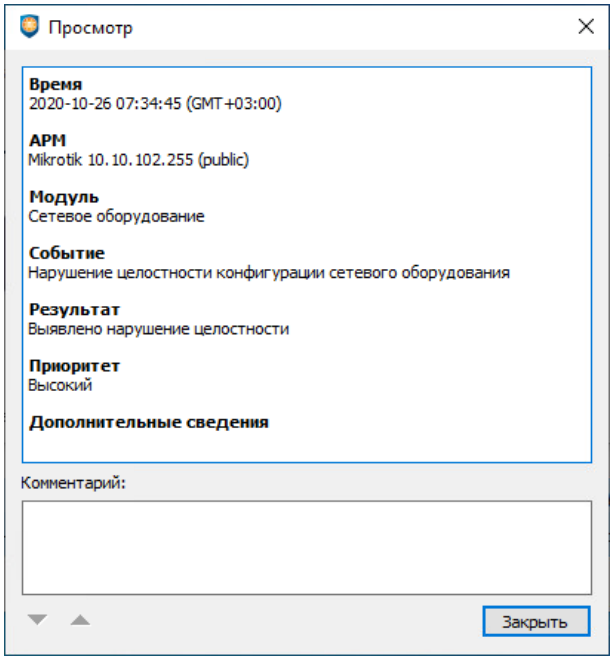

Рис. 189. Просмотр сведений об инциденте безопасности

На вкладке «Конфигурация» соответствующий параметр будет выделен цветом (рис. 190).

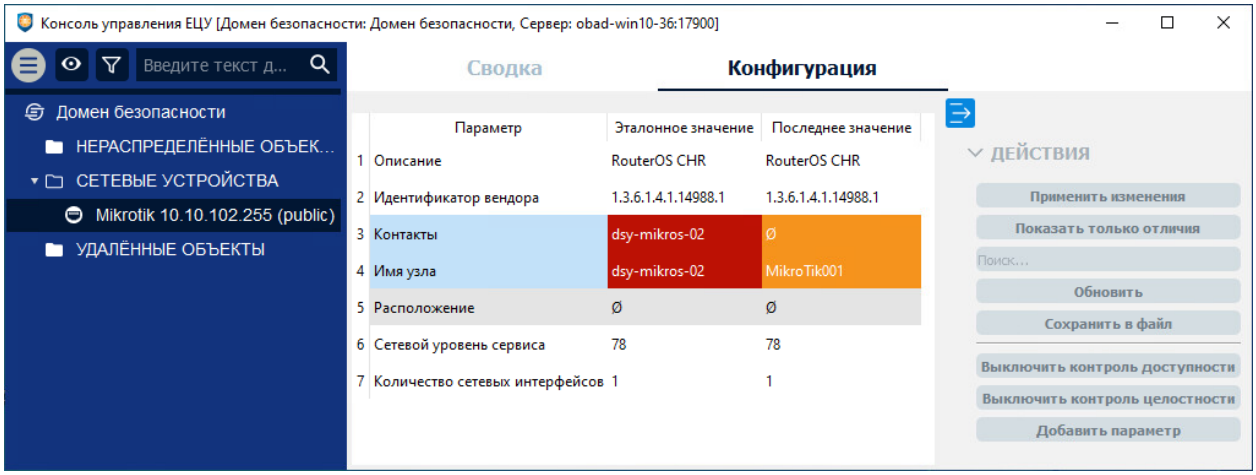

Рис. 190. Нарушение целостности контролируемого параметра

На вкладке «Конфигурация» на панели инструментов «Действия» доступны следующие команды:

1. «Применить изменения», которая предназначена для принятия последних полученных значений

конфигурации за эталонные;

2. «Показать только отличия/Показать все поля» — команды предназначены для перехода в режим отображения параметров конфигурации, целостность которых нарушена или для возвращения к просмотру всех параметров соответственно;
3. «Поиск…» — позволяет искать параметры конфигурации;
4. «Обновить», которая предназначена для получения актуальных значений конфигурации от устройства;
5. «Сохранить в файл», которая предназначена для сохранения отчета о конфигурации сетевого устройства в формате «txt»;
6. «Включить/Выключить контроль доступности», которая предназначена для изменения состояния контроля доступности сетевого устройства;
7. «Включить/Выключить контроль целостности», которая предназначена для изменения состояния контроля целостности значений конфигурации сетевого устройства;
8. «Добавить параметр» позволяет задать для нового контролируемого параметра:
    - имя;
    - OID;
    - флаг «Контролировать параметр».

   За эталонное значение будет принято значение, полученное от сетевого устройства при следующей проверке.

15 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 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 (существует возможность создавать несколько уровней подчинения). Ограничения по количеству подчиненных у главного домена безопасности устанавливаются лицензией.

15.1 Ввод ДБ в подчинение

15.1.1 Ввод ДБ в подчинение в процессе установки

Для ввода в подчинение Домена безопасности в процессе установки ЕЦУ необходимо:

1. убедиться, что Домен безопасности, в подчинение которому осуществляется ввод, доступен по сети;
2. запустить процесс установки ЕЦУ;
3. на шаге «Выбор типа домена» выбрать пункт «Подчиненный домен безопасности» (рис. 191).

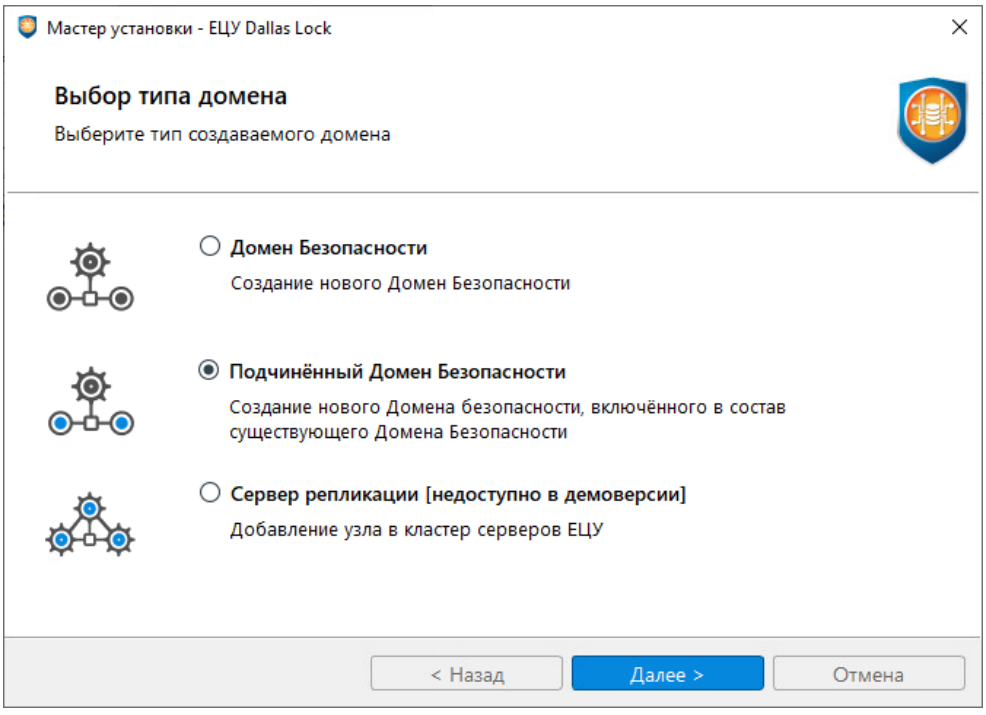

Рис. 191. Шаг «Выбор типа домена» в мастере установки ЕЦУ

4. задать параметры главного ДБ (рис. 192):
   - адрес главного ДБ;
   - ключ доступа к ДБ;

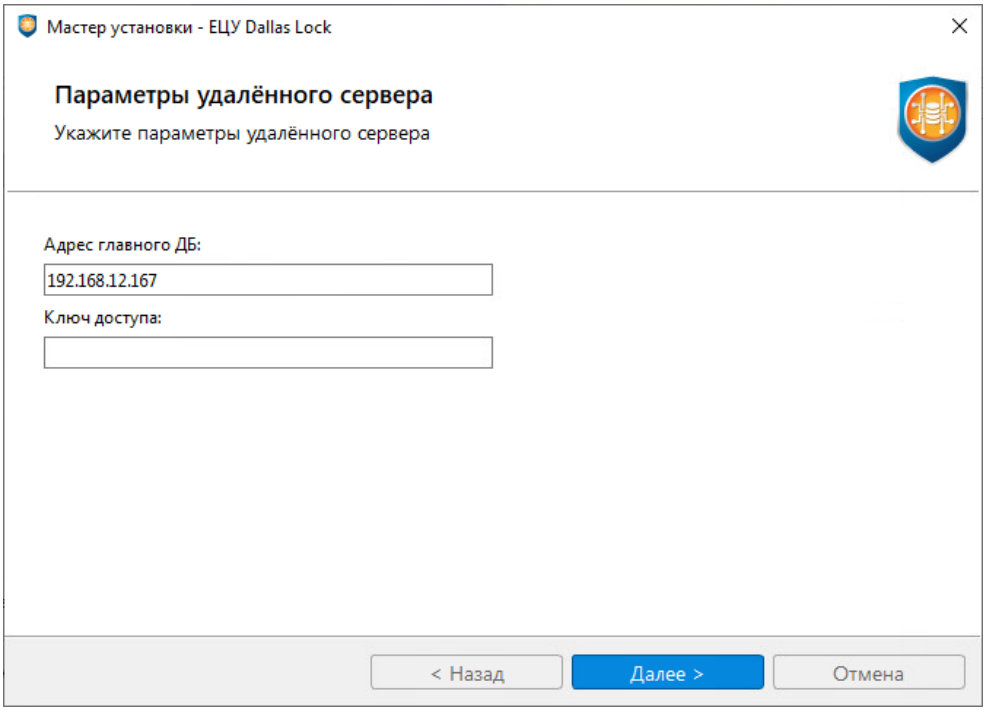

Рис. 192. Параметры удаленного сервера

5. далее продолжить и завершить установку ЕЦУ;
6. после завершения установки подчиненного ДБ в дереве главного ДБ появится введенный в подчинение ДБ (рис. 193).

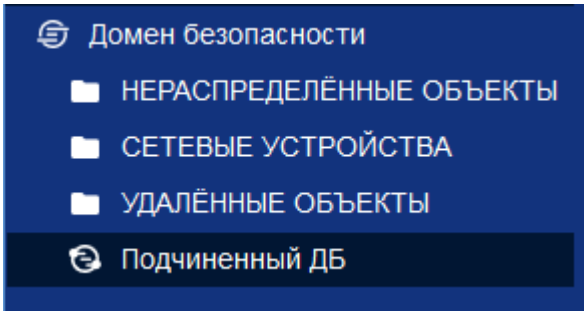

Рис. 193. Подчиненный ДБ в дереве родительского

15.1.2 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. 194);

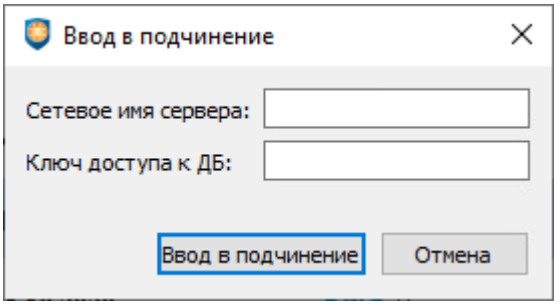

Рис. 194. Ввод в подчинение

5. нажать кнопку «Ввод в подчинение».

Если процесс ввода в подчинение прошел успешно, то через некоторое время появится соответствующее сообщение (рис. 195).

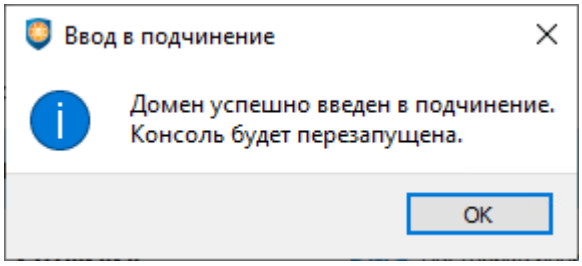

Рис. 195. ДБ успешно введен в подчинение

После перезапуска консоли на уровне ДБ на вкладке «Сводка» → «Информация об объекте» отобразится информация о родительском домене (рис. 196).

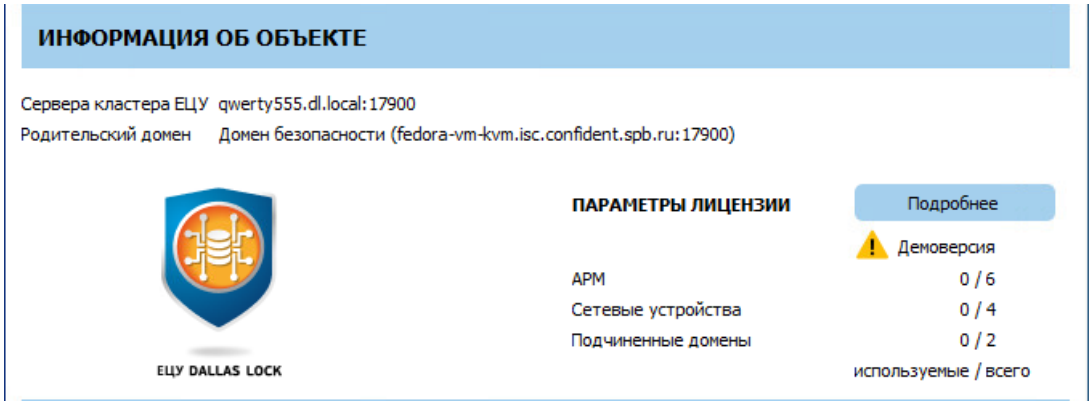

Рис. 196. Информация о родительском домене

Также в дереве главного ДБ появится введенный в подчинение ДБ (рис. 193).

15.2 Вывод ДБ из подчинения

15.2.1 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. 197) нажать кнопку «Вывод из подчинения».

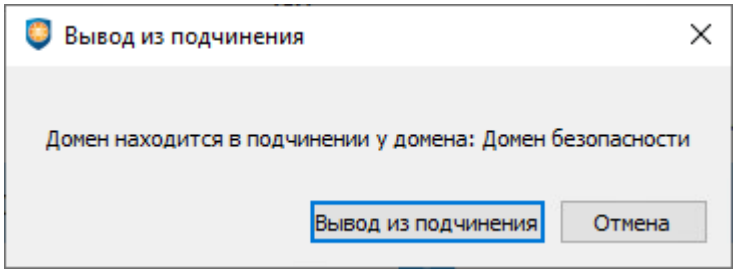

Рис. 197. Вывод из подчинения

Если процесс вывода домена из подчинения прошел успешно, то через некоторое время появится соответствующее сообщение (рис. 198).

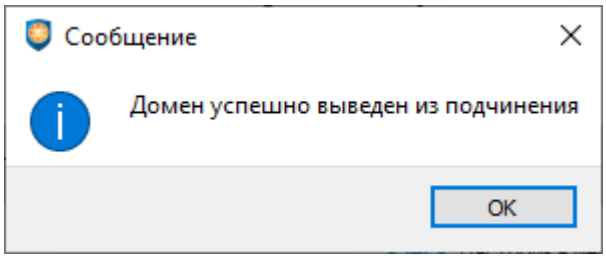

Рис. 198. ДБ успешно выведен из подчинения

15.2.2 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 подчиненный ДБ» (рис. 200) или выбрать соответствующую команду из контекстного меню, нажав правой кнопкой мыши на подчиненный ДБ в дереве (рис. 199).

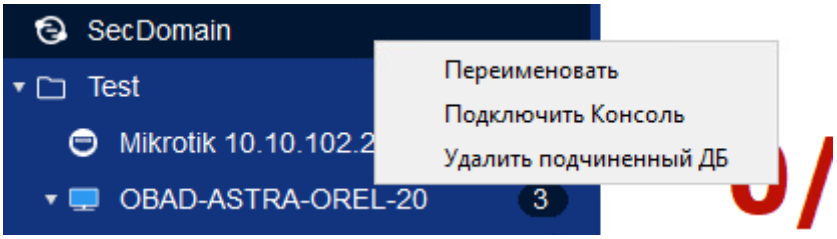

Рис. 199. Вывод из подчинения посредством контекстного меню

Рис. 200 Команды панели инструментов для подчиненного ДБ

Выведенный из подчинения ДБ переместится в базовую группу «Удаленные объекты».

15.3 Настройка подчиненного домена безопасности

В дереве главного Домена безопасности ЕЦУ 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» (при условии, что настроено оповещение об отсутствии связи с объектом).

Администратор ЕЦУ 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.

15.3.1 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;
- по расписанию (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».

15.3.2 Сводка подчиненного ДБ

Вкладка «Сводка» на уровне подчиненного ДБ отображает общее состояние подчиненного ДБ (рис. 201).

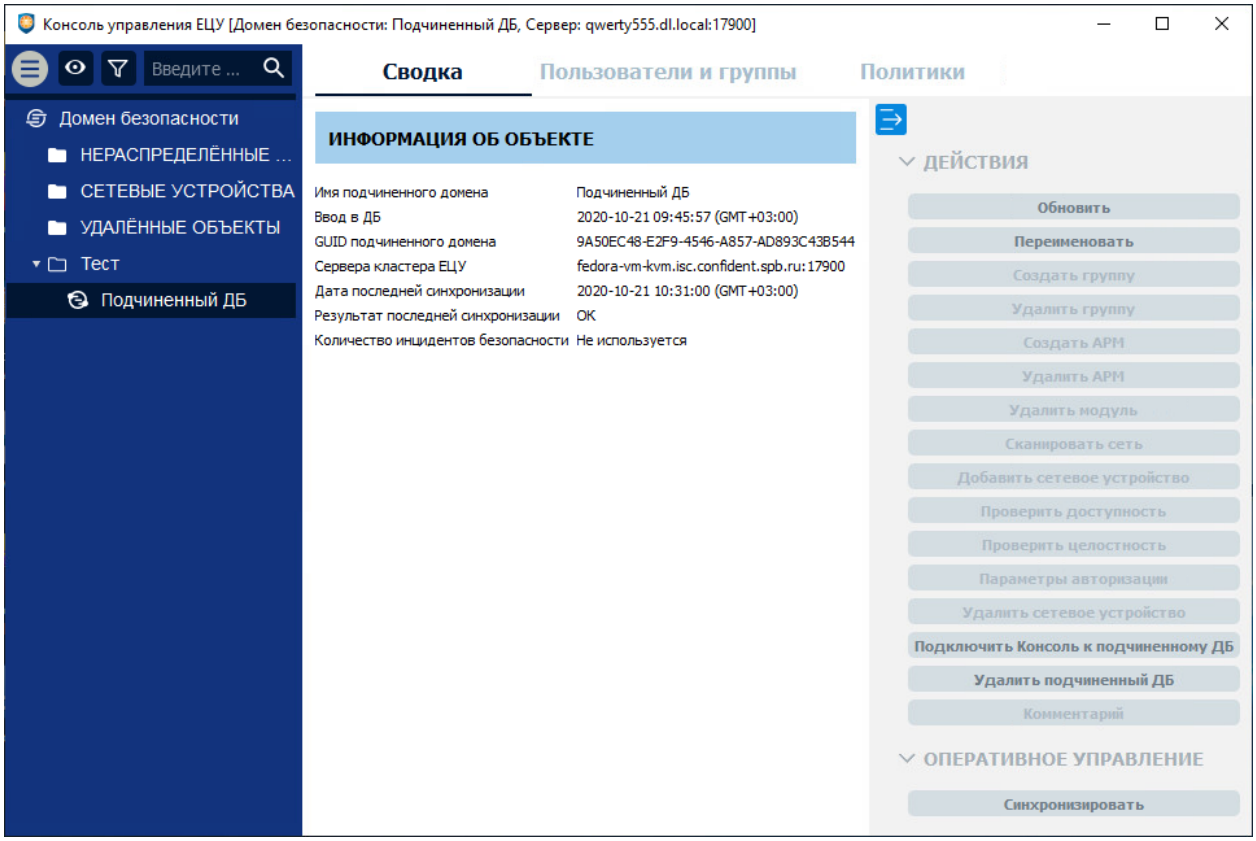

Рис. 201. Вкладка «Сводка»

Доступны следующие разделы информационной панели.

Информация об объекте
В информационной панели отображается следующая информация о текущем состоянии модуля: • имя подчиненного домена; • информация о дате и времени ввода в ДБ; • GUID подчиненного домена; • серверы 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. подключить консоль к подчиненному ДБ;
3. удалить подчиненный ДБ.

Доступны следующие команды оперативного управления на панели инструментов:

1. синхронизировать.

15.3.3 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.

15.3.4 Политики подчиненного ДБ

Вкладка «Политики» на уровне подчиненного ДБ позволяет редактировать политики на подчиненном ДБ (рис. 202).

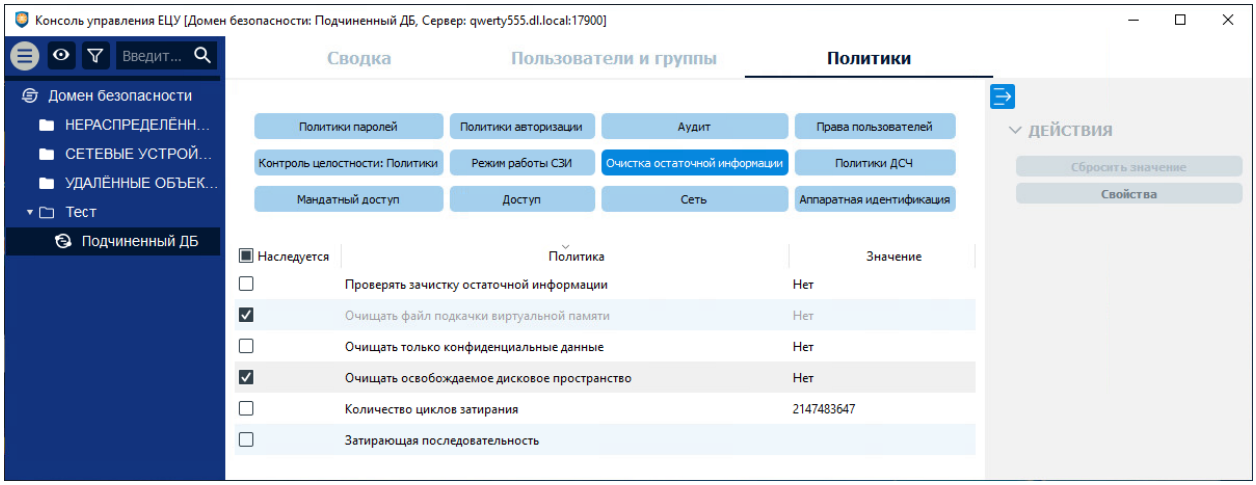

Рис. 202. Вкладка «Политики»

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.