

УТВЕРЖДЕН
ПФНА.26.20.40.143.001 ИЗ-ЛУ
(взамен ПФНА.501410.001 ИЗ-ЛУ)

**ЕДИНЫЙ ЦЕНТР
УПРАВЛЕНИЯ**

Dallas Lock



Инструкция по использованию

ПФНА.26.20.40.143.001 ИЗ
(взамен ПФНА.501410.001 ИЗ)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	5
ТЕРМИНЫ.....	5
СОКРАЩЕНИЯ	6
ПРЕДСТАВЛЕНИЕ МОДУЛЕЙ В ИНТЕРФЕЙСЕ ЕЦУ	7
1 НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ ЕЦУ DALLAS LOCK	9
1.1 СТРУКТУРА ЕЦУ.....	9
1.2 ВОЗМОЖНОСТИ ЕЦУ	9
1.3 РЕКОМЕНДАЦИИ ПО ПРИМЕНЕНИЮ ЕЦУ	12
2 УСТАНОВКА И УДАЛЕНИЕ ЕЦУ DALLAS LOCK	14
2.1 ТРЕБОВАНИЯ К АППАРАТНОМУ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ	14
2.2 УСТАНОВКА ЕЦУ DALLAS LOCK.....	17
2.3 УДАЛЕНИЕ ЕЦУ DALLAS LOCK	30
2.4 УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ	34
2.5 О ПРОГРАММЕ	36
3 ОБЩИЕ ПРИНЦИПЫ РАБОТЫ ЕЦУ DALLAS LOCK.....	38
3.1 СИНХРОНИЗАЦИЯ	38
3.2 РЕПЛИКАЦИЯ	38
4 АДМИНИСТРИРОВАНИЕ ЕЦУ DALLAS LOCK.....	39
4.1 ЗАПУСК КОНСОЛИ ЕЦУ	39
4.2 ОПИСАНИЕ КОНСОЛИ ЕЦУ	40
4.3 НАСТРОЙКИ ЛИЦЕНЗИРОВАНИЯ	43
4.4 ПЕРЕРАСПРЕДЕЛЕНИЕ ТЕРМИНАЛЬНЫХ СЕССИЙ	46
4.5 МЕХАНИЗМ АВТОМАТИЗИРОВАННОЙ МИГРАЦИИ С СБ НА ЕЦУ	47
4.6 ПАРАМЕТРЫ ДОМЕНА БЕЗОПАСНОСТИ	53
4.7 НАСТРОЙКА ИНЦИДЕНТОВ БЕЗОПАСНОСТИ	59
4.8 МЕНЕДЖЕР ДОМЕНОВ	63
4.9 ПАРАМЕТРЫ РАБОТЫ.....	64
5 ДОМЕН БЕЗОПАСНОСТИ ЕЦУ	70
5.1 Сводка для ДБ.....	70
5.2 Пользователи ДБ	74
5.3 РОЛЕВАЯ МОДЕЛЬ УЧЕТНЫХ ЗАПИСЕЙ ДБ	98
5.4 Политики ДБ.....	98
5.5 МЕЖСЕТЕВОЙ ЭКРАН	138
5.6 СИСТЕМА КОНТРОЛЯ НАКОПИТЕЛЕЙ	146
5.7 КОНТРОЛЬ РЕСУРСОВ.....	150
5.8 СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ	153
5.9 БЕЗОПАСНАЯ СРЕДА СОВ (ПЕСОЧНИЦА).....	180
5.10 СРЕДСТВО ОБНАРУЖЕНИЯ И РЕАГИРОВАНИЯ	182
5.11 Задания ДБ.....	189
5.12 ЖУРНАЛ ДБ.....	192
6 ГРУППЫ ДОМЕНА БЕЗОПАСНОСТИ.....	194
6.1 БАЗОВЫЕ ГРУППЫ	194
6.2 НАСТРОЙКА ГРУПП	194
7 АРМ ДОМЕНА БЕЗОПАСНОСТИ ЕЦУ.....	204
7.1 НАСТРОЙКА АРМ	204
8 МОДУЛИ ДОМЕНА БЕЗОПАСНОСТИ ЕЦУ	209

8.1	НАСТРОЙКА модуля	209
9	МОДУЛЬ СЗИ DALLAS LOCK 8.0-С/К.....	218
9.1	Ввод модуля в ДБ	218
9.2	Вывод модуля из ДБ	220
9.3	УДАЛЕННОЕ РАЗВЕРТЫВАНИЕ СЗИ DALLAS LOCK 8.0.....	221
9.4	УДАЛЕННОЕ ОБНОВЛЕНИЕ СЗИ НСД DALLAS LOCK 8.0	237
9.5	НАСТРОЙКА модуля СЗИ DALLAS LOCK 8.0	241
10	МОДУЛЬ СЗИ НСД DALLAS LOCK LINUX.....	248
10.1	Ввод модуля в ДБ.....	248
10.2	Вывод модуля из ДБ	249
10.3	УДАЛЕННОЕ РАЗВЕРТЫВАНИЕ СЗИ НСД DALLAS LOCK LINUX.....	251
10.4	УДАЛЕННОЕ ОБНОВЛЕНИЕ СЗИ НСД DALLAS LOCK LINUX	257
10.5	НАСТРОЙКА модуля СЗИ НСД DALLAS LOCK LINUX.....	260
11	МОДУЛЬ СЗИ ВИ DALLAS LOCK	267
11.1	Ввод модуля в ДБ.....	267
11.2	Вывод модуля из ДБ	268
11.3	НАСТРОЙКА СЗИ ВИ DALLAS LOCK	268
12	МОДУЛЬ СДЗ DALLAS LOCK.....	274
12.1	Ввод модуля в ДБ.....	274
12.2	Вывод модуля из ДБ	276
12.3	НАСТРОЙКА модуля СДЗ DALLAS LOCK	276
13	МОДУЛЬ СДЗ УБ DALLAS LOCK.....	281
13.1	Ввод модуля в ДБ.....	281
13.2	Вывод модуля из ДБ	282
13.3	НАСТРОЙКА модуля СДЗ УБ DALLAS LOCK	282
14	МОДУЛЬ WAF DALLAS LOCK.....	285
14.1	Ввод модуля в ДБ.....	285
14.2	Вывод модуля из ДБ	287
14.3	НАСТРОЙКА модуля WAF DALLAS LOCK	288
15	АГЕНТ ЕЦУ.....	293
15.1	ТРЕБОВАНИЯ К АППАРАТНОМУ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ.....	293
15.2	УСТАНОВКА и УДАЛЕНИЕ АГЕНТА ЕЦУ	294
15.3	РЕГИСТРАЦИЯ АГЕНТА ЕЦУ в ДБ	305
15.4	НАСТРОЙКА модуля АГЕНТ ЕЦУ WINDOWS/LINUX.....	307
15.5	НАСТРОЙКА модуля АГЕНТ ЕЦУ ANDROID	314
16	KASPERSKY SECURITY CENTER	318
16.1	НАСТРОЙКА KASPERSKY SECURITY CENTER	318
16.2	ПОДКЛЮЧЕНИЕ к KASPERSKY SECURITY CENTER.....	318
16.3	ОТКЛЮЧЕНИЕ KASPERSKY SECURITY CENTER.....	320
16.4	НАСТРОЙКА KASPERSKY SECURITY CENTER	320
16.5	НАСТРОЙКА модуля KASPERSKY ENDPOINT SECURITY.....	324
17	СЕТЕВОЕ ОБОРУДОВАНИЕ	327
17.1	РЕГИСТРАЦИЯ СЕТЕВОГО УСТРОЙСТВА в ДБ	327
17.2	УДАЛЕНИЕ СЕТЕВОГО УСТРОЙСТВА из ДБ	331
17.3	НАСТРОЙКА СЕТЕВОГО УСТРОЙСТВА	332
18	ПОДЧИНЕННЫЙ ДОМЕН БЕЗОПАСНОСТИ	338
18.1	Ввод ДБ в подчинение.....	338

18.2	Вывод ДБ из подчинения	340
18.3	Настройка подчиненного домена безопасности	342

ПРИЛОЖЕНИЕ А.....347

A.1	Шаблоны автоматизированных систем	347
A.2	Шаблоны государственных информационных систем	348
A.3	Шаблоны информационных систем персональных данных.....	350

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 <http://www.dallaslock.ru/>. На данном сайте можно заказать комплекс услуг по проектированию, внедрению и сопровождению продукта. Также при необходимости можно обратиться в службу технической поддержки по электронному адресу: helpdesk@confident.ru.

ТЕРМИНЫ

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

Термин	Определение
<i>Автоматизированное рабочее место</i>	виртуальная или физическая рабочая станция, используемая в ЕЦУ как способ представления совокупности нескольких модулей в качестве единой машины
<i>Группа</i>	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
<i>Доверенный домен безопасности</i>	Домен безопасности, находящийся с ДБ в доверительных отношениях
<i>Домен безопасности ЕЦУ</i>	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
<i>Дерево домена безопасности</i>	структурированное отображение объектов домена безопасности в виде иерархии в консоли ЕЦУ
<i>Задание</i>	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.
<i>Модуль</i>	представление отдельного продукта производства ООО «Конфидент» : • СЗИ Dallas Lock 8.0 редакции «К» и «С»; • СЗИ НСД Dallas Lock Linux; • СЗИ ВИ Dallas Lock; • СДЗ Dallas Lock; • СДЗ УБ Dallas Lock; • шлюз безопасности WAF Dallas Lock; • Агент ЕЦУ. Каждый модуль может использоваться независимо от других

<i>Консоль ЕЦУ</i>	приложение, предназначенное для управления ЕЦУ Dallas Lock и доменом безопасности ЕЦУ
<i>Кластер серверов ДБ</i>	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
<i>Локальное/Удаленное администрирование модуля</i>	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 <i>localhost</i>
<i>Оперативное управление</i>	процесс управления модулем путем отправки команд, выполняемых на стороне модуля, и не требующих передачи результатов на ЕЦУ . Например, команда на выключение модуля
<i>Подчиненный домен безопасности</i>	домен безопасности, входящий в ДБ на более низком уровне иерархии
<i>Репликация конфигурации</i>	повторение функциональности серверов ЕЦУ для обеспечения отказоустойчивости и распределения нагрузки по возможности наиболее оптимальным образом
<i>Синхронизация</i>	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
<i>Субъект доступа</i>	сотрудник предприятия, у которого есть учетная запись. Учетная запись характеризуется логином, паролем, аппаратным идентификатором (АИ), расписанием, группой и т.д. Учетная запись должна быть единой для всех модулей ЕЦУ
<i>Централизованное управление</i>	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
<i>АИ</i>	аппаратный идентификатор
<i>АИБ</i>	администратор информационной безопасности
<i>АРМ</i>	автоматизированное рабочее место
<i>БД</i>	база данных
<i>ВМ</i>	виртуальная машина
<i>ДБ</i>	домен безопасности ЕЦУ
<i>ДВК</i>	датчик вскрытия корпуса
<i>ДСЧ</i>	датчик случайных чисел

<i>ЕЦУ</i>	Единый центр управления Dallas Lock
<i>ЗПС</i>	замкнутая программная среда
<i>КПСН</i>	ключ преобразования съемных накопителей
<i>КУ</i>	консоль управления
<i>КЦ</i>	контроль целостности
<i>ЛВС</i>	локальная вычислительная сеть
<i>МЭ</i>	межсетевой экран
<i>НСД</i>	несанкционированный доступ
<i>ОС</i>	операционная система
<i>ПК</i>	персональный компьютер
<i>ПО</i>	программное обеспечение
<i>СДЗ</i>	средство доверенной загрузки Dallas Lock
<i>СДЗ УБ</i>	средство доверенной загрузки уровня базовой системы ввода-вывода
<i>СЗИ</i>	средство защиты информации
<i>СЗИ ВИ</i>	система защиты информации в виртуальных инфраструктурах
<i>СКН</i>	система контроля накопителей
<i>СОВ</i>	система обнаружения вторжений
<i>СОР</i>	средство обнаружения и реагирования
<i>СУ</i>	сетевое устройство
<i>Сервер УД</i>	сервер управления доступом
<i>ТС</i>	техническое средство
<i>УЗ</i>	учетная запись
<i>ФС</i>	файловая система
<i>ШОС</i>	штатная операционная система
<i>ЦУ СЗИ ВИ</i>	Центр управления СЗИ ВИ Dallas Lock
<i>AD</i>	Active Directory
<i>DL8.0</i>	СЗИ Dallas Lock 8.0
<i>FQDN</i>	имя домена
<i>SP (Service Pack)</i>	пакет обновлений для ОС
<i>WAF</i>	web application firewall

ПРЕДСТАВЛЕНИЕ МОДУЛЕЙ В ИНТЕРФЕЙСЕ ЕЦУ

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

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

Продукт	Наименование модуля	
	Основное обозначение	Поддерживается с версии (итерации)
СЗИ Dallas Lock 8.0 редакции «К» и «С»	Dallas Lock 8.0	версия 8.0.689.0 (ИК8) и выше
СЗИ НСД Dallas Lock Linux	Dallas Lock Linux	версия 3807 (ИК2) и выше
СЗИ ВИ Dallas Lock	СЗИ ВИ Dallas Lock	версия 4.68 (ИК4) и выше
СДЗ Dallas Lock	СДЗ Dallas Lock	версия 348.1 (ИК4) и выше
СДЗ УБ Dallas Lock	СДЗ УБ Dallas Lock	все версии
шлюз безопасности WAF Dallas Lock	по умолчанию соответствует системному имени хоста, может быть задано АИБ вручную	все версии
Агент ЕЦУ	Агент ЕЦУ	все версии

1 НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ ЕЦУ DALLAS LOCK

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

- создание единого отказоустойчивого домена безопасности (далее — ДБ) и организация централизованного управления средствами защиты информации линейки **Dallas Lock**:
 - **СЗИ НСД Dallas Lock 8.0** редакций «К» и «С» (далее — **DL8.0**);
 - **СЗИ НСД Dallas Lock Linux**;
 - **СЗИ ВИ Dallas Lock**;
 - **СДЗ Dallas Lock**;
 - **СДЗ УБ Dallas Lock**;
 - **WAF Dallas Lock**;
- удаленное управление рабочими станциями и серверами;
- удаленная настройка, а также сбор журналов и отчетов с рабочих станций и серверов при помощи **Агента ЕЦУ**;
- контроль целостности настроек сетевого оборудования (по SNMP/SSH) и сбор событий по Syslog;
- интеграция со сторонними продуктами:
 - антивирусные системы;
 - SIEM-системы.

1.1 Структура ЕЦУ

ЕЦУ Dallas Lock состоит из следующих основных компонентов:

1. Серверный компонент ЕЦУ (Служба ЕЦУ). Выполняет основные функции ЕЦУ:

- обеспечивает централизованное оперативное управление и аудит модулей;
- обеспечивает контроль и управление сетевыми устройствами;
- позволяет объединять несколько серверов **ЕЦУ** в единую логическую единицу — кластер Домена безопасности;
- обеспечивает работу механизма репликации конфигурации в рамках одного кластера ДБ;
- позволяет объединять несколько ДБ в единую логическую единицу, имеющую структуру вложенности со связями типа «родитель-потомок».

2. Консоль ЕЦУ. Пользовательский интерфейс, предназначенный для управления настройками службы **ЕЦУ**, а также для отображения на экране информации о работе службы.

1.2 Возможности ЕЦУ

При работе с сетевым оборудованием доступны следующие возможности:

- сканирование сети для обнаружения оборудования по протоколам SNMP и SSH;
- ввод сетевого оборудования под управление домена безопасности **ЕЦУ**;
- удаленная перезагрузка сетевого оборудования;
- поддержка собственной расширяемой базы файлов конфигурации оборудования;
- сохранение отчета о конфигурации сетевого оборудования;
- настройка параметров оборудования, берущихся под контроль;
- сравнение текущих значений параметров конфигурации оборудования с заданным эталоном значением;
- сигнализация о нарушении целостности;
- прием сообщений по протоколу Syslog.

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 APM;
- удаленное обновление модуля на APM;
- управление пользователями и группами пользователей на модуле;

- управление политиками безопасности;
- миграция с сервера безопасности настроек МЭ, СОВ, СКН и контроля устройств;
- управление заданиями на:
 - получение конфигурации;
 - применение конфигурации;
 - проверку целостности контролируемых объектов;
 - изменение параметров лицензии;
 - удаление модуля;
 - поиск индикаторов компрометации (IoC);
- сбор журналов модуля;
- отправка сигнализации об инцидентах безопасности;
- включение неактивного режима работы модуля или компонентов;
- управление мандатными метками (**только для Dallas Lock 8.0 редакции «С»**);
- настройка аппаратных идентификаторов;
- контроль и перераспределение терминальных сессий;
- управление профилем МЭ «Изоляция узла», позволяющим изолировать АРМ от сети передачи данных с возможностью управления со стороны **ЕЦУ**;
- централизованное управление межсетевым экраном;
- централизованное управление компонентом СОВ, включая управление индикаторами компрометации (IoC) и правилами автоматического реагирования в рамках СОР;
- централизованное управление компонентом СКН, включая управление ключами преобразованных съемных накопителей;
- централизованное управление контролем устройств;
- управление разблокировкой компьютера с установленным модулем.

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

- завершение работы и перезагрузка модуля;
- отображение информации о состоянии модуля;
- синхронизация политик/пользователей;
- удаленное развертывание модуля на АРМ;
- удаленное обновление модуля на АРМ;
- управление пользователями и группами пользователей на модуле;
- управление политиками безопасности;
- управление заданиями на:
 - удаление модуля;
 - изменение параметров лицензии;
 - получение конфигурации;
 - применение конфигурации;
 - поиск индикаторов компрометации (IoC);
- сбор журналов модуля;
- отправка сигнализации об инцидентах безопасности;
- настройка аппаратных идентификаторов;
- централизованное управление межсетевым экраном;
- централизованное управление компонентом СОВ, включая управление индикаторами компрометации (IoC) и правилами автоматического реагирования в рамках СОР;
- централизованное управление компонентом СКН;
- централизованное управление контролем устройств.

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

- отображение информации о состоянии модуля;
- синхронизация политик/пользователей¹;
- управление пользователями и группами пользователей¹ на модуле;
- синхронизация и управление политиками безопасности;

¹ Для модулей **СЗИ ВИ ИК4**. Для **СЗИ ВИ ИК5** доступно управление встроенными учетными записями пользователей на модуле и синхронизация встроенных учетных записей пользователей.

- настройка неактивного режима работы модуля²;
- управление заданиями на:
 - проверку обновлений;
 - получение конфигурации;
 - применение конфигурации;
 - получение отчета о параметрах безопасности **СЗИ ВИ**;
- сбор журналов модуля;
- открытие веб-интерфейса администрирования;
- отправка сигнализации об инцидентах безопасности;
- централизованное управление межсетевым экраном.

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.);
- удаленная авторизация пользователя;
- удаленное управление оболочкой администрирования **СДЗ Dallas Lock**;
- синхронизация политик/пользователей;
- управление пользователями и группами пользователей на модуле;
- управление политиками безопасности;
- управление заданиями на:
 - очистку журнала;
 - получение конфигурации;
 - применение конфигурации;
 - получение отчета об аппаратном обеспечении;
 - получение отчета о конфигурации;
 - сброс ДВК;
 - тестирование функций **СДЗ**;
- сбор журналов модуля;
- отправка сигнализации об инцидентах безопасности;
- взаимодействие с агентом ШОС³;
- настройка аппаратных идентификаторов.

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

- завершение работы и перезагрузка модуля;
- сбор журналов аудита в единую систему хранения **ЕЦУ** или базу данных;
- отображение информации о состоянии модуля (процент заполнения журнала, последнее подключение, контроль версии установленной сборки, результат последней проверки КЦ и т. д.);
- синхронизация политик/учетных записей;
- управление заданиями на:
 - очистку журнала;
 - получение конфигурации;
 - применение конфигурации;
 - получение отчета об аппаратном обеспечении;
 - получение отчета о конфигурации;
 - тестирование функций;
- разблокировка учетных записей;
- сигнализация о событиях НСД в реальном времени;
- запись в память токенов информации о пользователе в формате, поддерживаемом **СДЗ УБ Dallas Lock**.

² Для модулей **СЗИ ВИ ИК4**.

³ Для модулей **СДЗ ИК4**.

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

- завершение работы и перезагрузка модуля;
- отображение информации о состоянии модуля (состояние подключения, режим работы, имя шлюза безопасности, IP-адрес шлюза безопасности, анализ журналов событий 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);
- перевод шлюза безопасности в режиме кластера в состояние Master;
- сброс временных блокировок;
- однокомандное управление активацией и деактивацией аварийного режима;
- открытие веб-интерфейса администрирования;
- управление заданиями на:
 - обновление базы решающих правил;
 - создание и восстановление резервной копии;
 - сброс к заводским настройкам;
 - применение файла лицензии;
- сбор журналов модуля;
- сигнализация и мониторинг инцидентов безопасности с графическим отображением.

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

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

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

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

1.3 Рекомендации по применению ЕЦУ

Ниже (таблица 1) представлены рекомендации по применению существующих инструментов централизованного управления **ЕЦУ Dallas Lock** в зависимости от количества клиентских рабочих станций.

Таблица 1. Рекомендации по применению

Количество клиентских APM	Кластер серверов ЕЦУ	Подчиненные ДБ	Хранение журналов во внешней БД (PostgreSQL)	Выгрузка событий в SIEM-систему
Менее 500			=	
500 – 5 000	=	=	+	=
5 000 – 10 000	+	=	+	=

10 000 – 50 000 и более	+	+	+	+
----------------------------	---	---	---	---

"=" — опционально, "+" — рекомендуется применять

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 Live USB, работающих на 64-битной архитектуре процессоров под управлением операционных систем семейства Windows (x64):

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

и семейства GNU Linux⁴ (x64):

- Debian 10.x;
- Debian 11.x;
- Debian 12.x;
- Ubuntu 18.04 LTS;
- Ubuntu 20.04 LTS;
- Ubuntu 22.04 LTS;
- Ubuntu 24.04 LTS;
- Astra Linux Common Edition (Open) 2.12;
- Astra Linux Special Edition (Смоленск) 1.6, 1.7, 1.8;
- Альт Сервер 9;
- Альт Сервер 10.0, 10.1, 10.2, 10.4;
- Альт 8 СП Сервер 10;
- Альт Рабочая Станция 9.x;
- Альт Рабочая Станция 10.0, 10.1, 10.2, 10.4;
- Альт Рабочая Станция К 10.0, 10.1, 10.3, 10.4;
- Альт 8 СП Рабочая Станция 10;
- РЕД ОС 7.3 Муром;
- РЕД ОС 8;
- ROSA FRESH DESKTOP 12.

На ОС должны быть установлены все актуальные обновления. В противном случае может появиться ошибка с просьбой установить обновления и повторить установку **ЕЦУ**.

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

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

В Таблица 2 представлены рекомендации в части минимальных системных требований для оптимальной работы в зависимости от состава домена **ЕЦУ**.

Таблица 2. Минимальные системные требования

Состав ЕЦУ			
Кластер: нет АРМ: 2 тысяч УЗ: 5 тысяч Назн. АИ: 5 тысяч Зарег. СКН: 10 тысяч	Кластер: нет АРМ: 8 тысяч УЗ: 20 тысяч Назн. АИ: 20 тысяч Зарег. СКН: 40 тысяч	Кластер: нет АРМ: 20 тысяч УЗ: 50 тысяч Назн. АИ: 50 тысяч Зарег. СКН: 100 тысяч	Кластер: да АРМ: 50 тысяч УЗ: 125 тысяч Назн. АИ: 125 тысяч Зарег. СКН: 250 тысяч

⁴ Для инсталляции и работы с консолью ЕЦУ под ОС семейства Linux требуется графическая оболочка.

Минимальные системные требования			
Компонент «Служба ЕЦУ» ОС: Клиентская Процессор: Intel Core i5/ Intel Xeon E3 (8 ядер ⁵) Оперативная память: 16 ГБ Накопитель: SSD Свободное пространство: 50 ГБ	Компонент «Служба ЕЦУ» ОС: Клиентская Процессор: Intel Core i7/ Intel Xeon E5 (8 ядер ⁵) Оперативная память: 32 ГБ Накопитель: SSD Свободное пространство: 50 ГБ	Компонент «Служба ЕЦУ» ОС: Серверная Процессор: Intel Core i7/ Intel Xeon E5 (16 ядер ⁵) Оперативная память: 32 ГБ Накопитель: SSD Свободное пространство: 50 ГБ	Компонент «Служба ЕЦУ» ОС: Серверная Процессор: Intel Core i7/ Intel Xeon E5 (16 ядер ⁵) Оперативная память: 32 ГБ Накопитель: SSD Свободное пространство: 50 ГБ
Компонент «Консоль ЕЦУ» ОС: Клиентская Процессор: Intel Core i5/ Intel Xeon E3 (4 ядра ⁵) ОЗУ: 8 ГБ Накопитель: HDD Свободное пространство: 2 ГБ	Компонент «Консоль ЕЦУ» ОС: Клиентская Процессор: Intel Core i5/ Intel Xeon E3 (4 ядра ⁵) ОЗУ: 8 ГБ Накопитель: HDD Свободное пространство: 2 ГБ	Компонент «Консоль ЕЦУ» ОС: Клиентская Процессор: Intel Core i5/ Intel Xeon E3 (4 ядра ⁵) ОЗУ: 16 ГБ Накопитель: HDD Свободное пространство: 2 ГБ	Компонент «Консоль ЕЦУ» ОС: Клиентская Процессор: Intel Core i5/ Intel Xeon E3 (4 ядра ⁵) ОЗУ: 16 ГБ Накопитель: HDD Свободное пространство: 2 ГБ
Минимальное пространство для хранения журналов на каждую тысячу клиентов (в течение 1 года): 1 ТБ			
Минимальные системные требования для компьютера с установленной БД PostgreSQL ⁶			
ОС: Клиентская Процессор: Intel Core i5/Intel Xeon E3 (8 ядер ⁵) ОЗУ: 16 ГБ Накопитель: SSD			



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



Для хранения журналов во внешней базе данных необходимо использовать PostgreSQL версии 13 или выше, или СУБД Jatoba.

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

- электронные ключи Touch Memory (iButton)⁷:
 - DS-1992;
 - DS-1993;
 - DS-1995;
 - DS-1996;

⁵ Физические ядра без учета Hyper-Threading.

⁶ Внешнюю базу данных рекомендуется использовать при количестве клиентов от 10 тысяч.

⁷ Для ОС Linux электронный ключ Touch Memory (iButton) поддерживается только для чтения, то есть его можно только назначить пользователю. Запись учетных данных пользователя на такой идентификатор не производится.

- USB-ключи Aladdin eToken⁸;
 - Pro/Java;
 - 72K;
- смарт-карты Aladdin eToken Pro/SC;
- USB-ключи Guardant ID 2.0;
- USB-ключи и смарт-карты Рутокен (Rutoken):
 - Рутокен (Rutoken);
 - Рутокен (Lite);
 - Рутокен ЭЦП;
 - Рутокен ЭЦП 2.0;
 - Рутокен ЭЦП 3.0;
 - Рутокен ЭЦП PKI;
 - Рутокен S⁹;
- USB-ключи и смарт-карты JaCarta:
 - JaCarta SF/ГОСТ;
 - JaCarta ГОСТ;
 - JaCarta PKI;
 - JaCarta PKI/Flash;
 - JaCarta LT;
 - JaCarta PRO;
 - JaCarta-2 PKI/ГОСТ;
 - JaCarta-2 ГОСТ;
- USB-ключи и смарт-карты ESMART:
 - ESMART Token;
 - ESMART Token ГОСТ;
 - ESMART 64K.

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



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



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



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



При использовании аппаратного идентификатора eToken совместно с SafeNet на операционных системах Linux необходимо дополнительно установить пакеты *libssl-dev* (deb based linux) или *libssl-devel* (rpm based linux).

⁸ Для USB-ключа eToken 32Кб обеспечивается только возможность усиления механизма аутентификации. Запись учетных данных пользователя на такой идентификатор не производится в силу ограниченного объема доступной памяти аппаратного идентификатора.

⁹ Для ОС Linux недоступно форматирование ключа.



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

2.2 Установка ЕЦУ Dallas Lock

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



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



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 потребуются 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 А-запись с именем сервера **ЕЦУ**, закодированным в пьюникоде (punycode).



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 *tracert <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.



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

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

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

Подробнее о настройке способа хранения журналов описано в разделе [«Параметры журналов»](#).



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

2.2.1 Порядок установки ЕЦУ Dallas Lock в ОС семейства Windows



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.

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».`



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

Для установки **ЕЦУ Dallas Lock** в ОС семейства Windows необходимо:

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

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

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



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**.



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

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

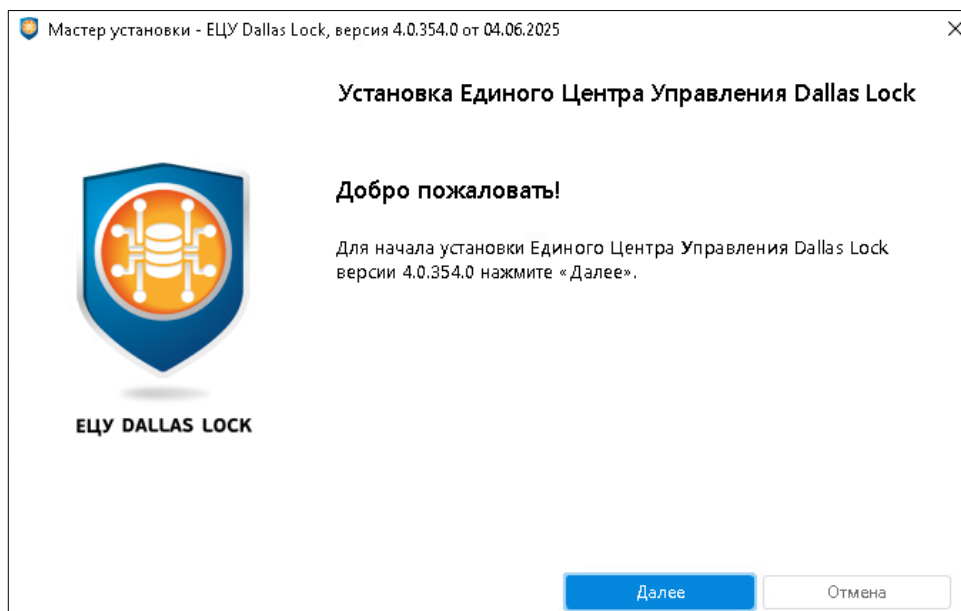


Рис. 1. Окно начала установки **ЕЦУ Dallas Lock**

Для продолжения установки нажать кнопку **Далее**.

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

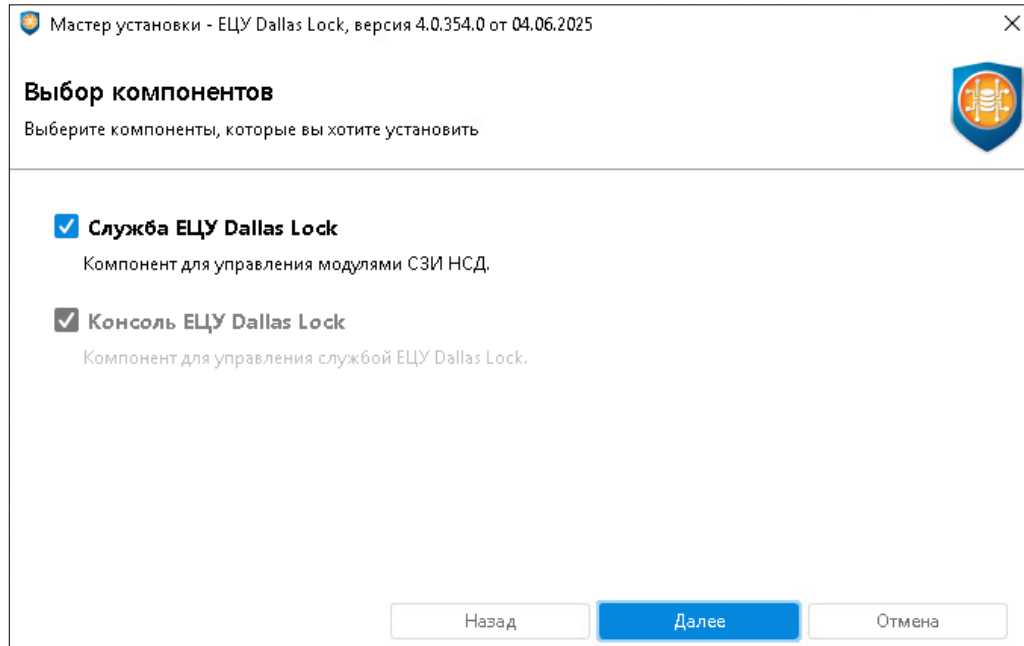


Рис. 2. Выбор компонентов для установки ЕЦУ Dallas Lock



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

4. На следующем шаге установки необходимо предъявить аппаратный ключ или файл лицензии, направляемый вместе с кодом технической поддержки по электронным средствам связи, для применения лицензии на устанавливаемый сервер (рис. 3).

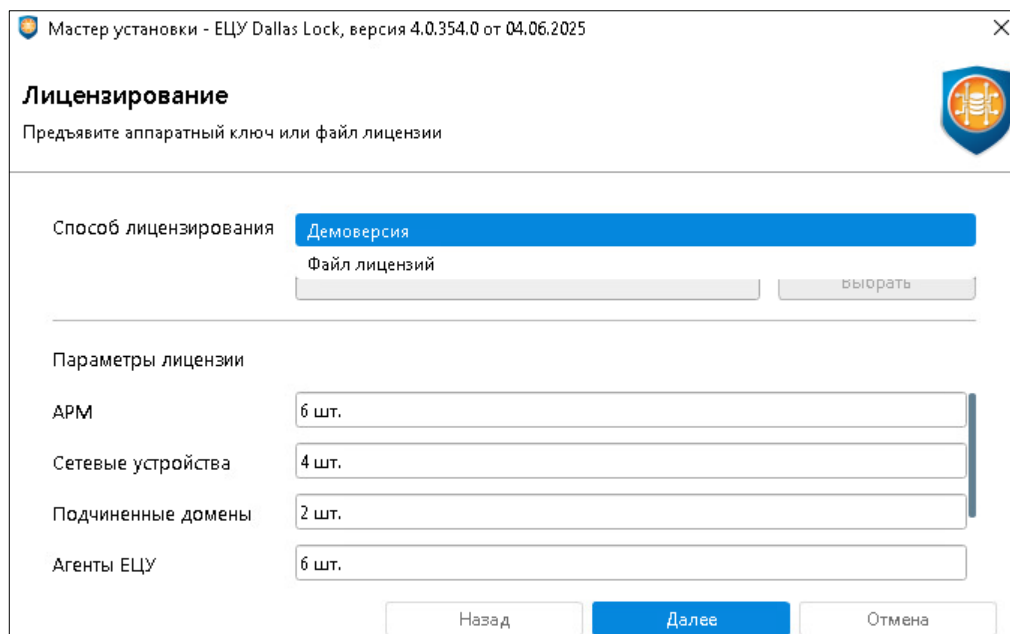


Рис. 3. Применение лицензии



Выбор в качестве способа лицензирования аппаратного ключа станет доступен после предъявления на ТС соответствующего аппаратного ключа.



Применить лицензию возможно и после установки **ЕЦУ**: требуется установить демоверсию **ЕЦУ Dallas Lock** и добавить лицензию в окне **Состояние лицензии** (см. [«Настройки лицензирования»](#)).

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»](#) соответственно.

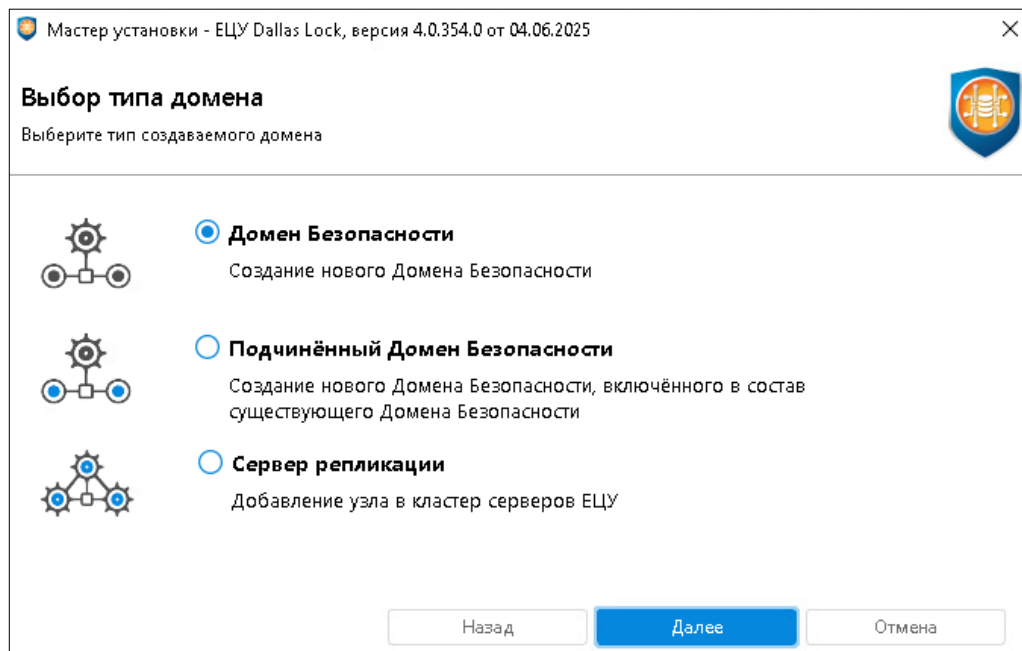
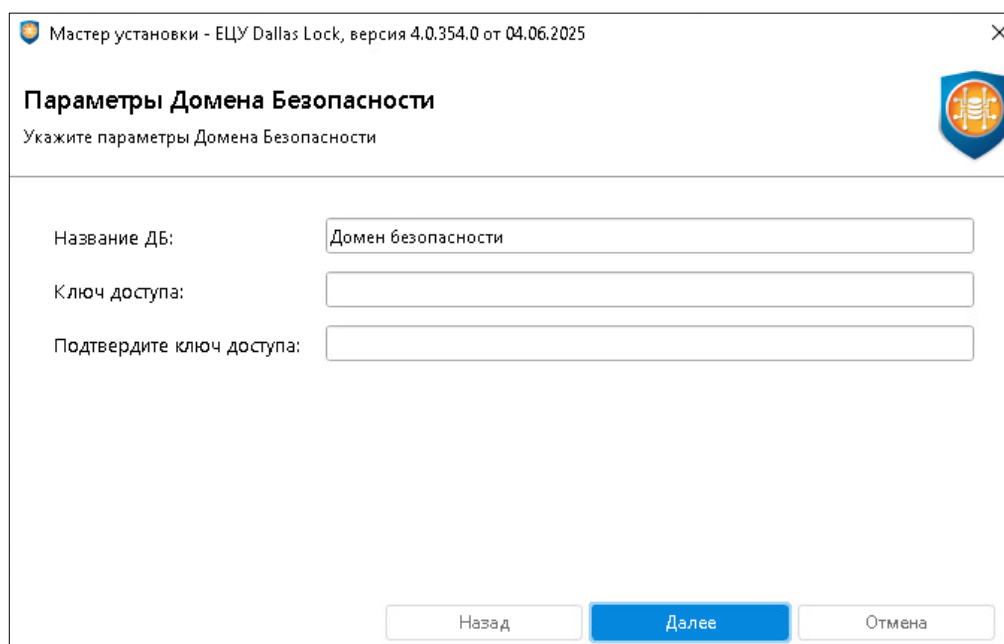


Рис. 4. Выбор типа создаваемого домена

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



Мастер установки - ЕЦУ Dallas Lock, версия 4.0.354.0 от 04.06.2025

Параметры Домена Безопасности

Укажите параметры Домена Безопасности

Название ДБ:

Ключ доступа:

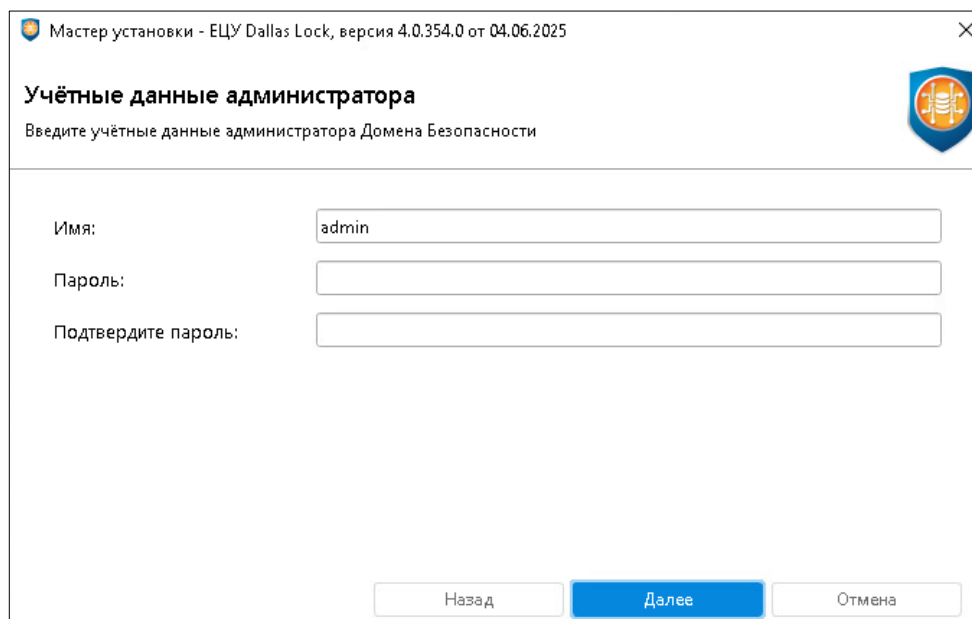
Подтвердите ключ доступа:

Рис. 5. Настройка параметров ДБ



Ключ доступа к ДБ предназначен для ввода новых объектов в ДБ и для подключения консоли управления (КУ) к серверу ЕЦУ.

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



Мастер установки - ЕЦУ Dallas Lock, версия 4.0.354.0 от 04.06.2025

Учётные данные администратора

Введите учётные данные администратора Домена Безопасности

Имя:

Пароль:

Подтвердите пароль:

Рис. 6. Настройка параметров учетной записи администратора ДБ

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

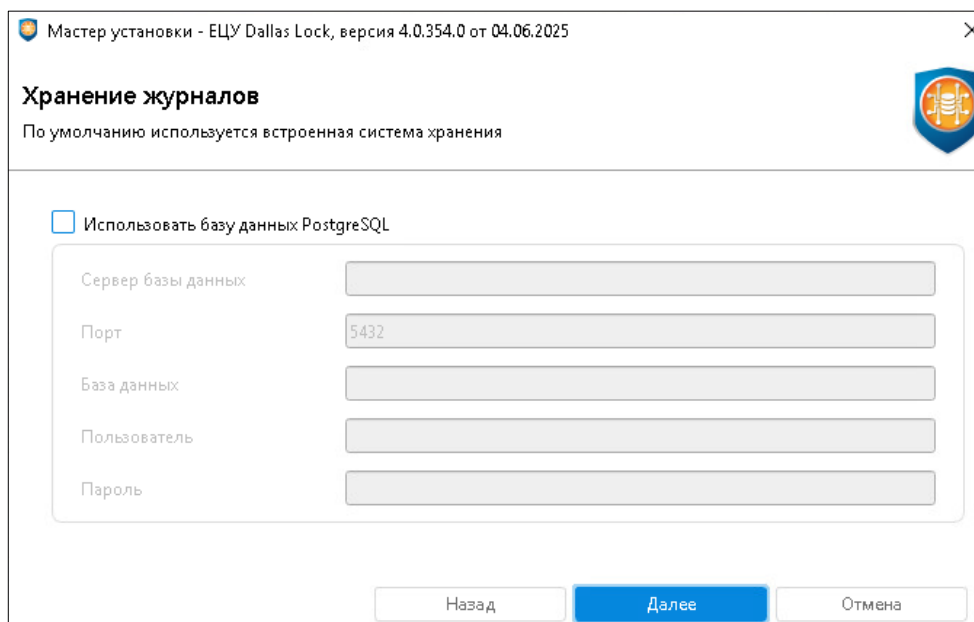


Рис. 7 Настройка базы данных PostgreSQL



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>.`



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

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

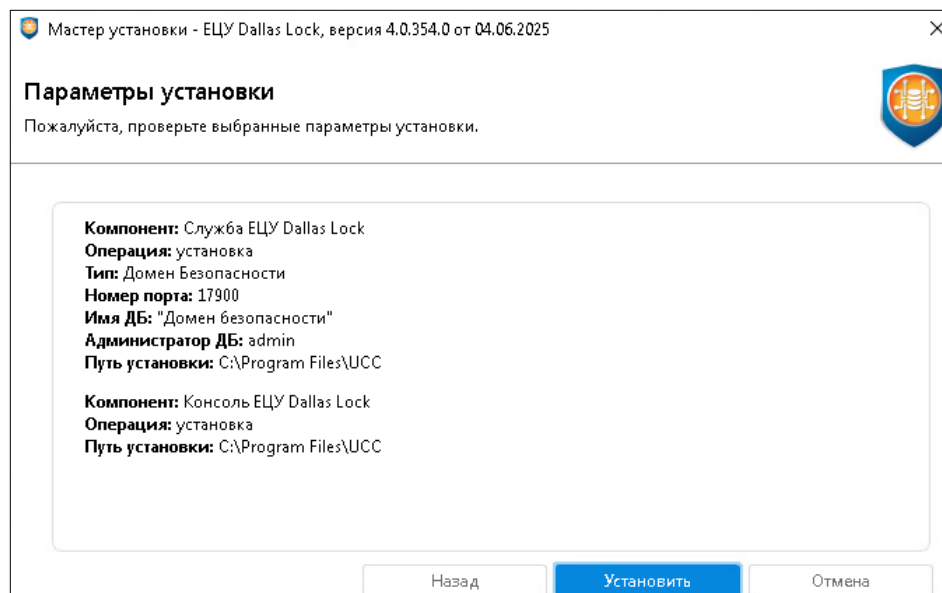


Рис. 8. Проверка параметров установки

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

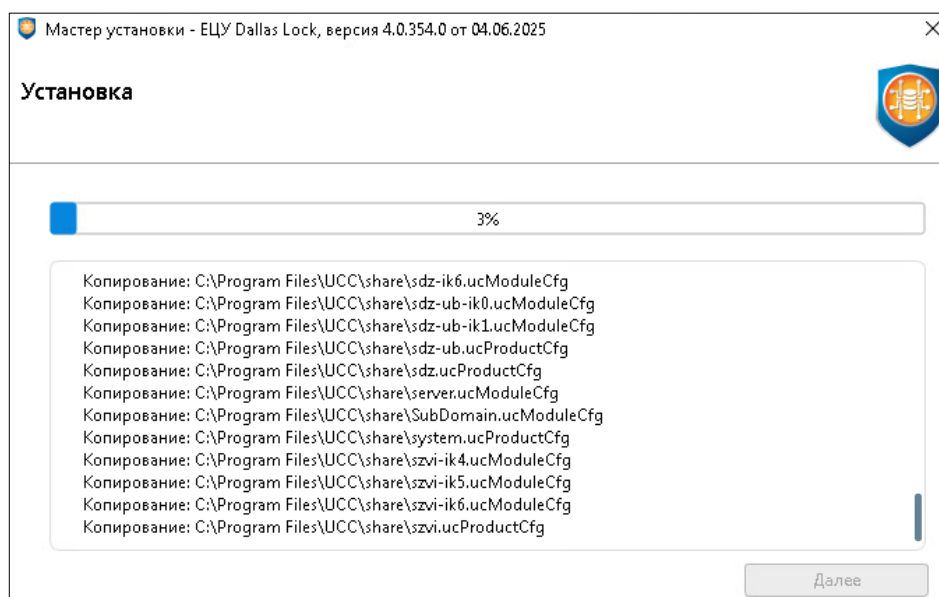


Рис. 9. Процесс установки ЕЦУ Dallas Lock

11. Нажать кнопку **Завершить** (рис. 10).

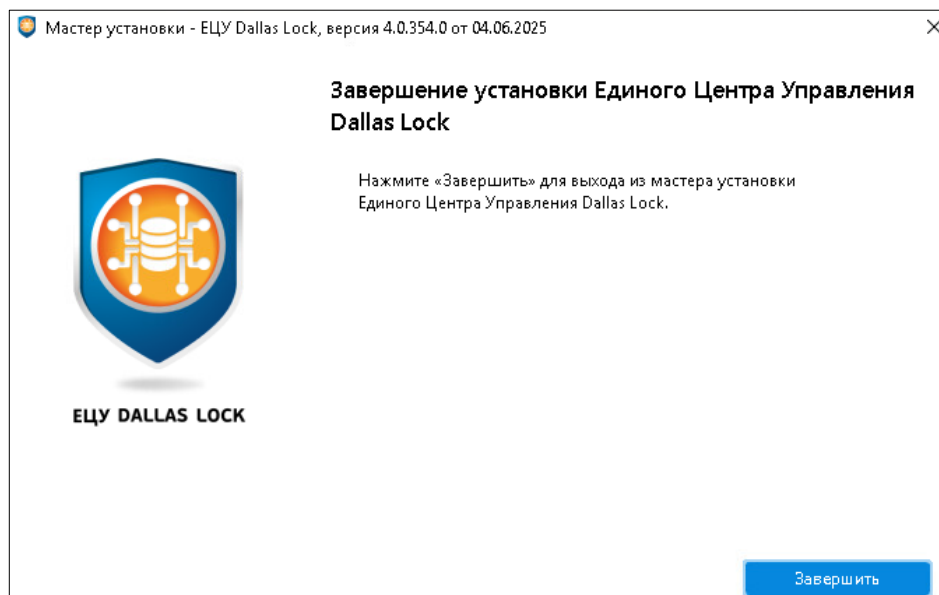


Рис. 10. Завершение процесса установки

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

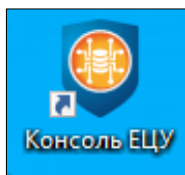


Рис. 11. Ярлык консоли ЕЦУ Dallas Lock

2.2.2 Порядок установки ЕЦУ Dallas Lock в ОС семейства Linux



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



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



Если в процессе установки **ЕЦУ Dallas Lock** планируется использовать лицензию, записанную на АИ Rutoken Lite, то необходимо перед установкой заранее установить драйверы производителя¹⁰. Для этого:

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



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



Для корректной установки **ЕЦУ** на операционных системах РЕД ОС требуется наличие пакетного менеджера yum. Данный пакетный менеджер следует устанавливать на ОС до первоначальной попытки установки ЕЦУ, иначе процесс установки **ЕЦУ** будет завершаться с ошибкой.

Для установки **ЕЦУ Dallas Lock** в ОС семейства Linux необходимо:

1. Скопировать в домашний каталог пользователя установочный файл «ucclnst», 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 «ucclnst» исполняемым:

- либо с помощью команды `ls -l`.

Пример:

`ls -l <enter>`

`rw-rw----` отображаются последовательно без пробелов флаги владельца, флаги группы, флаги всех остальных пользователей. В данном примере файл не является исполняемым ни для владельца, ни для группы, ни для всех остальных пользователей.

- либо можно открыть свойства файла, перейти на вкладку *Права* и убедиться, что в поле *Выполнение* поставлен флаг (рис. 12).

Если файл не является исполняемым, необходимо поставить флаг в поле *Выполнение*. Или использовать команду `chmod a+x <путь к файлу>.run`.

¹⁰ Для работы **ЕЦУ Dallas Lock** на Astra Special Edition (Смоленск) 1.6 и Astra Special Edition (Смоленск) 1.7 в режиме ЗПС необходимо использовать драйверы производителя версии 2.4.0.0.

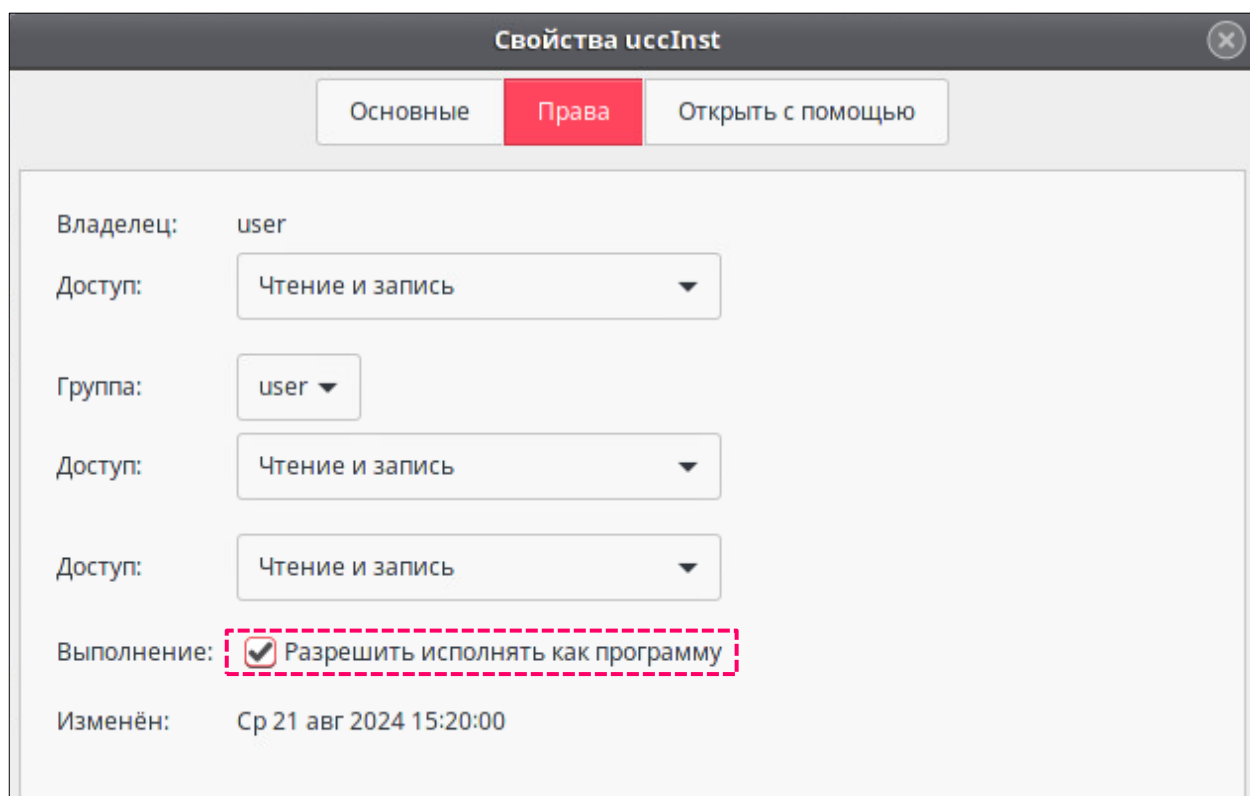


Рис. 12. Добавление прав на выполнение файла программы

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

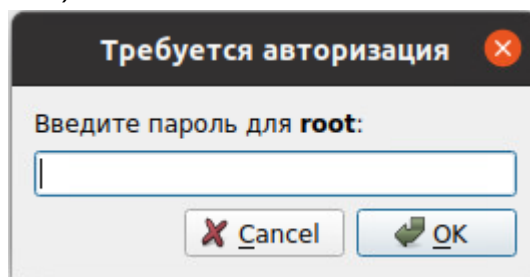


Рис. 13. Запуск программы установки

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

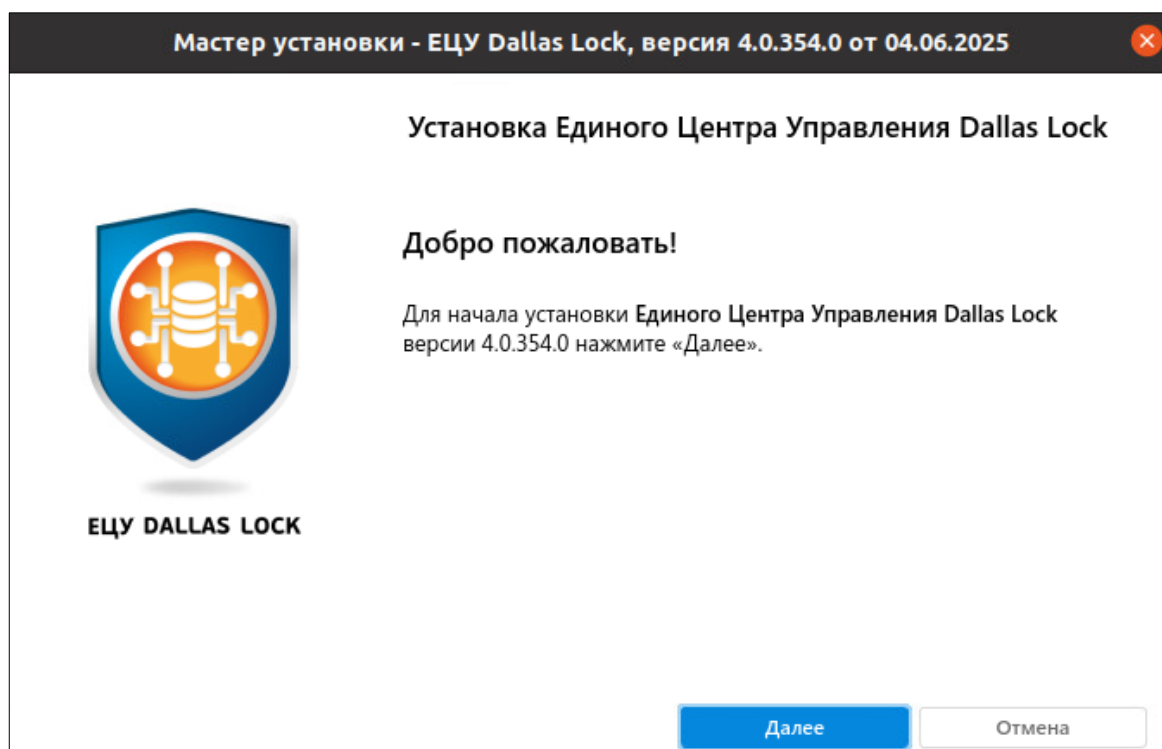


Рис. 14. Окно начала установки ЕЦУ Dallas Lock

5. Выбрать компоненты, которые будут установлены (рис. 15).

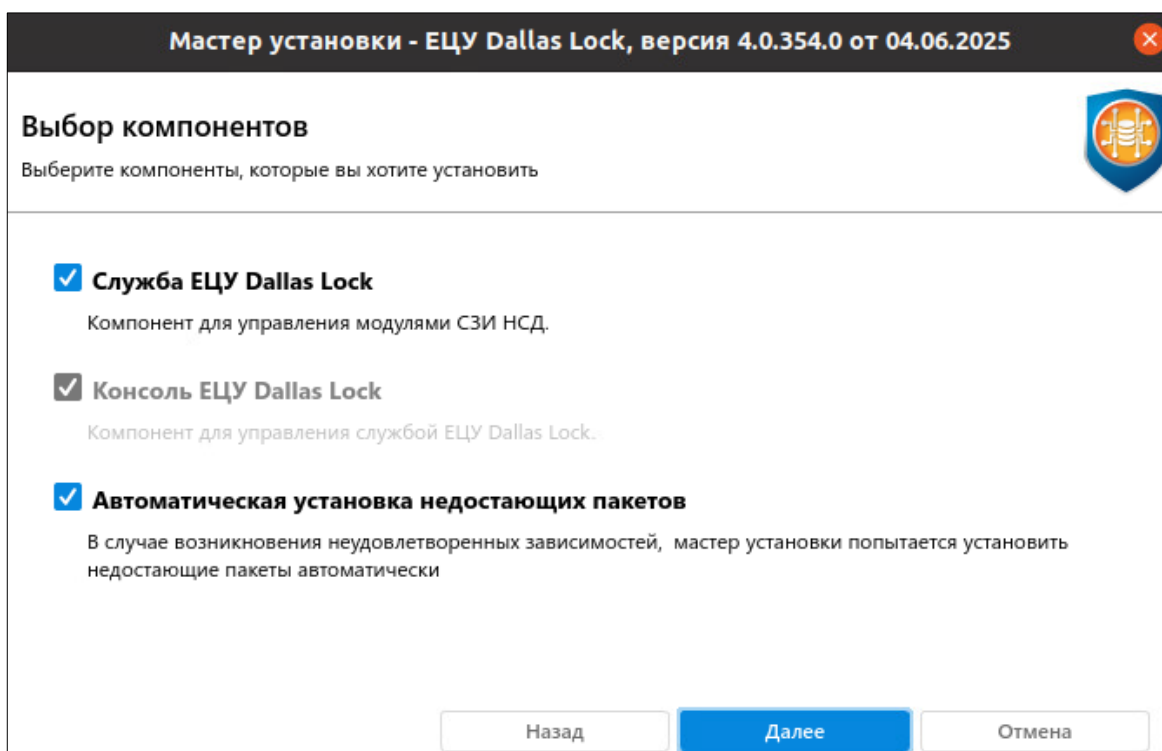


Рис. 15. Выбор компонентов для установки ЕЦУ Dallas Lock



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

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»](#)).



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

В процессе установки **ЕЦУ Dallas Lock** выполняется проверка наличия необходимых сторонних пакетов. При отсутствии пакетов в журнале мастера установки появляется запись с указанием отсутствующих пакетов.

Необходимо повторно запустить мастер установки, в диалоговом окне выбора компонентов для установки нажать чекбокс *Автоматическая установка недостающих пакетов* или установить их самостоятельно:

- для Debian 10.x, Debian 11.x, Debian 12.x:
 - libsassl2-modules-gssapi-mit
 - pcscd
 - libglib2.0-0
 - libsmbclient
 - libxkbcommon-x11-0
- для Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 24.04 LTS:
 - libsassl2-modules-gssapi-mit
 - pcscd
 - libglib2.0-0
 - libsmbclient
 - dbus-x11
- для Astra Linux Common Edition (Орел) 2.12, Astra Linux Special Edition (Смоленск) 1.6 и Astra Linux Special Edition (Смоленск) 1.7:
 - libsassl2-modules-gssapi-mit
 - pcscd
 - libglib2.0-0
 - libsmbclient
- для Альт Рабочая Станция 9.x, Альт Рабочая Станция (10.0, 10.1, 10.2), Альт Рабочая Станция К (10.0, 10.1, 10.3), Альт 8 СП Рабочая Станция 10, Альт Сервер 9, Альт Сервер (10.0, 10.1, 10.2) и Альт 8 СП Сервер 10:
 - libsassl2-plugin-gssapi
 - pcsc-lite
 - glib2
 - libgio
 - samba-libs
- для РЕД ОС 7.3 Муром и РЕД ОС 8:
 - cyrus-sasl
 - pcsc-lite
 - glib2
 - libsmbclient
- для ROSA FRESH DESKTOP 12:
 - pcsc-lite
 - lib64glib2.0_0
 - lib64smbclient0.

После завершения процесса установки **ЕЦУ Dallas Lock** в списке приложений появится ярлык Консоли **ЕЦУ Dallas Lock Консоль ЕЦУ** (рис. 16).



Рис. 16. Ярлык консоли ЕЦУ Dallas Lock



1) Если на АРМ с Linux уже установлены сторонние **СЗИ** или драйверы на другие аппаратные идентификаторы, и при этом в процессе установки **ЕЦУ** произошла ошибка установки, которая связана с пакетным менеджером, то может помочь команда `sudo apt --fix-broken install`.

2) Если в процессе установки **ЕЦУ** на Linux возникает ошибка вида: «...error whiel loading shared libraries: libxcb-xkb.so.1: cannot open shared object file: No such file or directory», то необходимо перед установкой вручную установить пакет «libxcb-xkb1».

2.2.3 Порядок установки ЕЦУ Dallas Lock на ОС без графического интерфейса

ЕЦУ возможно установить на операционную систему (ОС) без графического интерфейса (GUI). В командной строке в качестве атрибутов к команде `.ucclnst` можно указывать следующие ключи для установки (параметры мастера установки) (Таблица 3):

Таблица 3. Атрибуты установки ЕЦУ Dallas Lock на ОС без GUI

Атрибут	Описание
<code>--help</code>	Вывод на экран справки по параметрам установки Пример: <code>.ucclnst --help <enter></code>
<code>--version</code>	Возврат версии мастера
<code>--log=PATH</code>	Путь к файлу, куда будет записываться лог установки
<code>--no-gui</code>	Запуск мастера без графического интерфейса
<code>--force-update</code>	Если на АРМ уже установлен ЕЦУ предыдущей версии, то выполняет обновление (без этого флага вернет ошибку)
<code>--install-libs</code>	Автоматическая установка недостающих пакетов для ОС семейства GNU/Linux
<code>--component=all</code>	Выбор устанавливаемых компонентов — установка Консоли и Службы ЕЦУ (по умолчанию)
<code>--component=console</code>	Выбор устанавливаемых компонентов — установка только Консоли ЕЦУ
<code>--license=demo</code>	Выбор лицензии — демо-лицензия (по умолчанию)
<code>--license=token</code>	Выбор лицензии — использует токен для лицензирования ЕЦУ (при отсутствии токена с корректной лицензией выдает ошибку)
<code>--domain-type=standalone</code>	Выбор типа домена — создание нового Домена Безопасности (по умолчанию)
<code>--domain-type=subdomain</code>	Выбор типа домена — создание нового подчиненного Домена Безопасности

<code>--domain-type=cluster</code>	Выбор типа домена — добавление узла в кластер ЕЦУ
<code>--domain-name=TEXT</code>	Указать название нового Домена Безопасности
<code>--access-key=TEXT</code>	Указать ключ доступа нового Домена Безопасности
<code>--admin-login=TEXT</code>	Указать логин администратора
<code>--admin-password=TEXT</code>	Указать пароль администратора
<code>--journal-storage=internal</code>	Выбор типа хранилища журналов — встроенная БД (по умолчанию)
<code>--journal-storage=pg</code>	Выбор типа хранилища журналов — сервер PostgreSQL
<code>--db-server=USER:PWD@ADDRESS:PORT/DB_NAME</code>	Указать параметры подключения к БД
<code>--parent-domain=ACCESS_KEY@ADDRESS</code>	Указать параметры родительского Домена Безопасности
<code>--cluster-server=ACCESS_KEY@ADDRESS</code>	Указать параметры одного из серверов кластера ЕЦУ



Для установки **ЕЦУ** на серверные ОС ALT Linux без графического интерфейса (GUI) необходимо заранее вручную установить пакет «*xdg-utils*».

2.3 Удаление ЕЦУ Dallas Lock



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

2.3.1 Порядок удаления ЕЦУ Dallas Lock в ОС семейства Windows

Правом на удаление **ЕЦУ Dallas Lock** обладает пользователь с правами администратора ОС. В ОС Windows необходимо открыть **Пуск** → **Панель управления** → **Программы и компоненты**. В появившемся окне из списка выбрать программу **ЕЦУ Dallas Lock**, нажать **Удалить/Изменить** и подтвердить удаление (рис. 17).

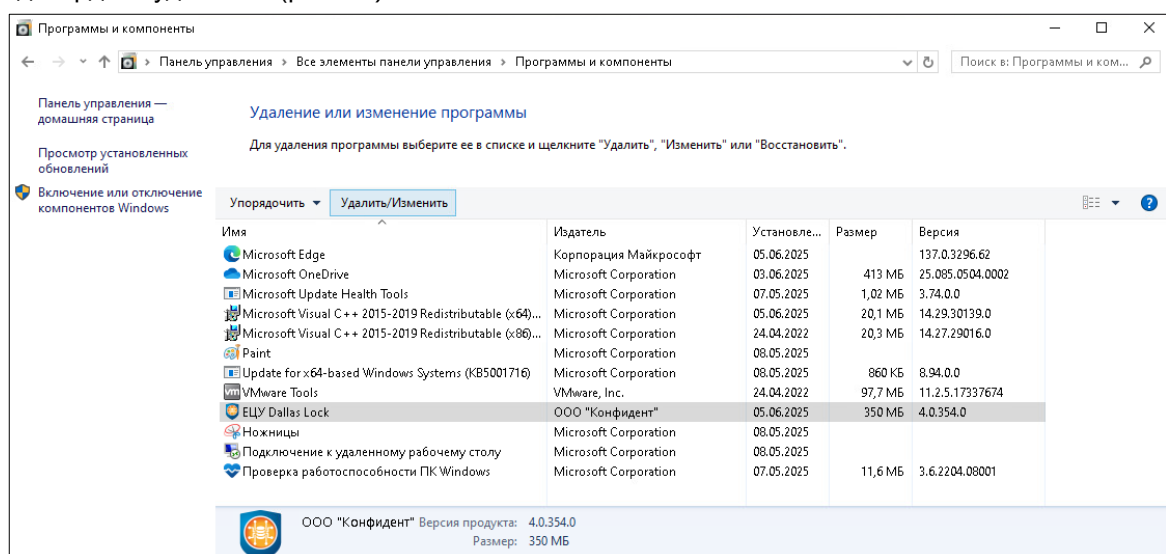


Рис. 17. Удаление ЕЦУ Dallas Lock

1. После подтверждения запустится мастер удаления **ЕЦУ Dallas Lock** (рис. 18). Для продолжения удаления нажать кнопку **Далее**.

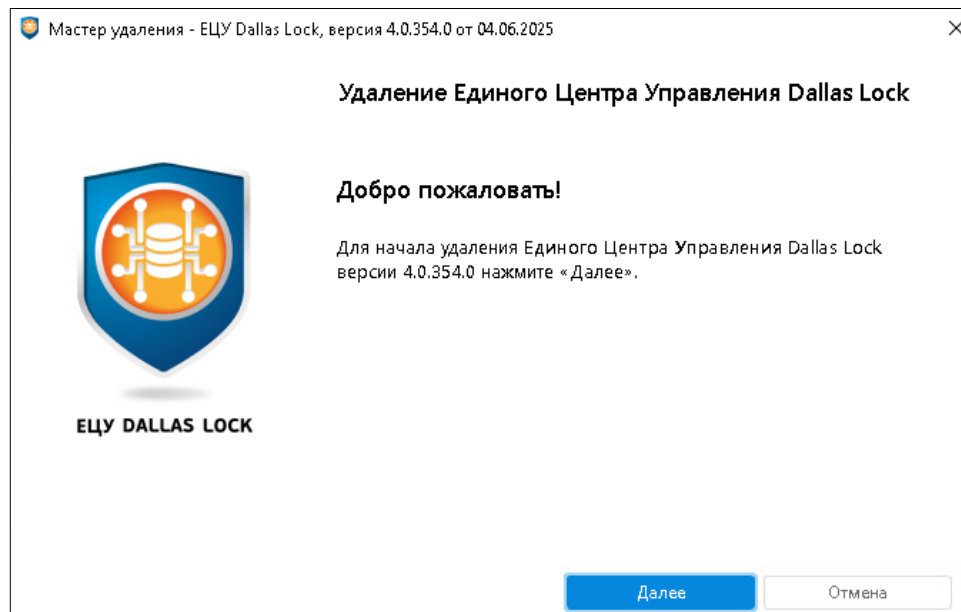


Рис. 18. Окно начала удаления ЕЦУ Dallas Lock

2. Выбрать компоненты, которые будут удалены (рис. 19).

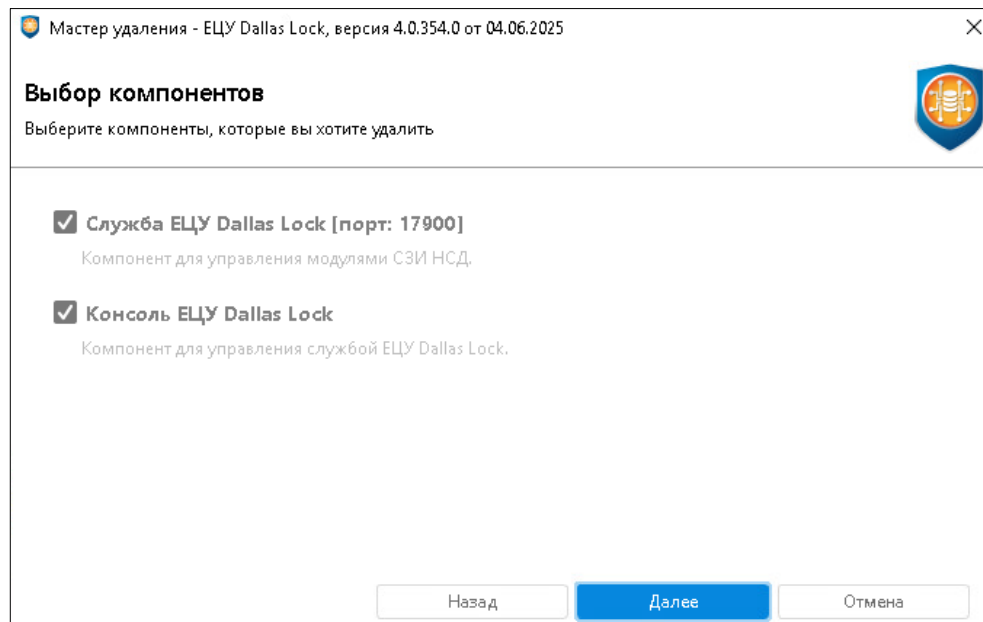


Рис. 19. Выбор компонентов для удаления ЕЦУ Dallas Lock

3. Подтвердить удаление конфигурационных файлов (рис. 20).

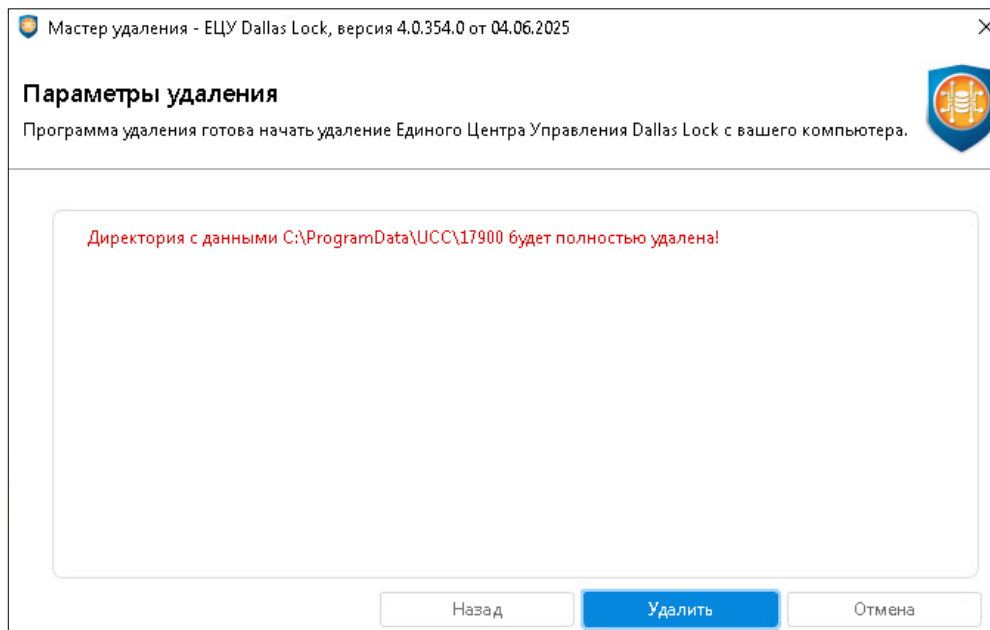


Рис. 20. Параметры удаления

4. Далее возможно наблюдать за процессом удаления (рис. 21). Если процесс прошел без ошибок, необходимо нажать кнопку **Далее**, чтобы перейти к окну завершения процесса удаления.

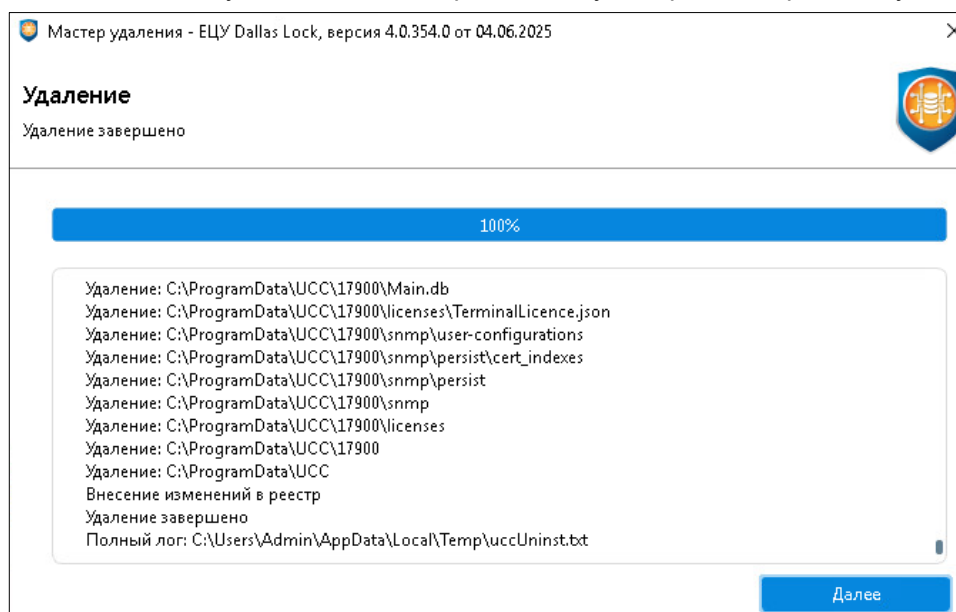


Рис. 21. Процесс удаления ЕЦУ Dallas Lock

5. Нажать кнопку **Завершить** (рис. 22).

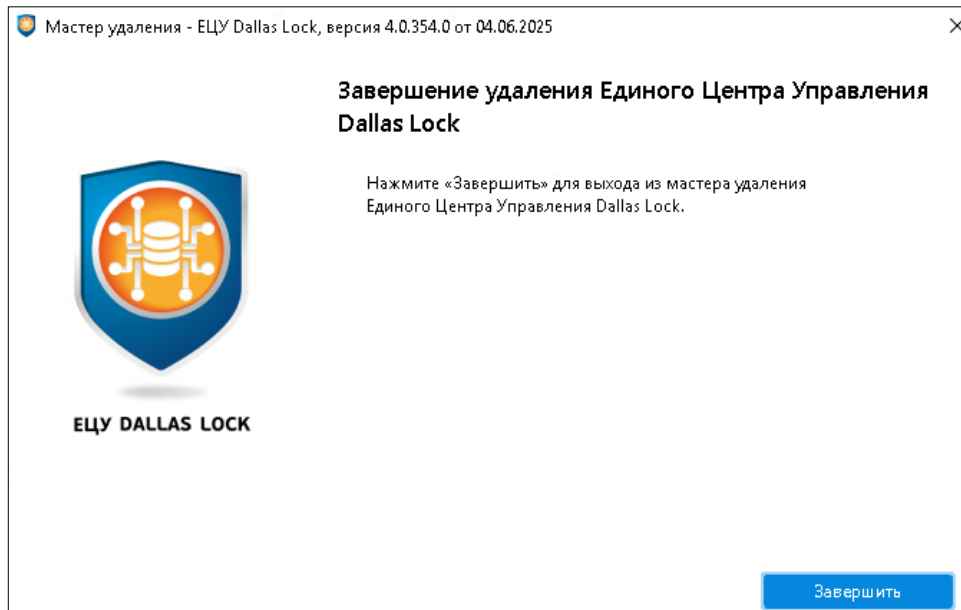


Рис. 22. Завершение процесса удаления

2.3.2 Порядок удаления ЕЦУ Dallas Lock в ОС семейства Linux

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

1. Для удаления **ЕЦУ Dallas Lock** необходимо запустить исполняемый файл *uccUninst*, который расположен в директории */opt/UCC/bin/uccUninst* в терминале. Для этого необходимо выполнить в терминале команду:
`sudo /opt/UCC/ bin/uccUninst`
2. После выполнения команды запустится окно мастера удаления **ЕЦУ Dallas Lock** (рис. 23).

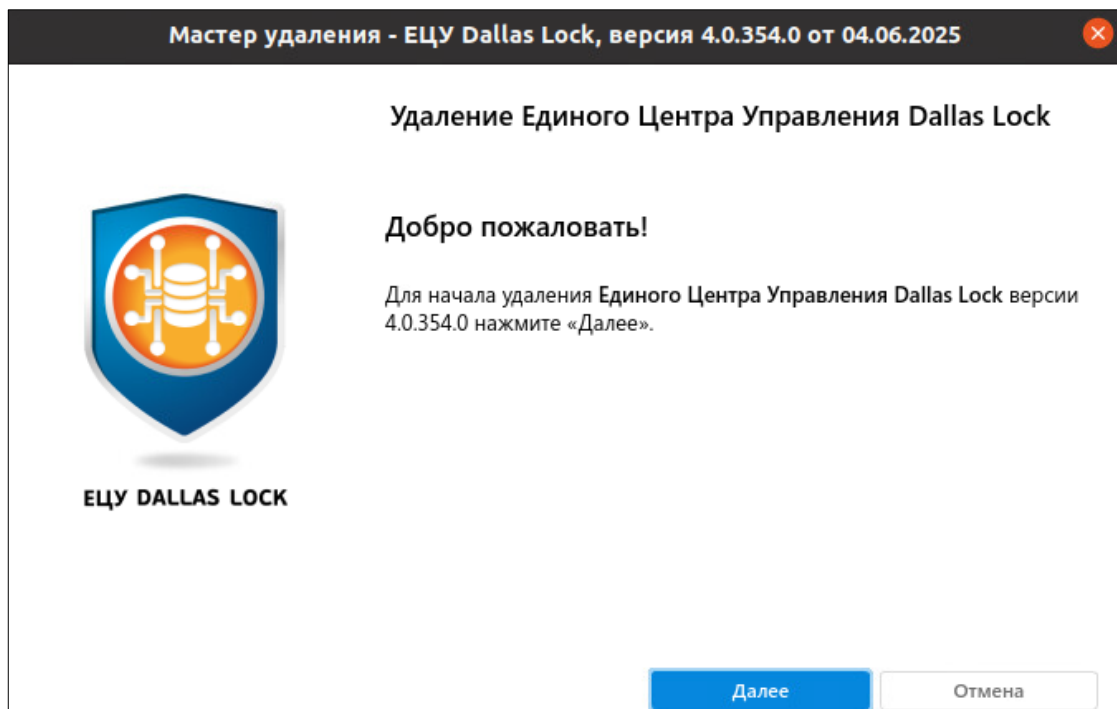


Рис. 23. Окно начала удаления ЕЦУ Dallas Lock

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 Управление конфигурацией

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

2.4.1 Сохранение конфигурации ЕЦУ

Для сохранения конфигурации **ЕЦУ Dallas Lock** в ОС семейства Windows или Linux необходимо открыть главное меню Консоли **ЕЦУ**  и выбрать пункт → **Управление конфигурацией**.

В блоке *Сохранение конфигурации ЕЦУ* (рис. 24) нужно задать путь к файлу конфигурации с помощью кнопки **Выбрать**, после нажать кнопку **Сохранить**.

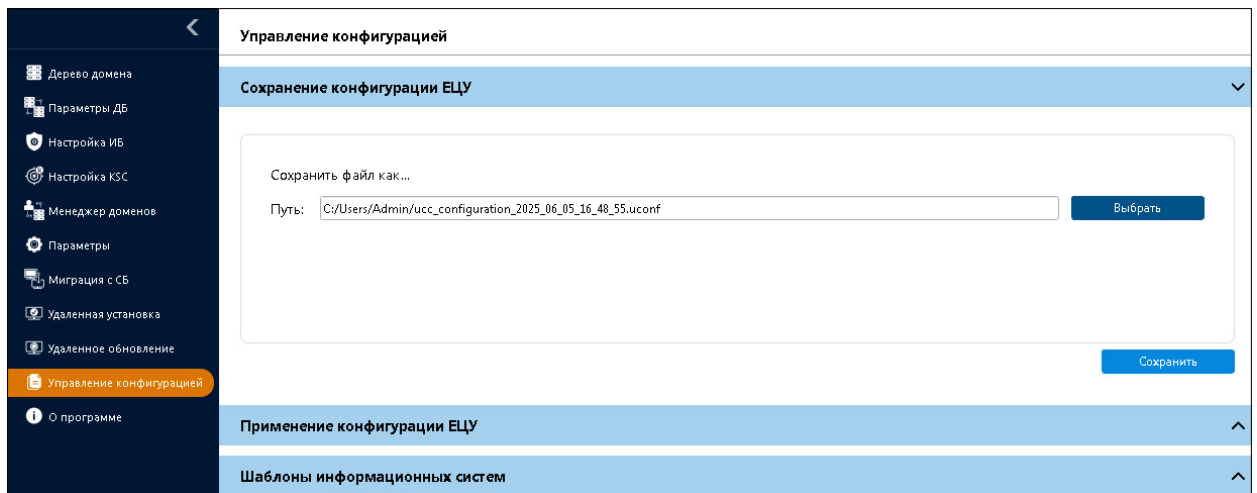


Рис. 24. Сохранение конфигурации



При незавершенном процессе миграции сохранить и применить конфигурацию не получится. Кнопки будут неактивны.

2.4.2 Применение конфигурации ЕЦУ



Применение конфигурации приведет к удалению всех данных домена безопасности.

Для применения конфигурации **ЕЦУ Dallas Lock** в ОС семейства Windows или Linux необходимо открыть главное меню Консоли **ЕЦУ**  и выбрать пункт → **Управление конфигурацией**.

В блоке *Применение конфигурации ЕЦУ* (рис. 25) необходимо указать путь к файлу конфигурации, для этого нужно:

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

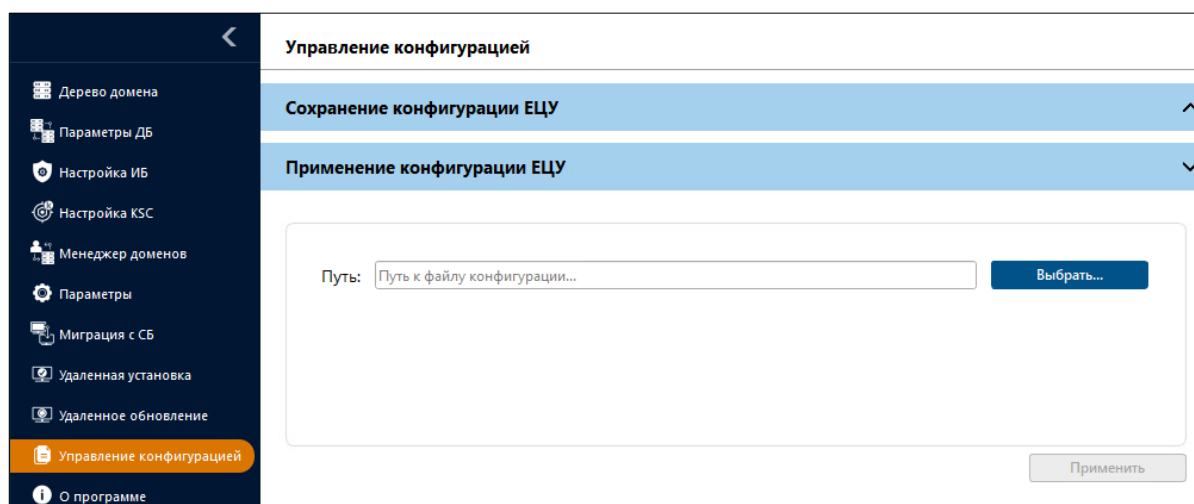


Рис. 25. Применение конфигурации

После применения конфигурации модули смогут выйти на связь с сервером **ЕЦУ** только в случае соответствия имени домена (FQDN) и IP-адреса старого и нового сервера **ЕЦУ**.

2.4.3 Шаблоны информационных систем

В **ЕЦУ Dallas Lock** реализована возможность применения шаблонов безопасности, содержащих в себе конкретные настройки под требования нормативных документов.



Шаблоны влияют только на те политики, для которых предусмотрены требования согласно нормативным документам, значения других политик выставляются администратором самостоятельно (либо используются по умолчанию) и при применении шаблонов остаются без изменений.

Для применения шаблона безопасности необходимо открыть главное меню Консоли **ЕЦУ** и выбрать пункт → **Управление конфигурацией**.

В блоке *Шаблоны информационных систем* необходимо выбрать из списка подходящий шаблон (или несколько шаблонов – выбираются из разных категорий) требуемой категории:

- шаблоны автоматизированных систем — устанавливаются параметры для АС, соответствующие требованиям к АС классов защищенности 1Б, 1В, 1Г и 1Д согласно РД ФСТЭК АС;
- шаблоны государственных информационных систем — устанавливаются параметры для ГИС, соответствующие требованиям к ГИС 1, 2 и 3 класса защищенности согласно Приказу ФСТЭК России № 17;
- шаблоны информационных систем персональных данных — устанавливаются параметры для ИСПДн, соответствующие требованиям к ИСПДн 1-4 уровня защищенности согласно Приказу ФСТЭК России № 21.



При совместном применении нескольких шаблонов для политик назначаются суммированные (более строгие) настройки — значения, накладывающие большие ограничения.

Изменяемые по шаблонам политики и их значения приведены в приложении (см. Приложение А).

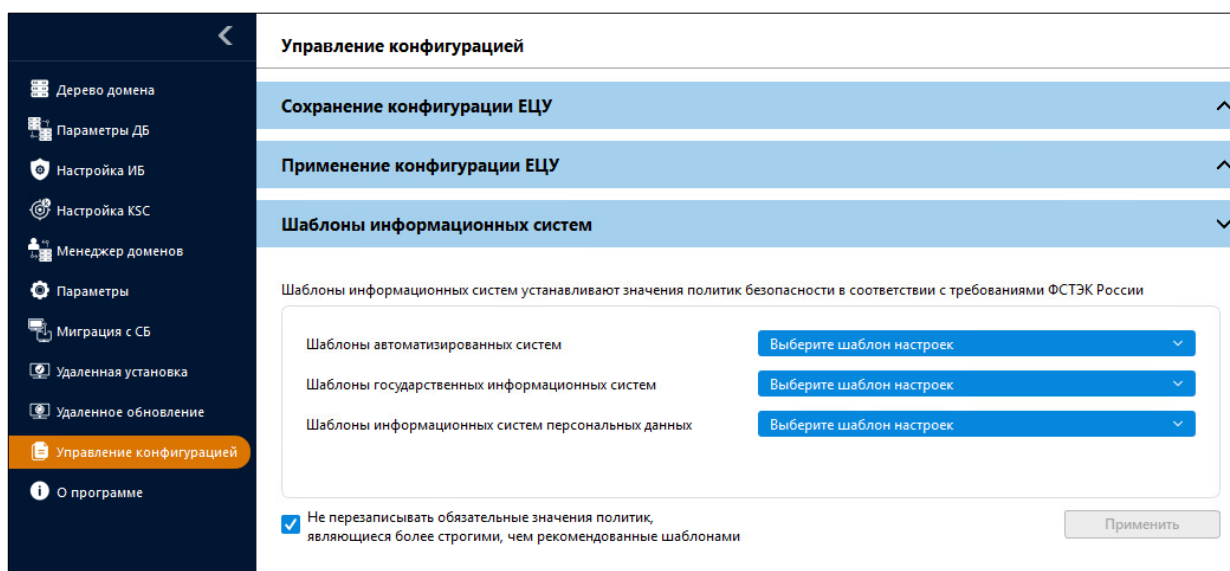


Рис. 26. Шаблоны информационных систем

Также при настройке шаблонов доступно включение/отключение флага *Не перезаписывать обязательные значения политик, являющиеся более строгими, чем рекомендованные шаблонами* (по умолчанию установлен):

- если флаг включен и в **ЕЦУ** администратором установлены более строгие значения политик, то эти значения остаются без изменений;
- если флаг включен, но в **ЕЦУ** установлены менее строгие значения политик, то при применении шаблона значения должны перезаписываться на более строгие;
- если флаг не установлен, то значения политик пользователя в любом случае должны быть перезаписаны на значения из шаблона.

Для применения шаблона необходимо нажать на кнопку **Применить**.

2.5 О программе

Для перехода к информационной странице **О программе** необходимо открыть главное меню Консоли **ЕЦУ** и выбрать пункт → **О программе**.

Откроется страница, содержащая следующие данные:

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

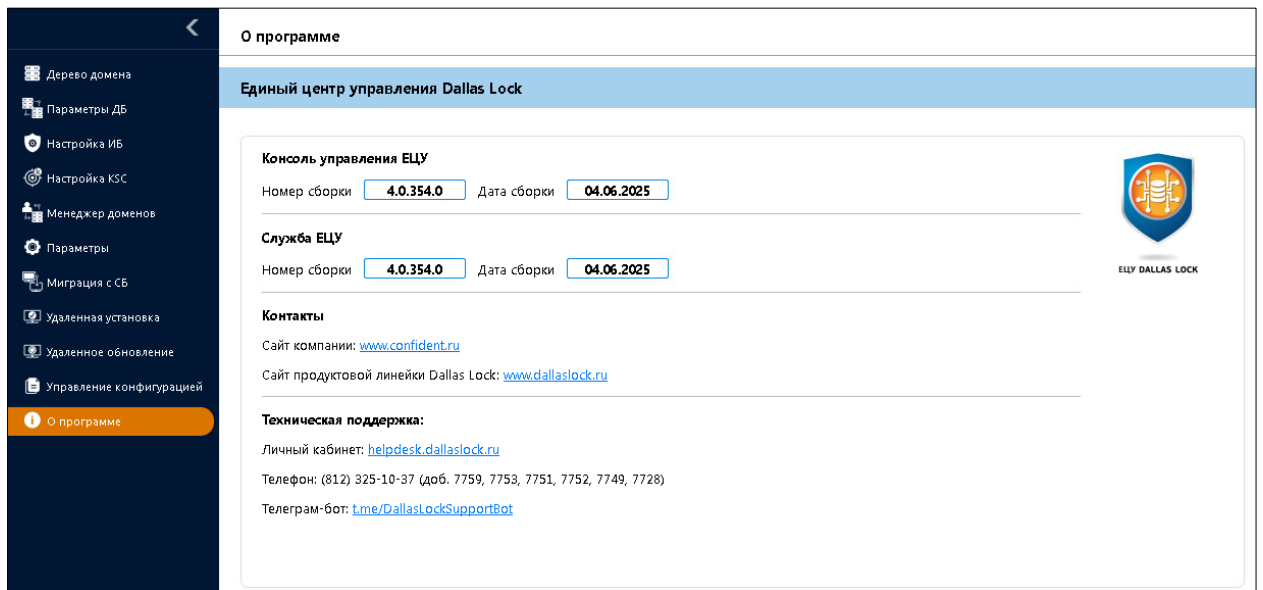


Рис. 27. Страница «О программе»

3 ОБЩИЕ ПРИНЦИПЫ РАБОТЫ ЕЦУ DALLAS LOCK

3.1 Синхронизация

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

Любые изменения параметров, политик, пользователей или групп, совершенные на подчиненном объекте, после синхронизации будут приведены в соответствие с параметрами, заданными в **ЕЦУ Dallas Lock**. Если параметры оставались без изменения (например, список пользователей), синхронизация этих параметров не происходит. Факты и результаты синхронизации фиксируются в журналах подчиненных объектов. Но если в процессе синхронизации на подчиненном объекте не было изменений, то запись в журнал не заносится.

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

Синхронизировать остальные модули с **ЕЦУ Dallas Lock** можно следующими способами:

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

3.2 Репликация

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

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



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

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

Реализовано динамическое применение изменений настроек на сторонние серверы.

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

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

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

4 АДМИНИСТРИРОВАНИЕ ЕЦУ DALLAS LOCK

4.1 Запуск консоли ЕЦУ

Запуск Консоли **ЕЦУ** осуществляется при условии, что компьютер, на котором расположена служба **ЕЦУ**, включен и доступен по сети.

Для запуска Консоли **ЕЦУ** необходимо запустить ярлык консоли, который появился после установки на рабочем столе ПК.

При первом запуске Консоли **ЕЦУ** необходимо выполнить регистрацию экземпляра Консоли в **ЕЦУ**. Для этого необходимо указать сетевое имя ПК, на котором установлена служба **ЕЦУ** и ключ доступа к Домену безопасности (рис. 28).

Рис. 28. Регистрация консоли ЕЦУ в Домене безопасности

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

Далее в окне подключения к серверу требуется заполнить поля (рис. 29):

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

Рис. 29. Ввод пароля учетной записи для входа в Консоль ЕЦУ

При необходимости сменить пароль для указанной учетной записи, можно поставив флаг в поле *Сменить пароль* до нажатия кнопки **Подключиться** (рис. 29). Затем ввести новый пароль и подтверждение пароля (рис. 30).

Рис. 30. Установка нового пароля пользователя

4.2 Описание консоли ЕЦУ

Главное окно Консоли **ЕЦУ** содержит следующие рабочие области (рис. 31):

Рис. 31. Главное окно консоли ЕЦУ

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

Главное меню консоли **ЕЦУ** содержит следующие пункты (рис. 32):

- «Дерево домена» (см. [«ДОМЕН БЕЗОПАСНОСТИ ЕЦУ»](#));
- «Параметры ДБ» (см. [«Параметры домена безопасности»](#));
- «Настройка ИБ» (см. [«Настройка инцидентов безопасности»](#));
- «Настройка KSC» (см. [«Настройка Kaspersky Security Center»](#));
- «Менеджер доменов» (см. [«Менеджер доменов»](#));
- «Параметры» (см. [«Параметры работы»](#));
- «Миграция с СБ» (см. [«Механизм автоматизированной миграции с СБ на ЕЦУ»](#));
- «Удаленная установка»:
 - см. [«Удаленное развертывание СЗИ Dallas Lock 8.0»](#);
 - см. [«Удаленное развертывание СЗИ НСД Dallas Lock Linux»](#);
 - см. [«Удаленная установка Агента ЕЦУ Windows»](#) и [«Удаленная установка Агента ЕЦУ Linux»](#);
 - см. [«Подготовка дистрибутива DL8.0 для AD»](#);
- «Удаленное обновление»:
 - см. [«Удаленное обновление СЗИ НСД Dallas Lock 8.0»](#);
 - см. [«Удаленное обновление СЗИ НСД Dallas Lock Linux»](#);
- «Управление конфигурацией» (см. [«Управление конфигурацией»](#));
- «О программе» (см. [«О программе»](#)).

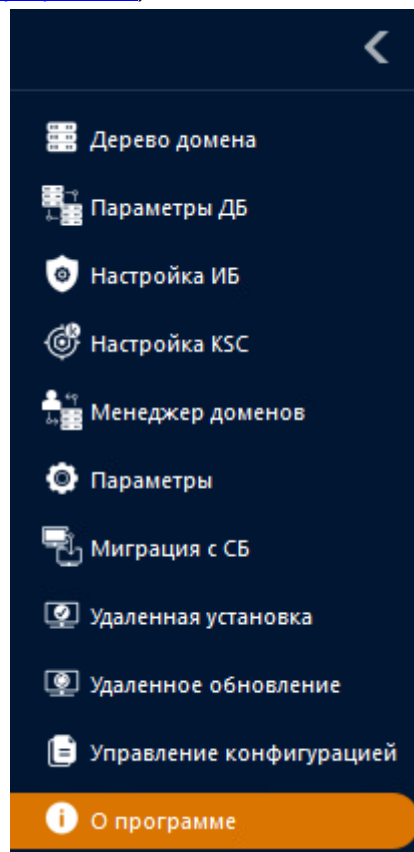


Рис. 32. Пункты главного меню

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.

Для объектов дерева ДБ можно настроить сортировку и фильтрацию:



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

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



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

- фильтрация по типу АРМ;
- фильтрация по модулям;
- фильтрация по сетевым устройствам;
- фильтрация по поддоменам;
- фильтрация по включенным объектам;
- фильтрация по выключенным объектам;
- фильтрация объектов, давно не выходивших на связь;
- фильтрация объектов с непрочитанными инцидентами безопасности.

Для сброса всех фильтров нужно нажать **Сбросить фильтры**.



Ручная сортировка активируется автоматически после перетаскивания объекта. Пользователи могут вручную изменять порядок отображения объектов в дереве ДБ, перетаскивая их на новое место.

Роль *Аудитор* имеет доступ к ручной сортировке, но не может перемещать объекты между различными уровнями вложенности.

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

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



— список вложенных объектов группы скрыт;



— список вложенных объектов группы отображается в дереве.

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

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

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

Удаление и переименование базовых групп недоступно.

Значки объектов, обозначающих модули, зависят от типа и состояния модуля.

Так как АРМ представляет собой совокупность модулей, состояние АРМ зависит от состояния модулей. Эта связь описывается следующим образом:



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



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



— если ни один из модулей в составе АРМ не выходил на связь с **ЕЦУ** свыше установленного параметром «Оповещения при отсутствии связи с объектом»

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

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

В дереве напротив объекта, на котором произошли инциденты безопасности индицируется их количество (рис. 33).



▼ [icon] TEST	86
▼ [icon] Linux-ARM	18
[icon] Dallas Lock 8.0 ИК8	6
[icon] Dallas Lock Linux ИК2	12
[icon] Mikrotik 10.10.102.244...	68

Рис. 33. 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.

При обновлении **ЕЦУ** с более ранних версий до ИК3 и новее, идентичные по имени объекты (независимо от регистра) автоматически переименовываются. Первое имя сохраняется, а последующие получают суффикс (N), где N — число (например, «Новая группа» переименовывается в «Новая группа (1)»).

4.3 Настройки лицензирования

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

- защищаемые АРМ;
- сетевые устройства;
- подчиненные домены;
- **Агенты ЕЦУ**;
- терминальные серверы;
- терминальные сессии.



При формировании лицензии необходимо учитывать, что количество АРМ должно быть всегда больше или равно количеству **Агентов ЕЦУ**, так как АРМ представляет собой совокупность модулей (на один АРМ с **Агентом ЕЦУ** пользователь может ввести другие модули и наоборот).

Если согласно приобретенной лицензии в Домен безопасности еще допустимо ввести **Агент ЕЦУ**, но лимит на количество АРМ достигнут, то **Агент ЕЦУ** возможно установить только на уже зарегистрированные в Домене безопасности **ЕЦУ** АРМ.

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

Информация о параметрах текущей лицензии доступна на уровне Домена безопасности на вкладке **Сводка** → **Информация об объекте** (рис. 34).

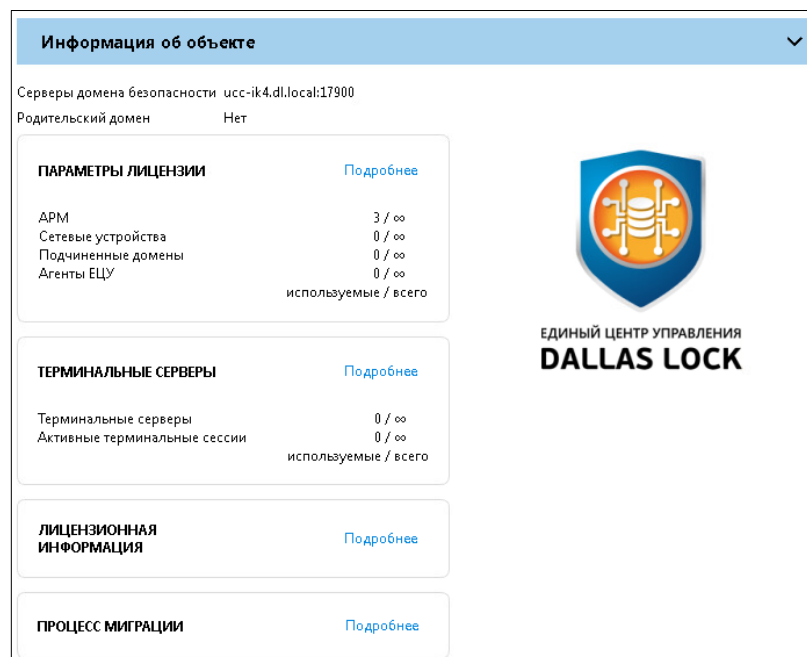


Рис. 34. Информация о параметрах лицензии

При нажатии кнопки **Подробнее** поля *Параметры лицензии* появляется окно **Состояние лицензии** (рис. 35), которое содержит информацию о состоянии лицензии для данного сервера, а также для каждого сервера в кластере ДБ.

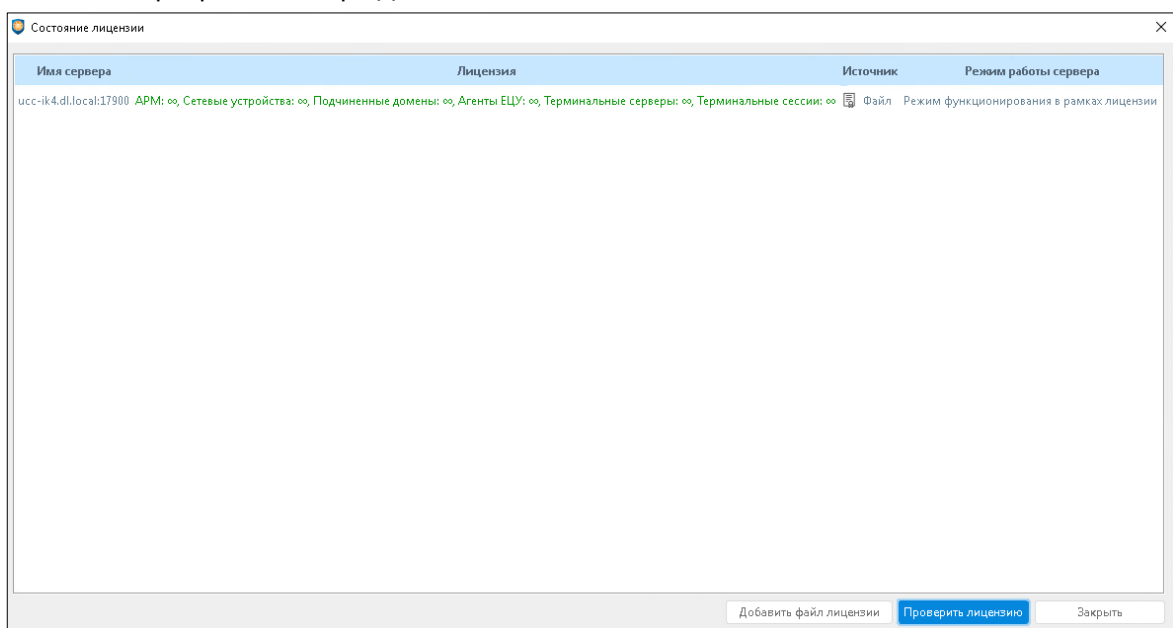


Рис. 35. Окно «Состояние лицензии»

Для добавления файла лицензии средствами **ЕЦУ**, необходимо:

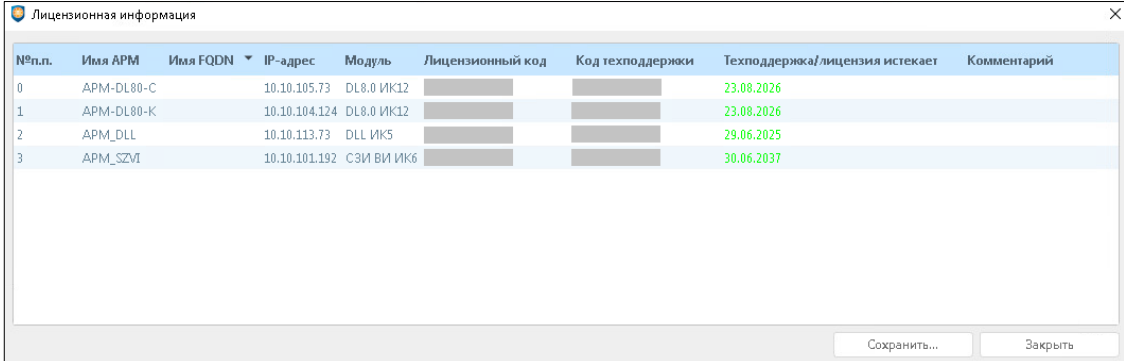
- нажать кнопку **Добавить файл лицензии**;
- указать путь к файлу формата `.ucLicenseKey`;
- нажать на кнопку **Проверить лицензию**.

В случае успешного применения, в столбце *Лицензия* появится соответствующая надпись с установленными количественными ограничениями по подчиненным объектам. Также информация о параметрах текущей лицензии изменится на вкладке *Сводка* (рис. 34).

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

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

При нажатии кнопки **Подробнее** поля *Лицензионная информация* появляется окно, содержащее лицензионную информацию (лицензионный код и код техподдержки) для всех модулей, введенных под управление **ЕЦУ** (рис. 36).



№п.п.	Имя АРМ	Имя FQDN	IP-адрес	Модуль	Лицензионный код	Код техподдержки	Техподдержка/лицензия истекает	Комментарий
0	APM-DL80-C		10.10.105.73	DL8.0 ИК12			23.08.2026	
1	APM-DL80-K		10.10.104.124	DL8.0 ИК12			23.08.2026	
2	APM_DLL		10.10.113.73	DLL ИК5			29.06.2025	
3	APM_SZVI		10.10.101.192	СЗИ ВИ ИК6			30.06.2037	

Рис. 36. Окно «Лицензионная информация»

Также в открывшемся окне отображается информация о сроке действия техподдержки: в столбце *Техподдержка/лицензия истекает* действующая техподдержка/лицензия выделена зеленым цветом, истекшая — красным.

Столбец *Комментарий* по умолчанию пустой и при необходимости может быть заполнен администратором вручную.

Для каждого из столбцов предусмотрена возможность сортировки путем нажатия левой кнопкой мыши на названии столбца.

Реализована возможность сохранения сформированного отчета с лицензионной информацией в файл (в формате .html или .csv) по кнопке **Сохранить....**

4.3.1 Особенности лицензирования кластера ДБ

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

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

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

В данном случае квота кластера рассчитывается следующим образом:

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

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



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 запуске сервера;
 - $MAX(Z)/X$ — количественные ограничения по подчиненным объектам, действующие в кластере **ЕЦУ**.
1. Если по итогам проверки параметров лицензии обнаружен корректно работающий ключ, при этом $(MAX(Z)/X \geq Y/X)$ — 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**.

4.4 Перераспределение терминальных сессий

В **ЕЦУ** реализован механизм перераспределения терминальных сессий, позволяющий динамически распределять квоты на использование терминальных сессий между терминальными серверами на модулях **СЗИ Dallas Lock 8.0**, зарегистрированных в ДБ **ЕЦУ**.

Информация о параметрах текущей лицензии на терминальные серверы и сессии доступна на уровне Домена безопасности на вкладке **Сводка** → **Информация об объекте** (рис. 37).

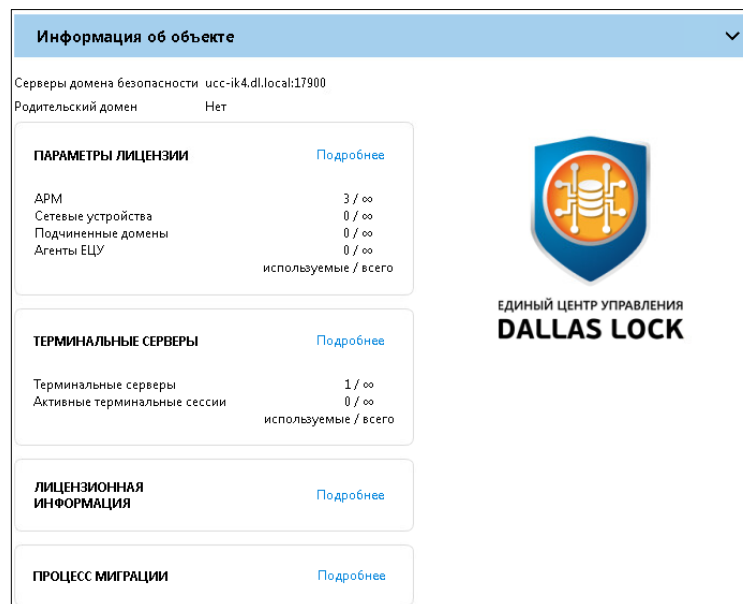
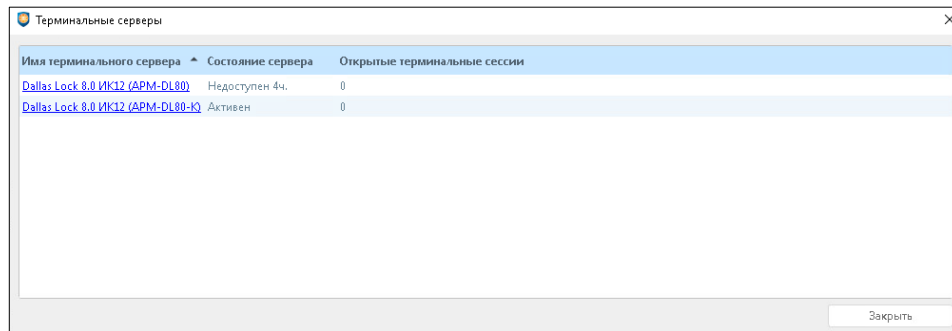


Рис. 37. Информация о параметрах лицензии на терминальные серверы



Блок информации *Терминальные серверы* на вкладке **Сводка** в разделе **Информация об объекте** отображается только при наличии квот на терминальные серверы и сессии в лицензии на **ЕЦУ Dallas Lock**.

При нажатии кнопки **Подробнее** поля *Терминальные серверы* появляется окно **Терминальные серверы** (рис. 38), которое содержит сводную информацию по всем терминальным серверам, введенным в ДБ ЕЦУ.



Имя терминального сервера	Состояние сервера	Открытые терминальные сессии
Dallas Lock 8.0 ИК12 (APM-DL80)	Недоступен 4ч.	0
Dallas Lock 8.0 ИК12 (APM-DL80-K)	Активен	0

Рис. 38. Окно «Терминальные серверы»

При нажатии на наименование АРМ с зарегистрированным терминальным сервером в столбце *Имя терминального сервера* осуществляется переход на уровень модуля **СЗИ Dallas Lock 8.0**, в соответствии с именем АРМ в столбце.

Для регистрации терминального сервера необходимо на уровне модуля **СЗИ Dallas Lock 8.0** нажать кнопку **Зарегистрировать терминальный сервер** на панели *Оперативное управление*.

Если модуль **СЗИ Dallas Lock 8.0** зарегистрирован как терминальный сервер, строка *Терминальный сервер* в разделе *Информация об объекте* будет иметь значение *Зарегистрирован*.



Прекращение обслуживания клиента в качестве терминального сервера возможно со стороны клиента, зарегистрированного в качестве терминального сервера. Более подробно о перераспределении терминальных сессий описано в Руководстве по эксплуатации **СЗИ НСД Dallas Lock 8.0**.

4.5 Механизм автоматизированной миграции с СБ на ЕЦУ

Механизм миграции создан для облегчения переноса данных при переходе с СБ на **ЕЦУ**.

Для подключения к СБ и получения структуры дерева клиентов, политик и учетных записей необходимо в главном меню консоли **ЕЦУ**  выбрать **Миграция с СБ** (рис. 39).

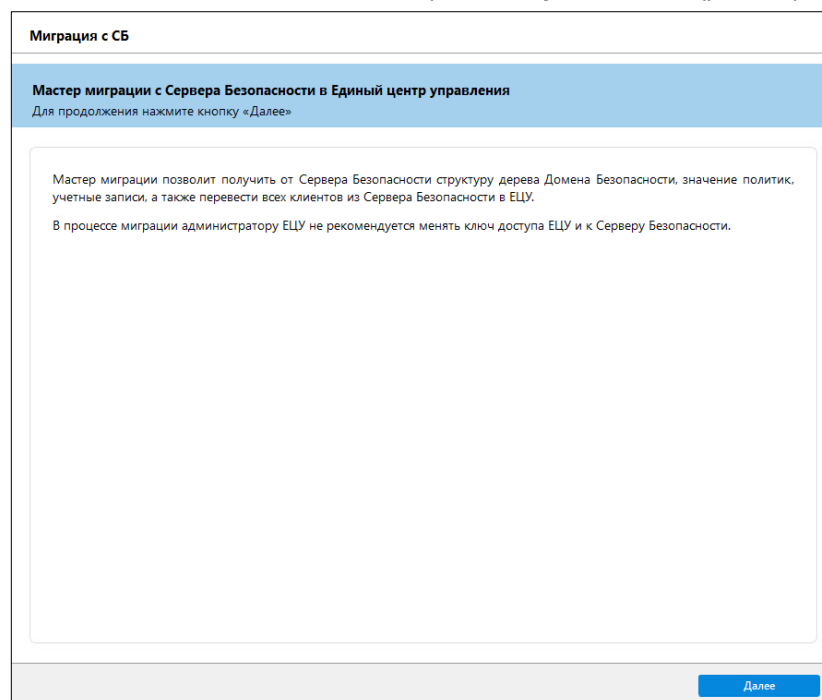


Рис. 39. Страница мастера миграции

Откроется страница мастера миграции с Сервера Безопасности в Единый центр управления. После ознакомления администратора с информацией, необходимо нажать кнопку **Далее** для перехода к странице **Решение коллизий неуникальных политик**. На данной странице предоставляется выбор типа клиента, политики которого должны быть приоритетными при возникновении коллизий при назначении политик на уровне групп в процессе миграции (рис. 40). На выбор доступны клиенты **Dallas Lock 8.0**, **Dallas Lock Linux** и **СДЗ Dallas Lock**.

The screenshot shows a window titled "Миграция с СБ". Below the title bar is a blue header with the text "Решение коллизий неуникальных политик" and a subtitle "Выберите тип клиента, значениями политик которого будет отдаваться приоритет при назначении политик на уровне групп". The main area contains a section "Тип клиента:" with three radio button options: "Dallas Lock 8.0" (selected), "Dallas Lock Linux", and "СДЗ Dallas Lock". An information icon is in the top right of this section. At the bottom are three buttons: "Назад", "Далее" (highlighted in blue), and "Отмена".

Рис. 40. Страница «Решение коллизий неуникальных политик»

После выбора типа клиента, политики которого должны быть приоритетными, необходимо нажать кнопку **Далее** для перехода к странице подключения к СБ (рис. 41).

The screenshot shows the same window titled "Миграция с СБ", but the blue header now says "Подключение к СБ" with the subtitle "Для подключения к СБ заполните все поля и нажмите кнопку «Далее»". The main area contains four input fields: "Имя или IP-адрес СБ:" with the value "10.10.105.96", "Ключ СБ:" with masked characters "*****" and a visibility icon, "Логин администратора СБ:" with the value "admin", and "Пароль администратора СБ:" with masked characters "****" and a visibility icon. At the bottom are three buttons: "Назад", "Далее" (highlighted in blue), and "Отмена".

Рис. 41. Подключение к СБ

Для подключения к СБ должны быть заполнены следующие поля:

- имя или IP-адрес СБ;
- ключ СБ (если был задан);
- логин администратора СБ;
- пароль администратора СБ.

После заполнения полей необходимо нажать кнопку **Далее** для перехода к окну выбора модулей/компонентов для миграции (рис. 43).



Если к СБ не удалось подключиться, то в окне подключения появляется сообщение с ошибкой. Ознакомившись с ошибкой, следует нажать **ОК** и повторить попытку подключения (рис. 42).

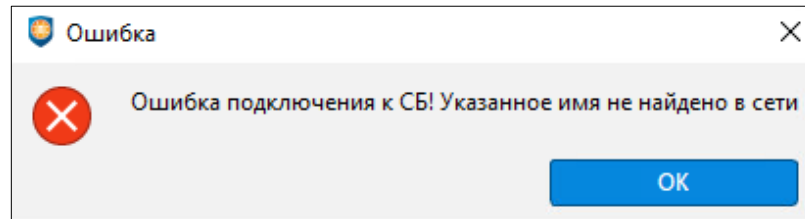


Рис. 42. Ошибка подключения к СБ

Миграция с СБ

Выбор модулей/компонентов для миграции
Если требуется, выберите дополнительные модули/компоненты и их настройки, которые нужно мигрировать

При миграции модуля будет передан список дескрипторов съемных накопителей и соответствующие им пользовательские описания и список КПСН.

☒ **Средство контроля съемных машинных носителей информации (СКН)**

При миграции правил МЭ будут очищены правила, созданные на ЕЦУ. Параметры "Список сетевых адаптеров" и "Выбранные сегменты сети" не мигрируют!

☒ **Межсетевой экран (МЭ)**

- ☒ Настройки МЭ
- ☒ Правила МЭ

Требуется выгрузить резервную копию настроенных правил МЭ. Выберите путь для сохранения:

C:/Users/user/firewall_rules_2024_12_26_11_39_38.fwconf ...

Назад **Далее** Отмена

Рис. 43. Выбора модулей/компонентов для миграции

На данной рабочей области предоставляется выбор модулей для миграции, для назначения необходимо установить флаг напротив строки и нажать кнопку **Далее**.

Доступные модули для выбора:

- Межсетевой экран (МЭ):
 - Настройки МЭ;
 - Правила МЭ;



Перед миграцией правил МЭ администратору **ЕЦУ** рекомендуется выгрузить копию существующих правил МЭ. Это позволит восстановить правила в случае возникновения ошибок.

- Система обнаружения вторжений (COB):
 - Сигнатуры COB;
 - Параметры COB (настройки эвристики, контроля приложений и реестра, глобальных параметров);
 - Настройки безопасной среды;
 - Доверенные адреса;
- Средство контроля съемных машинных носителей информации (СКН).



Если один и тот же дескриптор принадлежит разным объектам в **СБ** и **ЕЦУ**, приоритетным является дескриптор, зарегистрированный на **СБ**. В таком случае при миграции дескриптор, зарегистрированный на **ЕЦУ**, будет удален, а мигрировавший с **СБ** — зарегистрирован.



Если при миграции с **СБ** на **ЕЦУ** был передан КПСН, созданный с использованием алгоритмов от внешнего криптопровайдера, который отсутствует в перечне доступных на **ЕЦУ**, то при открытии «Свойств» такого КПСН появляется окно с ошибкой. Редактирование свойств для КПСН с недоступными криптопровайдерами запрещено.

После следует страница процесса миграции данных со списком выполняемых действий. По мере выполнения действий галочки в списке становятся зеленого цвета (рис. 44). Для перехода к следующему окну нужно нажать кнопку **Далее**.

Миграция с СБ

Процесс миграции
Для завершения процесса дождитесь выполнения всех действий и нажмите кнопку «Далее»

- ✓ Получение структуры домена безопасности
- ✓ Получение политик
- ✓ Получение учетных записей
- ✓ Получение дескрипторов сменных накопителей
- ✓ Создание структуры домена безопасности
- ✓ Регистрация учетных записей
- ✓ Применение значений политик
- ✓ Регистрация дескрипторов сменных накопителей
- ✓ Отправка регистрационных данных на СБ

Далее **Отмена**

Рис. 44. Процесс миграции с СБ на ЕЦУ



Процесс миграции при большом количестве дескрипторов может быть достаточно длительным. Рекомендуется воздержаться от использования **ЕЦУ** во время процесса миграции, чтобы избежать возможных ошибок и сбоев.

В следующем окне показана информация, которая перенеслась с СБ. Полный список можно увидеть по ссылке, указанной внизу страницы (рис. 45). Для завершения процесса нажать кнопку **Далее**.

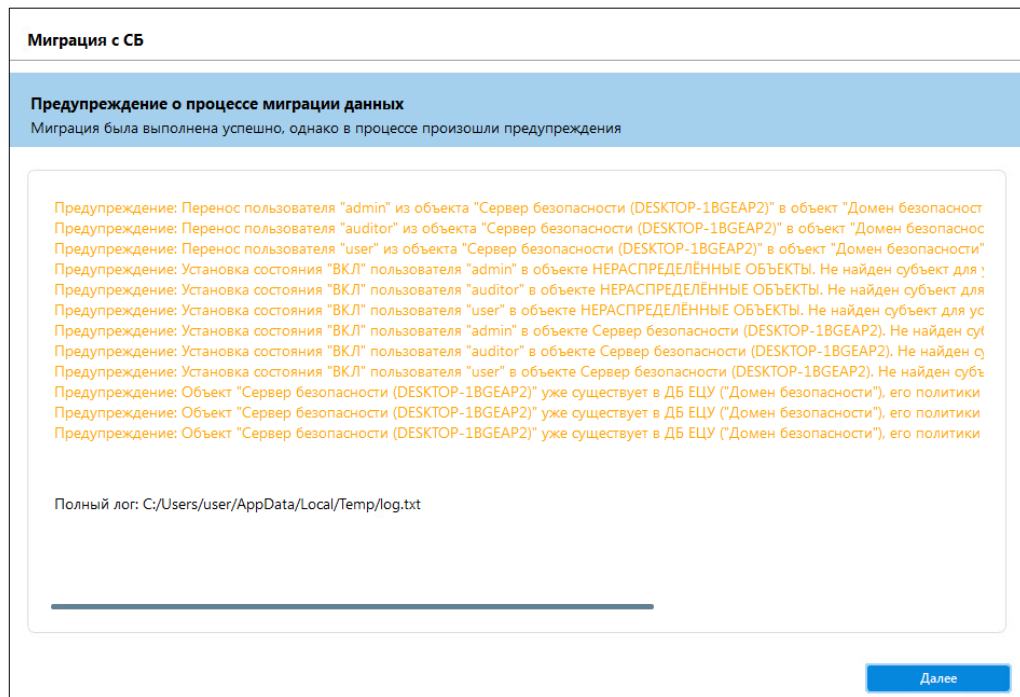


Рис. 45. Предупреждения о процессе миграции

После этого откроется страница ввода клиентов (рис. 46). Для того, чтобы закрыть мастер миграции, нужно нажать кнопку **Завершить**.

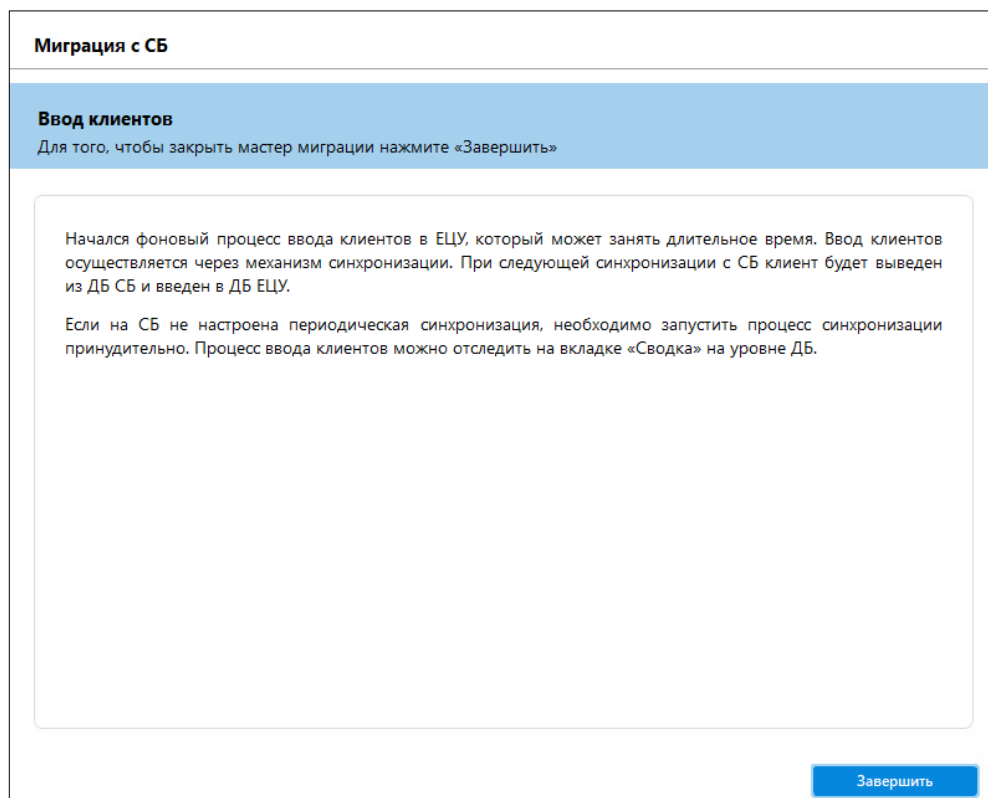


Рис. 46. Страница ввода клиентов

Ввод клиентов будет осуществляться в фоновом режиме. На консоли **ЕЦУ** данный процесс можно отследить на вкладке **Сводка** на уровне ДБ (рис. 34). Нажав «Подробнее», открывается окно «Состояние миграции» (рис. 47). Данное окно содержит таблицу с полями:

- «Создано» — содержит информацию о дате и времени начала миграции, также в данном

поле содержится иконка, которая указывает на статус миграции:

-  — миграция завершена успешно или принудительно;
-  — миграция в процессе;
- «Выполнено» — содержит информацию о дате и времени окончания миграции;
- «Имя СБ» — имя сервера безопасности, с которого происходит миграция;
- «Количество клиентов, мигрирующих на ЕЦУ» — показывает количество мигрировавших клиентов к общему числу клиентов на СБ;
- «Статус» — показывает состояние процесса миграции: «Успешно завершена», «В процессе» или «Принудительное завершение».



При миграции с СБ объекты с одинаковыми именами объединяются, вне зависимости от регистра. После объединения отображается имя, которое было ранее сохранено в ЕЦУ.

Данный процесс можно принудительно завершить, нажав кнопку **Принудительное завершение**. В случае принудительного завершения процесса миграции, еще не введенные в ЕЦУ клиенты останутся в составе домена СБ, а все неиспользованные шаблоны с настройками клиентов будут удалены.

Создано	Выполнено	Имя СБ	Количество клиентов, мигрирующих на ЕЦУ	Статус
 26.06.2024 15:38	26.06.2024 15:38	DESKTOP-1BGEAP2	1 из 1	Успешно завершена
 26.06.2024 15:40	26.06.2024 15:40	DESKTOP-1BGEAP2	0 из 0	В процессе

Рис. 47. Окно состояния миграции

При нажатии кнопки **Подробнее** открывается список клиентов с детальной информацией о типе модуля и о результате миграции каждого клиента, в т.ч. в этом списке будут отображаться клиенты, которые миграцию не поддерживают (рис. 48). Данное окно содержит таблицу с полями:

- «Состояние» — содержит информацию о дате и времени текущего статуса миграции, также в данном поле содержится иконка, которая указывает на статус миграции:
 -  — миграция клиента завершена успешно;
 -  — миграция клиента в процессе;
 -  — миграция клиента не завершена по причине принудительного завершения со стороны администратора или миграция клиента не поддерживается из-за версии;
- «Имя АРМ» — имя мигрирующего клиента;
- «Модуль» — название модуля **СЗИ**;
- «Статус» — показывает состояние процесса миграции: «Миграция успешно завершена», «Ожидание миграции», «Принудительное завершение миграции» или «Текущая версия клиента не поддерживает миграцию».

Кнопка **Сохранить** позволяет выгрузить в файл список клиентов с информацией о миграции. Поле **Поиск...** позволяет осуществить поиск по имени модуля и АРМ. Информацию можно фильтровать по типу модулей и статусу миграции, а также сортировать по столбцам.

Состояние миграции				
Поиск...				
Состояние	Имя АРМ	Модуль	Статус	
✓	15.09.2023 19:47	ucc_sdz	СДЗ Dallas Lock	Миграция успешно завершена
✓	15.09.2023 19:45	ucc-lin-2	Dallas Lock Linux	Миграция успешно завершена
✓	15.09.2023 19:45	ucc-lin-4	Dallas Lock Linux	Миграция успешно завершена
✓	15.09.2023 19:45	ucc-lin-3	Dallas Lock Linux	Миграция успешно завершена
✓	15.09.2023 19:45	ucc-lin-1	Dallas Lock Linux	Миграция успешно завершена
✓	15.09.2023 19:45	ucc-lin-5	Dallas Lock Linux	Миграция успешно завершена
✓	15.09.2023 19:45	UCC-WIN-3	Dallas Lock 8.0	Миграция успешно завершена
✓	15.09.2023 19:45	UCC-WIN-5	Dallas Lock 8.0	Миграция успешно завершена
✓	15.09.2023 19:45	UCC-WIN-1	Dallas Lock 8.0	Миграция успешно завершена
✓	15.09.2023 19:45	UCC-WIN-2	Dallas Lock 8.0	Миграция успешно завершена
✓	15.09.2023 19:45	UCC-WIN-4	Dallas Lock 8.0	Миграция успешно завершена
✗	15.09.2023 19:45	DL8-IK8	Dallas Lock 8.0	Текущая версия клиента не поддерживает миграцию
✗	15.09.2023 19:45	DL8-IK9	Dallas Lock 8.0	Текущая версия клиента не поддерживает миграцию
✗	15.09.2023 19:45	dll_ik2	Dallas Lock Linux	Текущая версия клиента не поддерживает миграцию

Рис. 48. Состояние миграции. Вкладка «Подробнее»

4.6 Параметры домена безопасности

Параметры работы домена безопасности настраиваются в главном меню Консоли ЕЦУ → **Параметры ДБ** (рис. 49). На данной странице мы можем сменить имя домена, установить ключ доступа, ввести домен в подчинение и настроить параметры кластера.

Для смены имени домена нужно в строке *Имя домена безопасности* ввести новое и нажать кнопку **Применить**.

Дерево домена

Параметры ДБ

Настройка ИВ

Настройка КС

Менеджер доменов

Параметры

Миграция с СБ

Удаленная установка

Удаленное обновление

Управление конфигурацией

О программе

Параметры домена безопасности

Имя домена безопасности

Домен безопасности

Применить

Установка ключа доступа

Введите новый ключ

Подтверждение ключа

Не используется

Применить

Ввод в подчинение

Сетевое имя сервера

Ключ доступа

Ввести

Параметры кластера

Сетевое имя сервера

Ключ доступа

Ввести

Рис. 49. Параметры домена безопасности

4.6.1 Установка ключа доступа

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**  и выбрать пункт **Параметры ДБ**.

В блоке *Установка ключа доступа* необходимо заполнить следующие поля и нажать кнопку **Применить** (рис. 50).

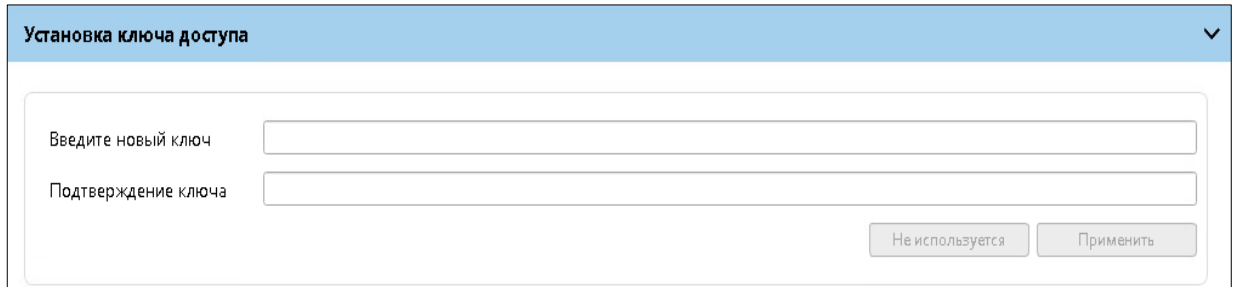


Рис. 50. Установка ключа доступа



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



Действие политики сложности пароля *Необходимо изменение пароля не меньше, чем в* не распространяется на ключ доступа к ДБ.

4.6.2 Ввод в подчинение

Для ввода домена безопасности в подчинение другому домену необходимо открыть главное меню

Консоли **ЕЦУ**  выбрать пункт **Параметры ДБ**.

В блоке *Ввод в подчинение* необходимо ввести имя сервера и ключ доступа (рис. 51).

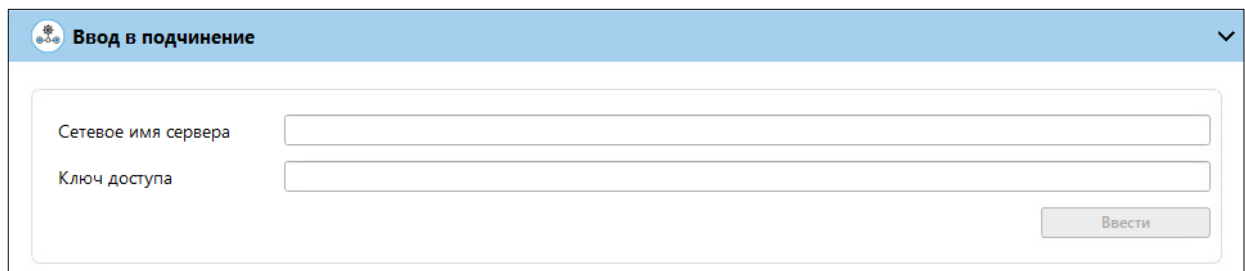


Рис. 51. Ввод в подчинение

После заполнения данных главного сервера ДБ нажать кнопку **Ввести**. Далее появится информационное сообщение об успешном вводе домена (рис. 52).

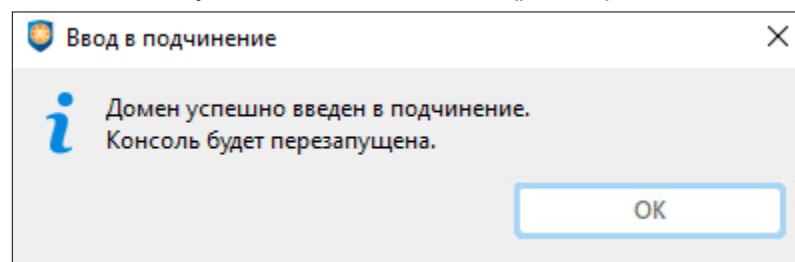


Рис. 52. Сообщение о вводе домена

Консоль **ЕЦУ** будет перезапущена. Для вывода домена из подчинения нажать кнопку **Вывести** (рис. 53).

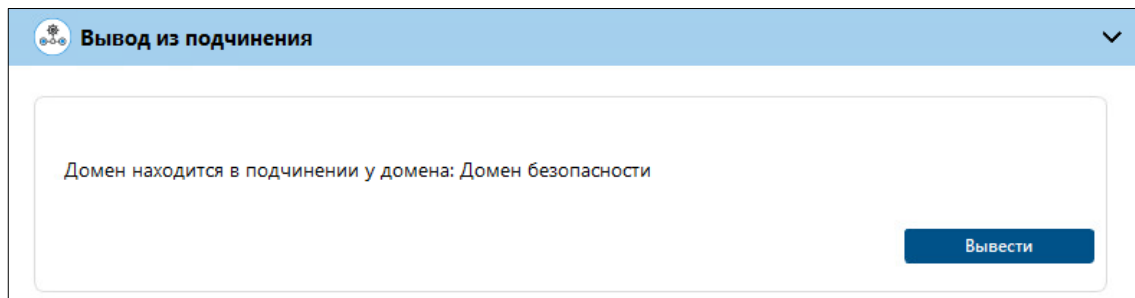


Рис. 53. Вывод из подчинения

Более подробно о подчиненном домене в главе [«ПОДЧИНЕННЫЙ ДОМЕН БЕЗОПАСНОСТИ»](#).

4.6.3 Параметры кластера

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

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

```
# IPv4 local connections:
```

```
host all all 0.0.0.0/0 password
```

Это позволит разрешить подключение к PostgreSQL с любого адреса, для подключения с IPv4 адресов к любой БД, любым пользователем (или настроить ограниченный доступ только с серверов **ЕЦУ Dallas Lock**);

- раскомментировать в файле `postgresql.conf` следующую строку:

```
listen_addresses = "*" 
```

Это позволит PostgreSQL отвечать на любом интерфейсе сервера (или настроить работу на определенном сетевом интерфейсе, доступном по сети с сервера **ЕЦУ Dallas Lock**);

- создать отдельную базу данных и учетную запись в PostgreSQL для **ЕЦУ Dallas Lock**, выполнив команды в командной оболочке SQL Shell (psql):

```
postgres=# create database <база_данных>;
```

```
postgres=# create role <админ_базы_данных> with login;
```

```
postgres=# \password <админ_базы_данных>;
```

```
postgres=# grant connect, create on database <база_данных> to <админ_базы_данных>;
```



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

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

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



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



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



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

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

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

Ввод в кластер ДБ в процессе установки



При создании кластера ДБ необходимо использовать одинаковые версии **ЕЦУ Dallas Lock**.



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

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

1. Запустить процесс установки **ЕЦУ Dallas Lock**.
2. На шаге **Выбор типа домена** выбрать пункт *Сервер репликации* (рис. 54).

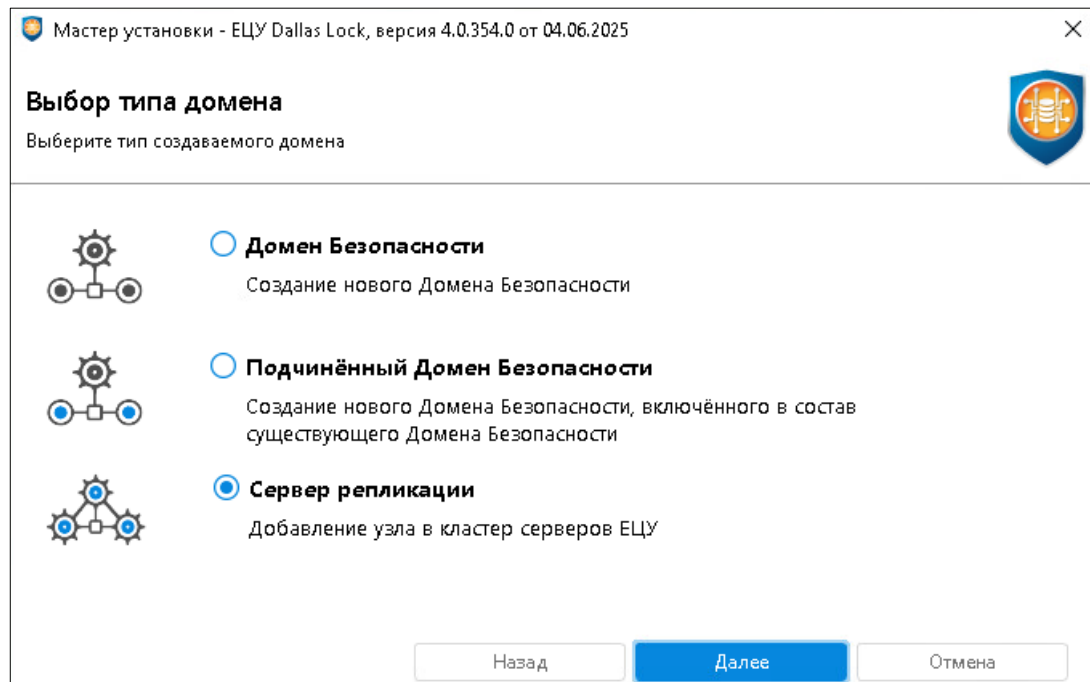


Рис. 54. Выбор типа создаваемого домена

3. Задать параметры главного ДБ (рис. 55):

- адрес главного ДБ;
- ключ доступа к ДБ.

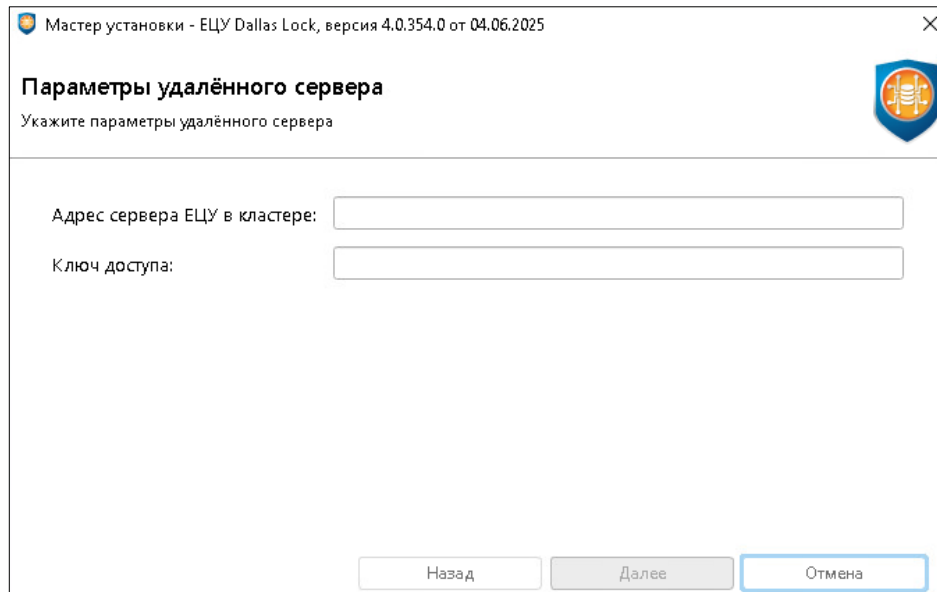


Рис. 55. Параметры удаленного сервера

4. Далее продолжить установку **ЕЦУ Dallas Lock**.

5. После завершения установки на серверах кластера **ЕЦУ Dallas Lock** на вкладке **Сводка** → **Информация об объекте** появится имя добавленного узла.

Ввод в кластер ДБ после установки



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

Для изменения настроек кластера ДБ после установки необходимо открыть главное меню

Консоли **ЕЦУ** → **Параметры ДБ**.

В блоке *Параметры кластера*, ввести текущий сервер **ЕЦУ Dallas Lock** в кластер ДБ для репликации и ключ доступа (рис. 56).

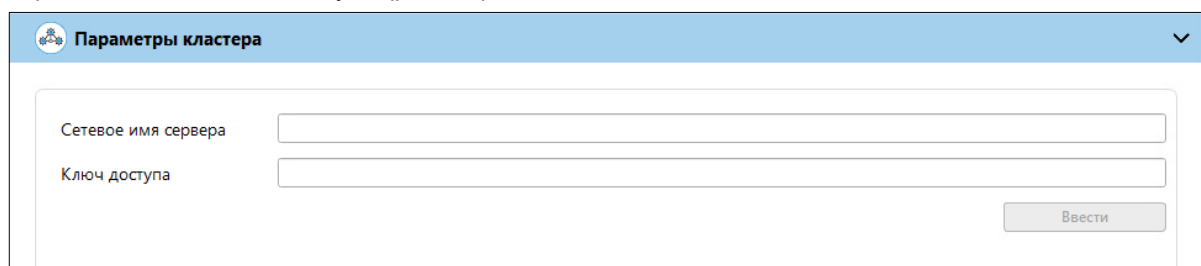


Рис. 56. Параметры кластера

После заполнения данных главного сервера ДБ нажать кнопку **Ввести**. Далее появится информационное сообщение об успешной регистрации сервера (рис. 57).

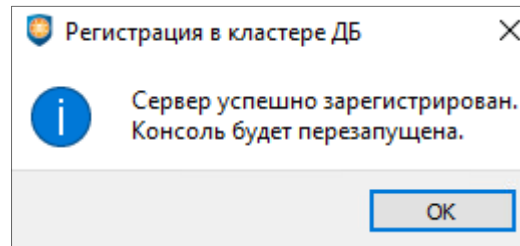


Рис. 57. Сообщение о регистрации в кластере ДБ

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

На уровне ДБ (вкладка **Сводка** → **Информация об объекте**) отобразятся имена всех серверов кластера **ЕЦУ Dallas Lock**, а также будут рассчитаны количественные ограничения лицензии, согласно особенностям назначения квот для домена (см. [«Особенности лицензирования кластера ДБ»](#)) (рис. 58).

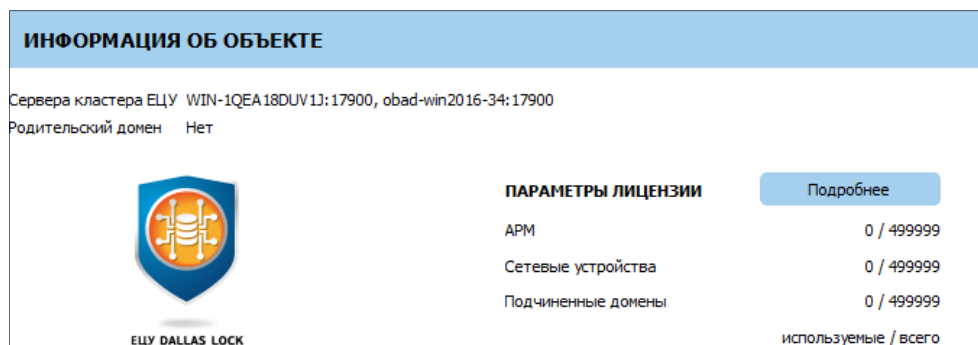


Рис. 58. Информация о кластере серверов

Вывод сервера из кластера ДБ

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

В блоке *Параметры кластера ДБ*, из списка серверов кластера выбрать сервер для вывода и нажать **Вывести**. Появится сообщение об успешном выводе сервера из кластера **ЕЦУ Dallas Lock** и далее Консоль **ЕЦУ** перезапустится.

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.

4.7 Настройка инцидентов безопасности

4.7.1 Настройка инцидентов безопасности



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

В **ЕЦУ Dallas Lock** предусмотрена возможность пользовательской настройки визуализации диаграмм инцидентов безопасности и управления оповещениями в зависимости от приоритета и типа события, а также реализована возможность экспорта инцидентов безопасности в файл на вкладке *Сводка* по кнопке **Экспорт** (рис. 59).

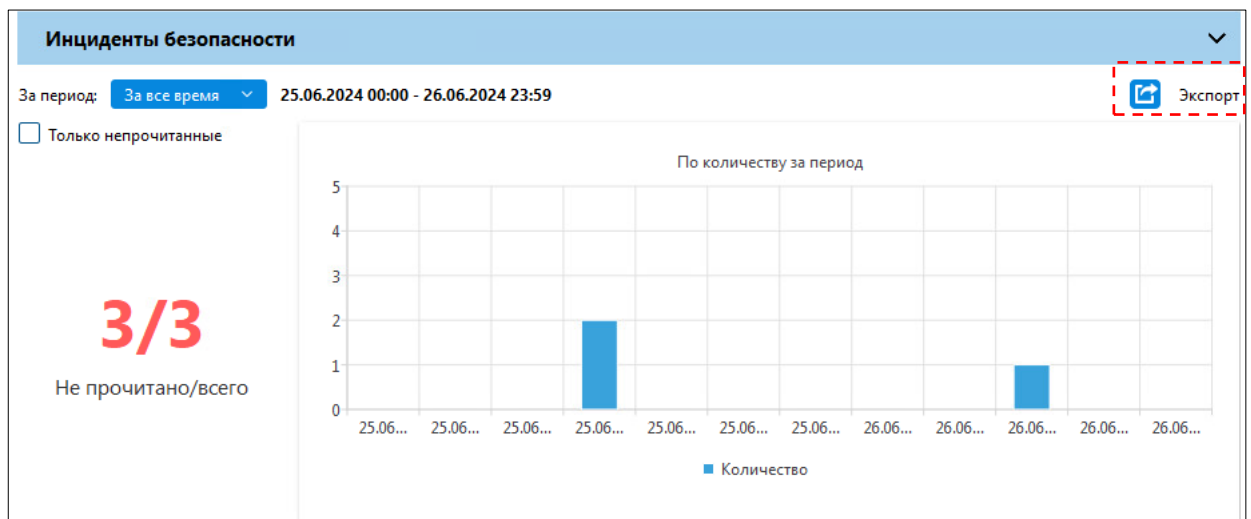


Рис. 59. Экспорт инцидентов безопасности

Для настройки инцидентов безопасности необходимо в главном меню консоли **ЕЦУ** выбрать категорию **Настройка ИБ**. При нажатии откроется страница **Настройка инцидентов безопасности** (рис. 60).

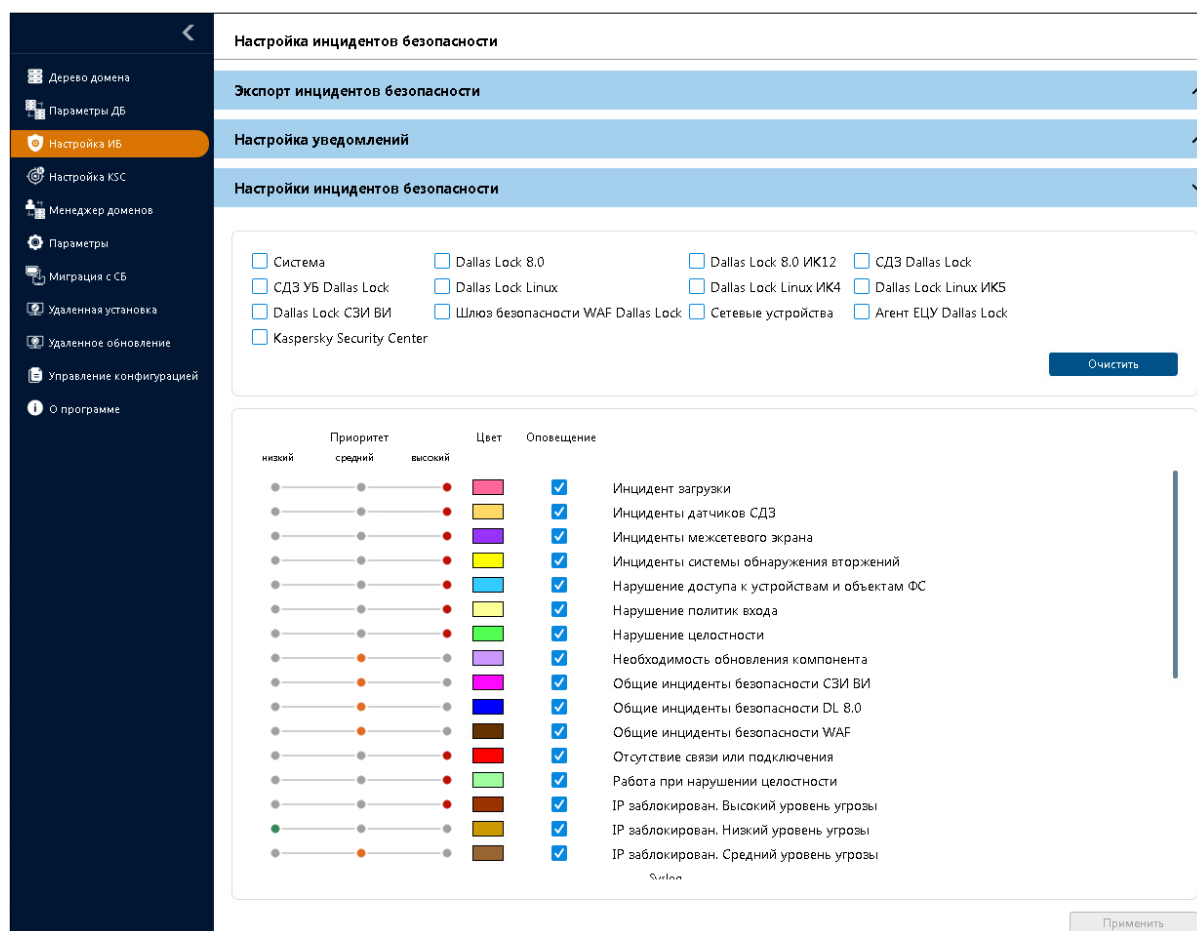


Рис. 60. Страница Настройки инцидентов безопасности

В верхней части блока *Настройка инцидентов безопасности* расположено поле с фильтрацией инцидентов информационной безопасности по модулям. Ниже расположена таблица, состоящая из трех столбцов:

- В столбце *Оповещение* приведен список доступных инцидентов безопасности, для которых осуществляется настройка.



При отключенном атрибуте *Оповещение* уведомление об инциденте безопасности не будет отображаться в трее и отправляться на e-mail. Регистрация события ИБ и отправка события в SIEM-систему при этом будут производиться всегда, независимо от состояния атрибута.

- В столбце *Приоритет* производится настройка приоритетов правил контроля приложений. Для каждого инцидента безопасности можно изменить приоритет выбором одного из значений. Доступны приоритеты событий: «Низкий», «Средний» и «Высокий». Настройки приоритетов влияют на внешний вид диаграммы «По приоритету» (вкладка **Сводка** → **Инциденты безопасности**).
- В столбце *Цвет* производится настройка цвета сегментов диаграммы «По типу» (отображается на вкладке **Сводка** → **Инциденты безопасности**). Для смены цвета инцидента безопасности нужно нажать левой кнопкой мыши по навигатору цвета и выбрать цвет из палитры (рис. 61).

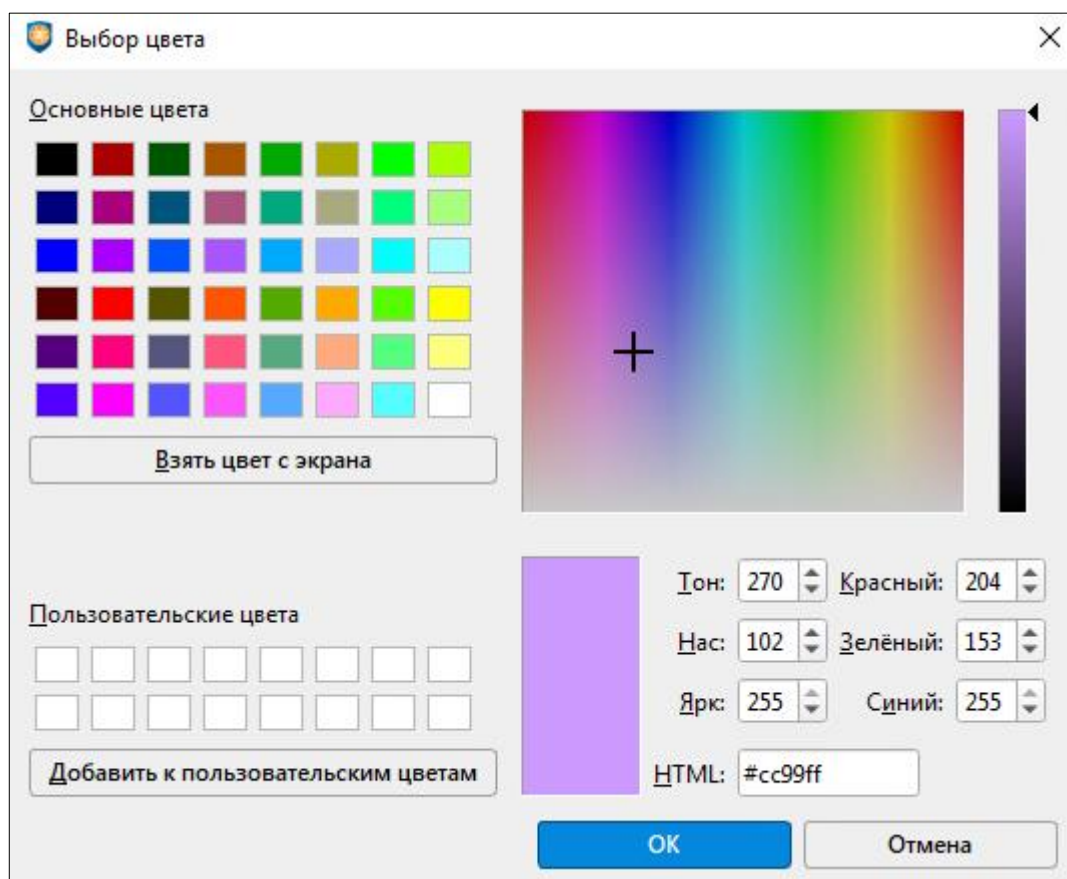


Рис. 61. Выбор цвета инцидента безопасности

Инциденты безопасности на модулях отслеживаются и сопровождаются сигнализацией на **ЕЦУ Dallas Lock**. На ПК с запущенной Консолью **ЕЦУ** воспроизводится звуковой сигнал о событии безопасности и выводится всплывающее сообщение в области уведомлений (рис. 62).

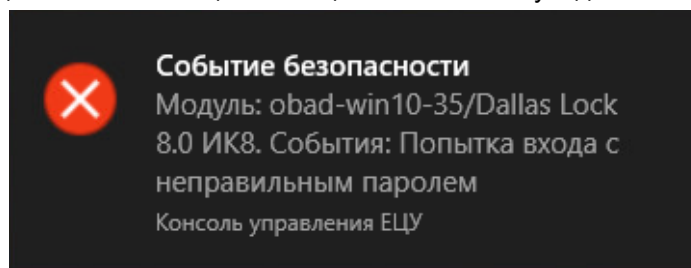


Рис. 62. Уведомление о событии безопасности на модуле

4.7.2 Настройка уведомлений

Для настройки уведомлений инцидентов безопасности необходимо открыть главное меню Консоли **ЕЦУ** → **Настройки ИБ**. В блоке *Настройка уведомлений* можно определить, кому и от кого будет отправлено письмо, также задать тему письма и его текст. Для редактирования блока необходимо установить флаг напротив строки *Отправлять уведомления на электронную почту* (по умолчанию флаг не выставлен). Тема и текст письма заданы по умолчанию (рис. 63).

В поле *Ключевые слова* необходимо заполнить поля:

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

В строке **Шифрование** выбрать необходимый вариант из предложенных:

- SSL/TLS;
- STARTTLS;
- Нет.

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

Рис. 63. Страница настройки уведомлений

4.7.3 Экспорт инцидентов безопасности

Для экспортирования инцидентов безопасности в SIEM-систему необходимо открыть главное меню

Консоли **ЕЦУ** → **Настройки ИБ**.

В блоке **Экспорт инцидентов безопасности** заполнить следующие поля (рис. 64):

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

Рис. 64. Экспорт инцидентов безопасности в SIEM

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

4.8 Менеджер доменов

! Для обеспечения возможности регистрации учетных записей домена Active Directory, FreeIPA, ALD PRO, Ред АДМ, Samba в Домене безопасности **ЕЦУ Dallas Lock**, развернутого на ПК с ОС Linux, необходимо указание полностью определенного имени домена.

Для просмотра информации о том, к какому домену принадлежит **ЕЦУ Dallas Lock**, необходимо открыть главное меню Консоли **ЕЦУ** → **Менеджер доменов**.

Откроется страница **Список подключенных доменов** (рис. 65). Страница менеджера доменов представляет из себя таблицу с тремя столбцами:

- Полностью определенное имя домена (FQDN);
- Способ добавления:
 - Автоматически;
 - Вручную;
- Комментарий.

Менеджер доменов

Список подключенных доменов

Менеджер обеспечивает возможность регистрации в Домене безопасности ЕЦУ учетных записей, созданных посредством доменных служб Active Directory, FreeIPA, ALD PRO, Ред АДМ, Samba

☒ **Автоматическое добавление доступных доменов при старте службы ЕЦУ**

Полностью определенное имя домена (FQDN)	Способ добавления	Комментарий

Рис. 65. Страница «Список подключенных доменов»

Для автоматического добавления домена нужно поставить чекбокс напротив строки *Автоматическое добавление доступных доменов при старте службы ЕЦУ*.

! Автоматическое добавление домена доступно только при условии, что ПК, на котором установлена служба **ЕЦУ**, введен в домен или является контроллером домена. При соблюдении данного условия возможно также и ручное добавление домена. При несоблюдении данного условия добавление домена требуется выполнять исключительно вручную.

Для того чтобы добавить новый домен вручную, необходимо:

1. Нажать на кнопку **Добавить новый домен**. На экране появится окно подключения к домену (рис. 66).

Подключение к домену

Введите имя домена

Комментарий

Рис. 66. Подключение к домену

2. Ввести имя домена и указать комментарий (при необходимости).
3. Нажать кнопку **Добавить**.
4. Убедиться, что домен появился в таблице.

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

4.9 Параметры работы

Параметры работы **ЕЦУ Dallas Lock** настраиваются в главном меню Консоли **ЕЦУ**  → **Параметры** (рис. 67).

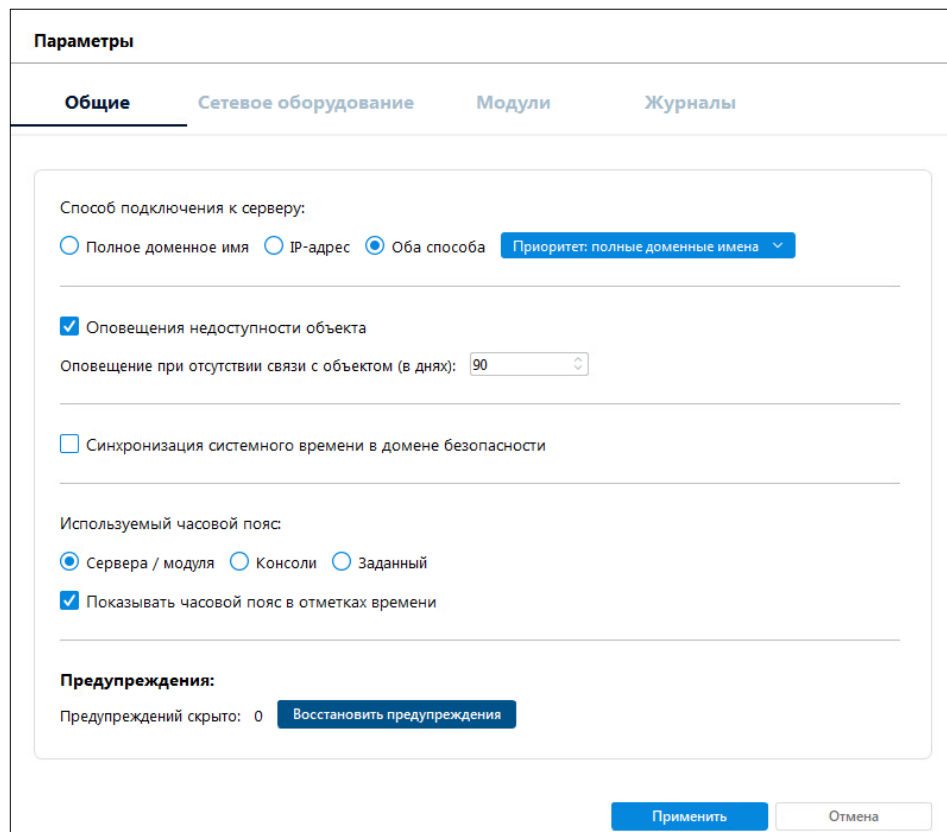


Рис. 67. Страница «Параметры»

4.9.1 Общие параметры работы

На вкладке **Общие** настраиваются параметры, общие для всех объектов ДБ (рис. 67).

На данной вкладке доступен выбор используемого способа подключения к серверу **ЕЦУ Dallas Lock**:

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

На вкладке производится настройка параметра **Оповещение недоступности объекта** с возможностью отключения/включения данного параметра и установки значения срока в днях, по истечении которого поступает оповещение об отсутствии связи с объектом.

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

Параметр **Используемый часовой пояс** позволяет выбрать источник часового пояса с помощью радиокнопки со значениями: *Сервера/модуля*, *Консоли* и *Заданный*. Также параметр

Используемый часовой пояс позволяет задать вид отображения времени в журналах Консоли ЕЦУ.

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

4.9.2 Параметры сетевого оборудования

На вкладке *Сетевое оборудование* задается периодичность проверок сетевого оборудования по протоколу SNMP и SSH (рис. 68).

The screenshot shows a web interface titled 'Параметры' (Parameters) with four tabs: 'Общие' (General), 'Сетевое оборудование' (Network Equipment), 'Модули' (Modules), and 'Журналы' (Logs). The 'Сетевое оборудование' tab is active. It contains the following settings:

- ☒ Периодическая проверка доступности (Periodic availability check). Below it, a dropdown menu for 'Периодичность проверки доступности (в минутах):' (Availability check frequency in minutes) is set to 60.
- ☒ Периодическая проверка целостности (Periodic integrity check). Below it, a dropdown menu for 'Периодичность проверки целостности (в минутах):' (Integrity check frequency in minutes) is set to 360.
- Обновление конфигурационных файлов сетевых устройств (Update network device configuration files) with a 'Выбрать...' (Select...) button.
- Syslog-сервер: (Syslog server):
 - ☒ Прием UDP-сообщений, порт: 514 (Receive UDP messages, port: 514)
 - ☐ Прием TCP-сообщений, порт: 1468 (Receive TCP messages, port: 1468)
- Фильтрация сообщений по важности (Message filtering by importance):
 - ☒ [Уровень 0] Чрезвычайная ситуация (Level 0: Emergency)
 - ☒ [Уровень 1] Тревога (Level 1: Alarm)
 - ☒ [Уровень 2] Критическое событие (Level 2: Critical event)
 - ☒ [Уровень 3] Ошибка (Level 3: Error)
 - ☒ [Уровень 4] Предупреждение (Level 4: Warning)
 - ☒ [Уровень 5] Уведомление (Level 5: Notification)
 - ☐ [Уровень 6] Информационное сообщение (Level 6: Informational message)
 - ☐ [Уровень 7] Отладочное сообщение (Level 7: Debug message)

At the bottom right, there are 'Применить' (Apply) and 'Отмена' (Cancel) buttons.

Рис. 68. Параметры SNMP и SSH

Доступны следующие параметры:

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

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

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

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

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

Ниже доступны следующие настройки Syslog-сервера:

- включение/выключение с помощью чекбокса приема Syslog-сообщений по UDP-протоколу и назначение соответствующего порта. По умолчанию чекбокс включен, поле *порт* активно, установлен 514 порт;
- включение/выключение с помощью чекбокса приема Syslog-сообщений по TCP-протоколу и назначение соответствующего порта. По умолчанию чекбокс выключен, поле *порт* неактивно, установлен 1468 порт;
- настройка уровней важности сообщений (таблица 4), обработку которых **ЕЦУ Dallas Lock** должен осуществлять. По умолчанию включены чекбоксы для уровней 0-5.

Таблица 4. Классификация уровней важности событий в Syslog

Значение	Уровень серьезности	Описание
0	Чрезвычайная ситуация (emergencies)	Система не работоспособна
1	Тревога (alerts)	Необходимо срочное вмешательство
2	Критические события (critical)	Критические события о состоянии СУ
3	Сообщения об ошибках (errors)	Условия ошибки
4	Всевозможные предупреждения (warning)	Условия предупреждения
5	Важные уведомления (notifications)	Нормальные, но важные условия (не являются ошибочными состояниями, но требуют особого внимания)
6	Информационные сообщения (informational)	Иные информационные сообщения, не требующие особого внимания
7	Отладочные сообщения (debugging)	Сообщения содержат информацию, используемую только при отладке

4.9.3 Параметры работы модулей

На вкладке *Модули* задается периодичность сбора журналов и синхронизации **ЕЦУ Dallas Lock** с модулями (рис. 69).

Существует возможность выбора необходимых типов объектов для работы в данном экземпляре консоли. В блоке *Выбор отображаемых модулей* необходимо проставить флаги рядом с объектами, с которыми предполагается работа в консоли.



При выборе функции *Автоматический режим* в меню **Выбор отображаемых модулей** будут включены флаги только введенных в ДБ модулей.

Параметры

Общие
Сетевое оборудование
Модули
Журналы

Выбор отображаемых модулей

Выберите необходимые модули для отображения их настроек в консоли:

Dallas Lock 8.0 ИК8

Dallas Lock 8.0 ИК9

Dallas Lock 8.0 ИК10

Dallas Lock 8.0 ИК11

CD3 Dallas Lock ИК4

CD3 Dallas Lock ИК5

CD3 УБ Dallas Lock ИК0

CD3 УБ Dallas Lock ИК1

Автоматический режим

Параметры

Период сбора журналов с модулей:

Никогда

Период синхронизации:

Никогда

Работа с отчетами

Периодичность проверки целостности:

5 мин.

Применить

Отмена

Рис. 69. Параметры модулей

В блоке *Параметры* настраиваются период сбора журналов с модулей и период синхронизации. Политики могут принимать значения от 5 минут до 1 недели и «Никогда». Значение по умолчанию — «Никогда».

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

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

4.9.4 Параметры журналов

На вкладке *Журналы* (рис. 70) в блоке *Выбор системы хранения журналов* отображается информация о текущем способе хранения журналов, выбранном в процессе установки, а также возможность редактирования способа хранения журналов уже на установленном **ЕЦУ Dallas Lock**.

67

При выборе *Использовать PostgreSQL* необходимо заполнить поля:

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

При выборе *Использовать внутреннюю систему хранения* заполнять поля не нужно.

По умолчанию выбрано значение *Использовать внутреннюю систему хранения*.

The screenshot shows the 'Parameters' window with the 'Logs' tab selected. Under the 'Log storage system selection' section, there are two radio buttons: 'Use internal storage system' (selected) and 'Use PostgreSQL'. Below these are input fields for 'Server address', 'Connection port' (set to 5432), 'Database name', 'Username', and 'Password'.

Рис. 70. Параметры хранения журналов

В блоке *Параметры архивации журналов* (рис. 71) производится настройка параметров архивации, которая активируется путем установки флага *Использовать архивацию журналов* — по умолчанию флаг не установлен, архивация отключена.

The screenshot shows the 'Log archiving parameters' window. It starts with an unchecked checkbox 'Use log archiving'. Below is a 'Log archiving schedule' section with a table for scheduling. The table has columns for days of the week (Пн, Вт, Ср, Чт, Пт, Сб, Вс) and rows for times from 00:00 to 22:00. A blue highlight is visible in the 'Пт' column at 20:00. Below the table, there is a dropdown for 'Archive logs older than' (set to 6 months), a checkbox for 'Archive size' (set to 16 GB), and an information icon with a note: 'The parameter sets a limit on the volume of data occupied. Upon reaching the set limit, old records in the archive will be deleted.' At the bottom right are 'Apply' and 'Cancel' buttons.

	Пн	Вт	Ср	Чт	Пт	Сб	Вс
00:00							
02:00							
04:00							
06:00							
08:00							
10:00							
12:00							
14:00							
16:00							
18:00							
20:00							
22:00							

Рис. 71. Параметры архивации журналов

По умолчанию архивируются все записи в журналах старше 6 месяцев в зависимости от установленного расписания, настраиваемого в таблице *Расписание архивации* (по умолчанию в таблице выбраны ячейки со значениями «Пт», «20:00»).

Параметр **Расписание архивации** является обязательным для заполнения. При попытке применения настроек архивации без выбора расписания выводится соответствующая ошибка (рис. 72).

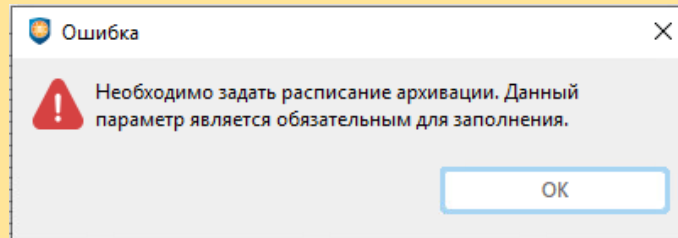


Рис. 72. Сообщение об ошибке

Срок хранения журналов можно изменить путем выбора необходимого значения из выпадающего списка параметра **Архивировать журналы старше**.



Для просмотра записи из архива необходимо указать в фильтрах журналов нужную дату.

Дополнительно, во избежание переполнения системы хранения, можно настроить ограничение по размеру архива, для чего необходимо установить флаг *Размер архива* (если флаг установлен, поле является обязательным для заполнения), после чего ввести требуемое значение (в ГБ) в текстовом поле — при достижении лимита старые записи в архиве будут удаляться.



Если в поле *Размер архива* выставить значение 0, то записи архивироваться не будут (все записи архива будут удалены, даже если только что были записаны новые).



Если на АРМ, на котором установлена служба **ЕЦУ**, свободного места менее 20 ГБ, то генерируется инцидент безопасности *Переполнение диска*, если свободного места менее 5 ГБ — генерируется инцидент безопасности *Переполнение диска* и отключается сбор журналов с модулей.

5 ДОМЕН БЕЗОПАСНОСТИ ЕЦУ

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

5.1 Сводка для ДБ

Для удобства работы возможно узнать общее состояние всего ДБ, данные сведения отображаются на вкладке *Сводка* (рис. 73).

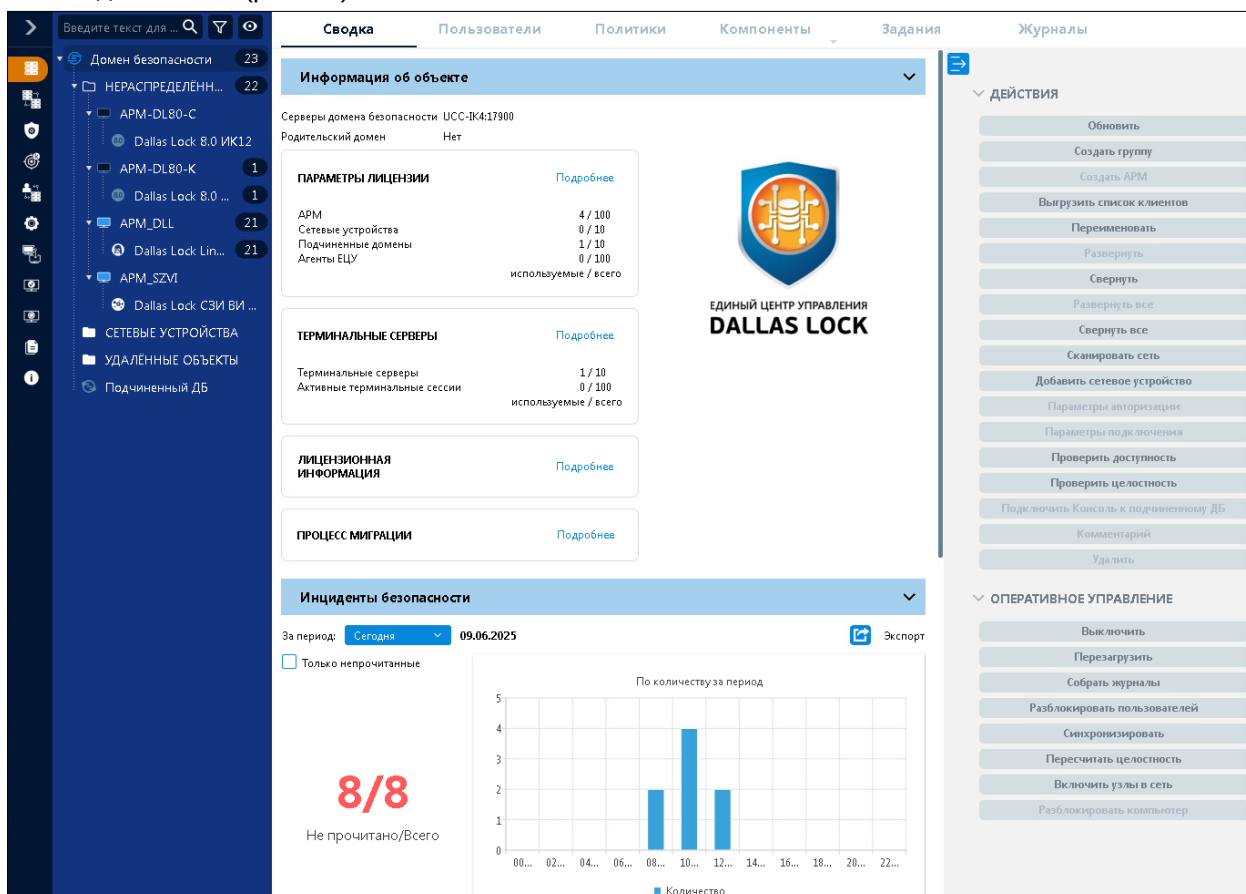


Рис. 73. «Сводка» Домена безопасности ЕЦУ

Доступны следующие действия с ДБ на панели инструментов:

1. Обновить информацию об объекте на вкладке *Сводка*;
2. Создать новую группу объектов в ДБ;
3. Выгрузить список клиентов;
4. Переименовать текущий ДБ;
5. Свернуть;
6. Развернуть все;
7. Свернуть все;
8. Сканировать сеть для обнаружения модулей и сетевых устройств;
9. Добавить новое сетевое устройство;
10. Проверить доступность сетевых устройств;
11. Проверить целостность сетевых устройств.

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

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

1. Выключить;
2. Перезагрузить;
3. Собрать журналы;
4. Сбросить блокировки;
5. Включить/выключить аварийный режим;
6. Разблокировать пользователей;
7. Синхронизировать;
8. Пересчитать целостность;
9. Включить/отключить аварийный режим;
10. Сделай мастером.

В рабочей области вкладки *Сводка* расположены следующие разделы:

1. «Информация об объекте» (рис. 74).

В данном разделе выводится информация:

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

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

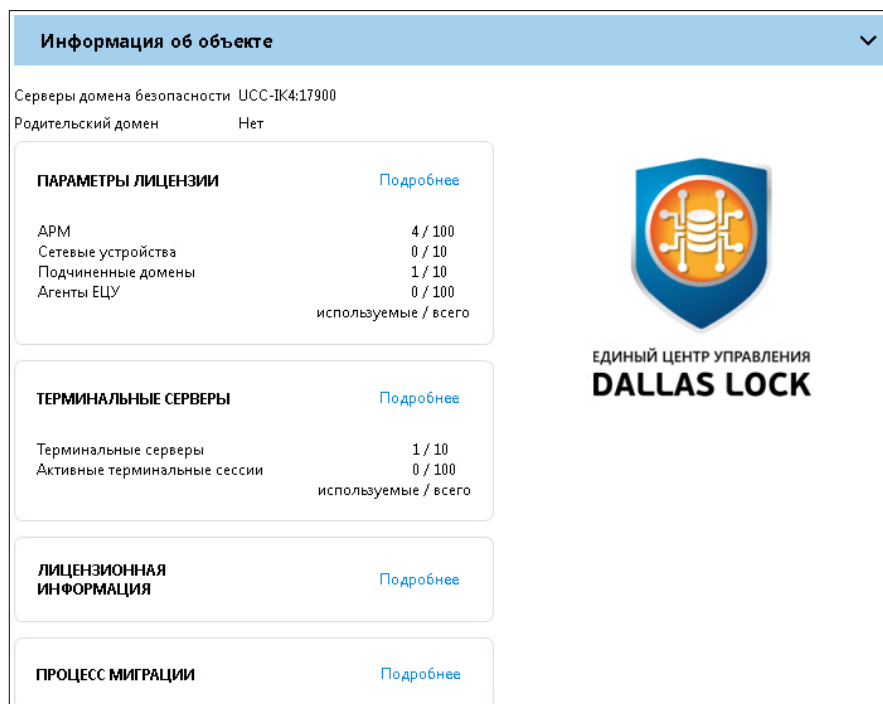


Рис. 74. Раздел «Информация об объекте»

2. «Инциденты безопасности» (рис. 75).

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

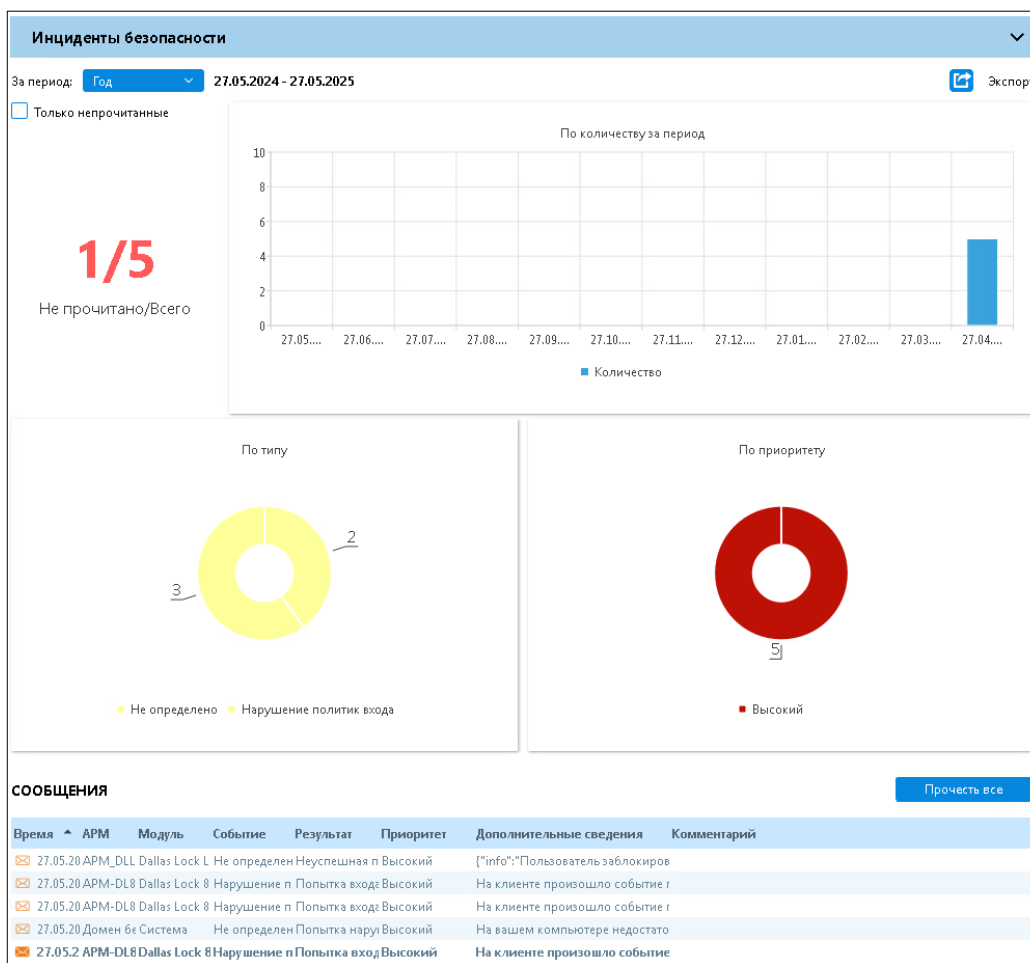


Рис. 75. Раздел «Инциденты безопасности»

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

- сегодня;
- вчера;
- неделя;
- месяц;
- год;
- за все время;
- выбрать свой — при выборе данного пункта в появившемся окне (рис. 76) возможно задать необходимый отрезок времени.

Выберите период времени

Период

С: 04.06.2024 16:31

По: 04.06.2025 16:31

Применить Отмена

Рис. 76. Выбор периода времени

В центральной части информационной панели *Инциденты безопасности* расположена гистограмма, которая отображает количество инцидентов безопасности всех типов за выбранный период времени с определенным шагом (рис. 75). При нажатии на элемент гистограммы, в таблице отображаются инциденты за выбранный шаг времени.

Под гистограммой расположены круговые диаграммы:

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

Подробнее о настройке отображения информационной панели *Инциденты безопасности* описано в разделе [«Настройка инцидентов безопасности»](#).

В нижней части данной информационной панели расположена таблица с сообщениями об инцидентах безопасности. С помощью контекстного меню можно управлять списком инцидентов безопасности (рис. 75):

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

Двойной клик по сообщению с инцидентом откроет окно с данными об этом инциденте (рис. 77), в таблице выбранное сообщение квитируется как прочитанное (при отсутствии чекбокса в контекстном меню *Не квитировать при просмотре*). Нажимая на кнопки **вверх** и **вниз**, можно отмечать сообщения как прочитанные, просматривая предыдущие или следующие инциденты. По кнопке **Перейти к модулю** → можно перейти к модулю, для которого зарегистрирован данный инцидент безопасности.

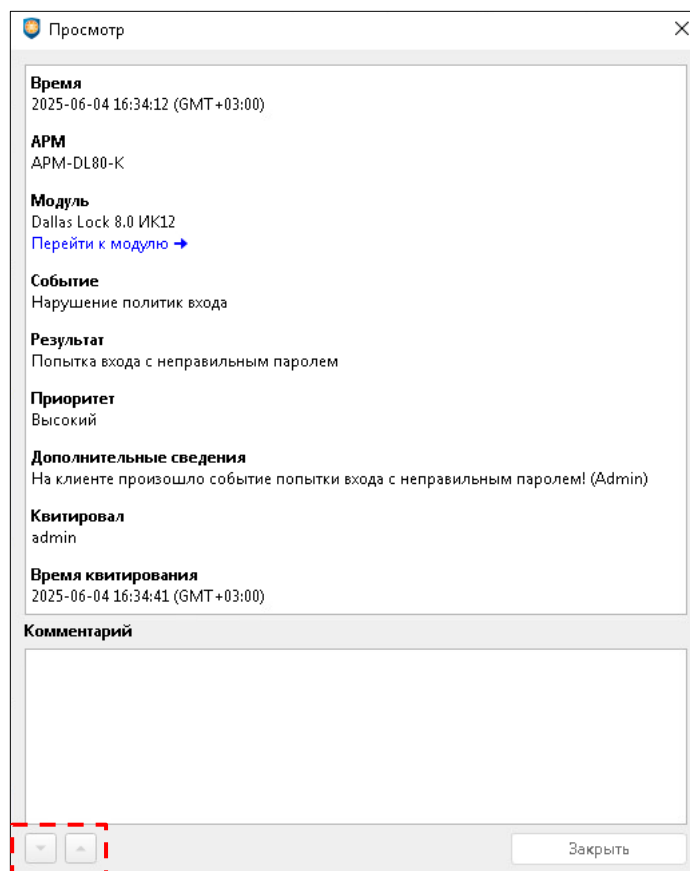


Рис. 77. Список учетных записей ДБ ЕЦУ

Реализована возможность экспорта отчета об инцидентах безопасности в файл по кнопке **Экспорт** (рис. 78). После нажатия **Экспорт**, в появившемся окне, нужно указать путь для сохранения отчета (в формате .html, .txt или .csv) с данными из таблицы с инцидентами безопасности.

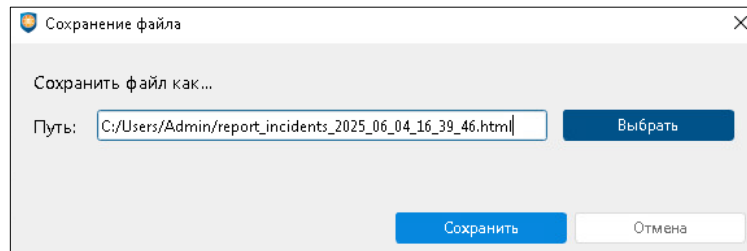


Рис. 78. Экспорт инцидентов безопасности в файл

В выгрузку отчета входит список инцидентов безопасности, который будет сохранен в виде таблицы с указанием события, времени, результата и модуля. Доступные форматы для выгрузки: txt, html и csv.



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

5.2 Пользователи ДБ

Вкладка *Пользователи* на уровне ДБ позволяет управлять глобальными учетными записями, группами пользователей ДБ **ЕЦУ Dallas Lock** и аппаратными идентификаторами (рис. 79).

Сводка	Пользователи		Политики	Компоненты	Задания	Журналы
	Пользователи	Группы	Аппаратные идентификаторы			
☒ Сост...	Учетная запись	Категория	Тип учетной записи ЕЦУ	Владелец	Роль администрирования	Полное имя
☒	admin	Глобальная	Все	Локальный	Администратор	Администратор по умолчанию
☒	anonymous	Глобальная	Система, DL8.0 (ИК10, ИК11), СЗИ ВИ (ИК4)	Локальный	Не назначено	Anonymous user
						Используется для сетевых входов с ...

Рис. 79. Список учетных записей ДБ ЕЦУ

5.2.1 Параметры пользователей

Категория **Пользователи** на уровне ДБ содержит список глобальных и модульных учетных записей ДБ.

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

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

- ☒ — отмеченное флагом поле означает, что данная учетная запись пользователя имеет доступ на уровне ДБ;
- ☐ — пустое поле означает, что учетная запись отключена для работы на уровне ДБ;



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

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

2. «Учетная запись» — содержит имя учетной записи;

3. «Категория» — содержит информацию о том, где была создана учетная запись;
4. «Тип учетной записи ЕЦУ» — содержит информацию о том, для модулей какого типа применяется данная учетная запись. Возможные значения:
 - Все — учетная запись применима для всех модулей (кроме модуля **WAF**);
 - DL 8.0 — учетная запись применима для модуля **СЗИ Dallas Lock 8.0** (см. [«МОДУЛЬ СЗИ DALLAS LOCK 8.0-С/К»](#));
 - DLL — учетная запись применима для модуля **СЗИ НСД Dallas Lock Linux** (см. [«МОДУЛЬ СЗИ НСД DALLAS LOCK LINUX»](#));
 - DL 8.0 СЗИ ВИ — учетная запись применима для модуля **СЗИ ВИ Dallas Lock** (см. [«МОДУЛЬ СЗИ ВИ DALLAS LOCK»](#));
 - СДЗ — учетная запись применима для модуля **СДЗ Dallas Lock** (см. [«МОДУЛЬ СДЗ DALLAS LOCK»](#));
 - СДЗ УБ — учетная запись применима для модуля **СДЗ УБ Dallas Lock** (см. [«МОДУЛЬ СДЗ УБ DALLAS LOCK»](#));
5. «Полное имя» — содержит полное имя учетной записи;
6. «Описание» — содержит описание учетной записи;
7. «Владелец» — указывает на каком уровне дерева **ЕЦУ Dallas Lock** была создана учетная запись;



Учетные записи не отображаются на вкладке *Пользователи* 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.



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*».

8. «Роль администрирования» (см. [«Ролевая модель учетных записей ДБ»](#)).

Для применения изменений списка учетных записей на модулях необходима синхронизация.

На панели управления в блоке *Фильтры* предусмотрена возможность фильтрации пользователей в соответствии с выбранными параметрами.

В категории **Пользователи** на вкладке *Пользователи* доступно только:

- создание и удаление пользователей;
- редактирование свойств пользователей;
- изменение типа, владельца и роли пользователей;
- сохранения списка пользователей.

При нажатии на кнопку **Сохранить список пользователей** открывается диалоговое окно, в котором необходимо выбрать папку для сохранения и ввести имя файла. В выгрузку входит полный список пользователей из **ЕЦУ**, который будет сохранен в виде таблицы с указанием имени учетной записи, типа и ip-адреса. Доступные форматы для выгрузки: txt и html.

Просмотр и настройка параметров пользователей доступны:

- по двойному щелчку левой кнопкой мыши на пользователя в списке;
- при выборе пункта *Свойства* из контекстного меню, вызванного щелчком правой кнопки мыши на пользователе в списке;
- при выделении учетной записи в списке и выборе пункта *Свойства* на панели инструментов *Операции с пользователями* (рис. 79).



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

После выполнения одного из этих действий открывается окно **Редактирование полей пользователя** (рис. 80).

Рис. 80. Редактирование полей пользователя

На вкладке **Общие** предлагается заполнить учетные данные и параметры пользователей (таблица 5).

Таблица 5. Общие параметры пользователей

Заполняемые данные и параметры	Применение
Поле <i>Аппаратный идентификатор</i> позволяет выбрать аппаратный идентификатор пользователя.	ЕЦУ Dallas Lock; СЗИ Dallas Lock 8.0; СДЗ Dallas Lock; СДЗ УБ Dallas Lock; СЗИ НСД Dallas Lock Linux
В поле <i>Описание</i> можно ввести любой комментарий. Длина комментария не более 95 символов. Вводить комментарий не обязательно	ЕЦУ Dallas Lock; СЗИ Dallas Lock 8.0; СЗИ НСД Dallas Lock Linux; СДЗ Dallas Lock; СДЗ УБ Dallas Lock; СЗИ ВИ Dallas Lock

В поле <i>Полное имя</i> указывается полное имя пользователя. Заполнять необязательно. По умолчанию поле имеет пустое значение.	ЕЦУ Dallas Lock; СЗИ Dallas Lock 8.0; СЗИ НСД Dallas Lock Linux; СЗИ ВИ Dallas Lock
Атрибут <i>Тип учетной записи Windows</i> позволяет выбрать один из типов учетных записей: внутренний, внешний, системный, приложение, гостевой (анонимный), временный. Для типа «Временный» обязательным условием является настройка расписания работы пользователя. По умолчанию тип учетной записи пользователя будет иметь значение «Не указан»	СЗИ Dallas Lock 8.0; СЗИ ВИ Dallas Lock
Значение «Да» в поле <i>Служебный пользователь Windows</i> предоставляет данной учетной записи пользователя особый статус. Требуется для корректной работы программ, при установке которых создаются свои учетные записи пользователей и осуществляется автоматический вход при загрузке ОС. Например, такой статус необходим при использовании программ VipNet или VMware. По умолчанию поле имеет значение «Нет»	СЗИ Dallas Lock 8.0; СЗИ ВИ Dallas Lock
Система защиты обеспечивает проверку целостности программно-аппаратной среды ПК, объектов ФС и реестра. Если для пользователя опция <i>Запрет входа при нарушении целостности</i> 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. По умолчанию поле имеет значение «Нет»	СЗИ Dallas Lock 8.0; СДЗ Dallas Lock; СДЗ УБ Dallas Lock; СЗИ ВИ Dallas Lock
В поле <i>Категория пользователя СДЗ</i> можно выбрать роль пользователя: Пользователь, Аудитор или Администратор. Значение поля по умолчанию — «Пользователь»  Штатные пользователи, допущенные к работе на защищенном компьютере, не должны иметь категорию <i>Администраторы</i> или <i>Аудиторы</i> .	СДЗ Dallas Lock; СДЗ УБ Dallas Lock
Атрибут <i>Автовход в СЗИ НСД</i> позволяет настроить автовход в СЗИ Dallas Lock 8.0 . По умолчанию параметры автовхода не заданы.  Данный атрибут не применим для вариантов исполнения изделия ПФНА.26.20.40.140.001-04 и ПФНА.26.20.40.140.001-05 (платы СДЗ Dallas Lock формата USB «KT-600-PLS» и USB «KT-600-Type A»).	СДЗ Dallas Lock
В поле <i>Имя</i> указывается пользователь, атрибут необходим для синхронизации и ввода модуля в ЕЦУ . По умолчанию поле имеет пустое значение.	СЗИ НСД Dallas Lock Linux; СЗИ ВИ Dallas Lock
В поле <i>Фамилия</i> указывается пользователь, атрибут необходим для синхронизации и ввода модуля в ЕЦУ . По умолчанию поле имеет пустое значение.	СЗИ НСД Dallas Lock Linux; СЗИ ВИ Dallas Lock
В поле <i>Отчество</i> указывается пользователь, атрибут необходим для синхронизации и ввода модуля в ЕЦУ . По умолчанию поле имеет пустое значение.	СЗИ НСД Dallas Lock Linux

В поле <i>Основная группа</i> указывается наименование основной группы пользователя. Поле заполняется во время создания учетной записи. По умолчанию поле имеет пустое значение	СЗИ НСД Dallas Lock Linux
Значение «Да» в поле <i>Системный пользователь Linux</i> указывает на то, что учетная запись пользователя является системной. По умолчанию поле имеет значение «Нет»	СЗИ НСД Dallas Lock Linux
Поле <i>Интерпретатор</i> указывает на интерпретатор командной строки. Обязательный атрибут учетной записи пользователя. По умолчанию имеет значение «/bin/bash».	СЗИ НСД Dallas Lock Linux
В поле <i>Домашняя директория</i> указывается путь к домашней директории пользователя. По умолчанию поле имеет пустое значение	СЗИ НСД Dallas Lock Linux
Значение «Да» в поле <i>Создать директорию</i> 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 «Да».	СЗИ НСД Dallas Lock Linux
В поле <i>Домен для Linux</i> указывается имя домена Active Directory, FreeIPA, ALD PRO, Ред АДМ, Samba. Атрибут обязателен для доменных учетных записей пользователей. По умолчанию поле имеет пустое значение	СЗИ НСД Dallas Lock Linux
В поле <i>Роль администрирования СЗИ Dallas Lock Linux</i> можно назначить категорию пользователя: Пользователь, Аудитор или Администратор. Значение поля по умолчанию — «Пользователь».	СЗИ НСД Dallas Lock Linux
 Штатные пользователи, допущенные к работе на защищенном компьютере, не должны иметь категорию «Администраторы» или «Аудиторы».	
В поле <i>e-mail</i> указывается электронная почта пользователя. Заполнять поле необязательно.	СЗИ ВИ Dallas Lock
В поле <i>Тип учетной записи (для СЗИ ВИ ИК4)</i> можно выбрать пользователей гипервизора. По умолчанию поле имеет значение «Пользователь Windows (Dallas Lock)».	СЗИ ВИ Dallas Lock
В поле <i>Роль пользователя консоли СЗИ ВИ</i> указывается роль пользователя в консоли СЗИ ВИ . По умолчанию поле имеет значение «Нет доступа».	СЗИ ВИ Dallas Lock
 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 <i>Администратор СЗИ ВИ</i> имеет значение «Да».	
Поле <i>Разрешить локальный вход в ОС с ЦУ СЗИ ВИ</i> по умолчанию имеет значение «Нет».	СЗИ ВИ Dallas Lock
Поле <i>e-mail</i> позволяет указать адрес электронной почты пользователя.	СЗИ ВИ Dallas Lock

В поле <i>Тип учетной записи (для СЗИ ВИ ИК5)</i> можно выбрать пользователей гипервизора. Поле имеет значение «Пользователь web-консоли ЦУ СЗИ ВИ (встроенные)» и недоступно для редактирования.	СЗИ ВИ Dallas Lock
В поле <i>Роль пользователя web-консоли СЗИ ВИ</i> указывается роль пользователя web-консоли СЗИ ВИ . По умолчанию поле имеет значение «Аудитор».	СЗИ ВИ Dallas Lock

На вкладке *Пароли* предлагается заполнить учетные данные и параметры пользователей, относящиеся к настройкам паролей (таблица 6).

Таблица 6. Параметры паролей пользователей

Заполняемые данные и параметры	Применение
Значение «Да» в поле <i>При следующем входе требовать смену пароля</i> означает, что одновременно 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; СДЗ УБ Dallas Lock; СЗИ ВИ Dallas Lock
Поле <i>Запрет изменения пароля</i> . По умолчанию поле имеет значение «Нет».	СЗИ Dallas Lock 8.0; СДЗ Dallas Lock; СДЗ УБ Dallas Lock; СЗИ ВИ Dallas Lock
Значение «Да» в поле <i>Пароль без ограничения срока действия</i> 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; СДЗ УБ Dallas Lock; СЗИ ВИ Dallas Lock
Поле <i>Максимальный срок действия пароля (в днях)</i> указывает на максимальный срок действия пароля в днях. 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 8.0; СДЗ Dallas Lock; СДЗ УБ Dallas Lock; СЗИ ВИ Dallas Lock; СЗИ НСД Dallas Lock Linux ¹¹
 Если нарушено соотношение максимального и минимального сроков действия пароля (минимальный срок больше максимального), то при синхронизации списка пользователей с модулями СЗИ НСД Dallas Lock Linux возникает ошибка, создание / изменение параметров таких учетных записей не осуществляется.	
Поле <i>Дата последней смены пароля</i> . По умолчанию поле имеет значение «Не определено».	СЗИ Dallas Lock 8.0; СДЗ Dallas Lock; СДЗ УБ Dallas Lock; СЗИ ВИ Dallas Lock; СЗИ НСД Dallas Lock Linux ¹¹

¹¹ Список параметров может меняться в зависимости от версии клиента.

На вкладке *Мандатный доступ* предлагается заполнить учетные данные и параметры, относящие к работе пользователя с уровнями доступа и мандатными метками в Домене безопасности (таблица 7).

Таблица 7. Мандатный доступ пользователей

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

На вкладке *Сеансы и расписание* предлагается заполнить учетные данные и параметры, относящиеся к ограничениям работы пользователя по времени (таблица 8).

Таблица 8. Сеансы и расписание пользователей

Заполняемые данные и параметры	Применение
Определить <i>Число разрешенных сеансов</i>. При установленном значении для каждой учетной записи будет проверяться количество одновременных интерактивных и сетевых сессий (входов) на модуле. По умолчанию поле имеет значение «Не используется»	СЗИ Dallas Lock 8.0; СЗИ НСД Dallas Lock Linux; СЗИ ВИ Dallas Lock
Необходимо задать <i>Расписание работы</i> 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). По умолчанию имеет значение «Без ограничения».  «Расписание работы» пользователя может быть определено с дискретностью 30 минут.	СЗИ Dallas Lock 8.0; СДЗ Dallas Lock; СДЗ УБ Dallas Lock; СЗИ НСД Dallas Lock Linux; СЗИ ВИ Dallas Lock
Указать допустимый <i>Период неиспользования (в днях)</i>. 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 НСД Dallas Lock Linux
Задать дату <i>Истечение срока действия учетной записи</i>. По умолчанию поле имеет значение «Без ограничений». При снятом флаге <i>Без ограничений</i> становится активным поле для выбора даты. В поле указывается дата, когда данная учетная запись будет заблокирована системой. В этом случае поле обязательно для заполнения. При активном флаге поле для установки даты неактивно, время действия учетной записи не ограничено.	СЗИ НСД Dallas Lock Linux

На вкладке *Запрет работы* предлагается заполнить учетные данные и параметры, относящиеся к ограничению работы пользователя при наступлении определенных событий в системе или установки запрета администратором (таблица 9).

Таблица 9. Запрет работы пользователей

Заполняемые данные и параметры	Применение
Значение «Да» в поле <i>Учетная запись отключена</i> 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; СДЗ УБ Dallas Lock; СЗИ ВИ Dallas Lock; СЗИ НСД Dallas Lock Linux
При значении «Да» поля <i>Запретить работу при событиях вскрытия корпуса</i> вход в систему блокируется при срабатывании ДВК. На экране приглашения в систему отображается соответствующее сообщение. По умолчанию поле имеет значение «Нет».  Данный атрибут применим только для варианта исполнения изделия ПФНА.26.20.40.140.001-01 (платы СДЗ Dallas Lock формата PCIe «КТ-500»).	СДЗ Dallas Lock
Значение «Да» в поле <i>Блокировать загрузку нештатной ОС</i> устанавливает запрет на загрузку ОС с носителя, отличающегося от указанного в поле <i>Загрузочное устройство</i> вкладки <i>Параметры</i> оболочки администратора СДЗ Dallas Lock. По умолчанию поле имеет значение «Да».	СДЗ Dallas Lock; СДЗ УБ Dallas Lock
При значении «Да» поля <i>Запретить работу при сломанных или ненастроенных часах</i> вход в систему блокируется при неисправности часов. На экране приглашения в систему отображается соответствующее сообщение. По умолчанию поле имеет значение «Нет».  Данный атрибут применим только для варианта исполнения изделия ПФНА.26.20.40.140.001-01 (платы СДЗ Dallas Lock формата PCIe «КТ-500»).	СДЗ Dallas Lock
При значении «Да» поля <i>Запретить работу при неисправности ДСЧ</i> 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».  Данный атрибут не применим для вариантов исполнения изделия ПФНА.26.20.40.140.001-04 и ПФНА.26.20.40.140.001-05 (платы СДЗ Dallas Lock формата USB «КТ-600-PLS» и USB «КТ-600-Type A»).	СДЗ Dallas Lock

На вкладке *Список групп* с помощью кнопки **Добавить...** администратор имеет возможность включить пользователя в определенную группу. В основной рабочей области отображены названия групп, в которые включен пользователь (рис. 81). При выборе группы из основной рабочей области ее возможно удалить из списка с помощью кнопки **Удалить**.

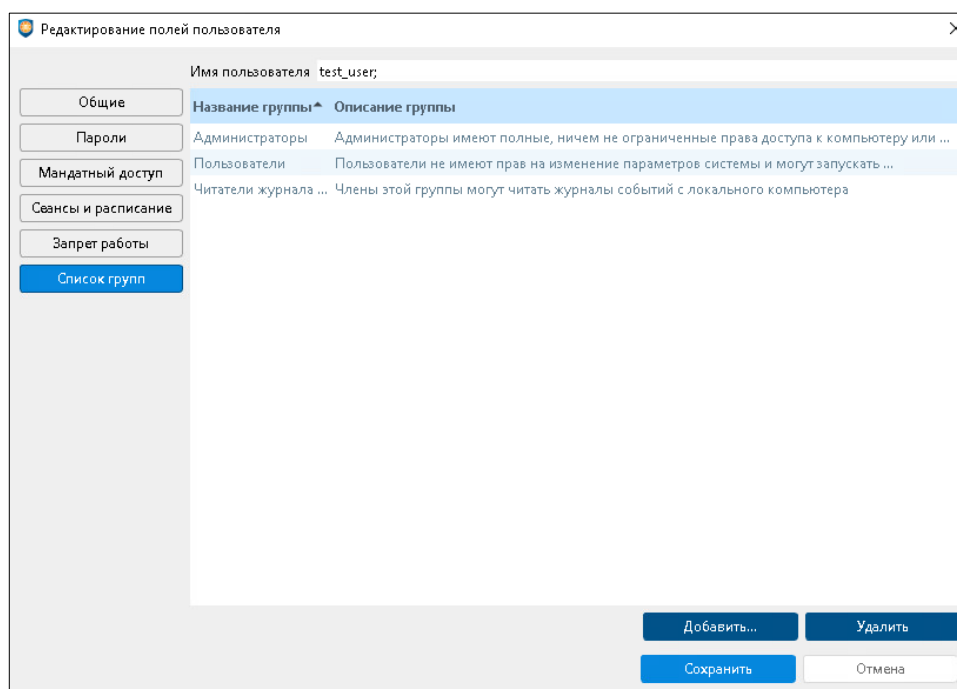


Рис. 81. Список групп пользователя

5.2.2 Параметры групп пользователей

Категория *Группы* на уровне ДБ содержит список глобальных и модульных учетных записей ДБ.

Рабочая область категории *Группы* представляет собой таблицу с полями:

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

- ☒ — отмеченное флагом поле означает, что данная группа пользователей имеет доступ на уровне ДБ;
- ☐ — пустое поле означает, что данная группа пользователей не имеет доступа на уровне ДБ.



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

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

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



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



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* доступно только:

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

На панели управления в блоке *Фильтры* предусмотрена возможность фильтрации групп пользователей в соответствии с выбранными параметрами и модулями.

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 выборе пункта **Свойства** на панели инструментов *Операции с группами*.

После выполнения одного из этих действий открывается окно *Редактирование полей группы* (рис. 82).

Название группы Test;	
Описание группы	
Администраторы СЗИ ВИ	Нет
Тип учетной записи (для СЗИ ВИ)	Группа Windows (Dallas Lock)

Рис. 82. Редактирование полей групп

На вкладке *Общие* предлагается оставить комментарий в поле *Описание группы*, обозначить, являются ли участники группы Администраторами **СЗИ ВИ**, и выбрать тип учетной записи (для **СЗИ ВИ**).

На вкладке *Dallas Lock Linux* предлагается выбрать значение атрибута *Системная группа*.

Системная группа — это группа, которой присваивается уникальный идентификатор (GUID — Globally Unique Identifier), числовое значение которого не превышает 1000¹².

Атрибут принимает значения «Да» и «Нет». По умолчанию значение атрибута «Нет».



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

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



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** → **Пользователи** формируется из учетных записей по умолчанию и зарегистрированных через Консоль **ЕЦУ**.

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

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

В **ЕЦУ Dallas Lock** возможна регистрация пользователей следующих видов:

1. Глобальные пользователи, созданные средствами Консоли **ЕЦУ**.
2. Доменные пользователи, созданные средствами службы AD (если ДБ находится в ЛВС под управлением контроллера домена) (см. [«Регистрация доменных пользователей в ДБ»](#)).

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* в Консоли **ЕЦУ**.
2. Выбрать категорию **Пользователи**.
3. На панели инструментов в операциях с пользователями нажать **Создать** или выбрать соответствующий пункт из контекстного меню.
4. На экране появится окно создания пользователя (рис. 83).

Рис. 83. Создание пользователя

5. В поле источник выбрать *Встроенный*.

12 На Альт Линукс значение GUID не превышает 500.

6. В поле *Имя пользователя* ввести логин (имя) регистрируемого пользователя. При вводе имени в системе существуют следующие правила:
- максимальная длина имени — 20 символов;
 - имя может содержать латинские символы, символы кириллицы, цифры и специальные символы (кроме запрещенных ОС: " \ [] : | < > + = ; , ? @ *);
 - имена объектов дерева не чувствительны к регистру символов, что позволяет использовать различные регистры клавиатуры без учета их различий (User и user являются одинаковыми именами);



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.



Имя учетной записи считается уникальным в рамках одного Домена безопасности.



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.



При создании учетной записи администратора Консоли **ЕЦУ** рекомендуется выставлять единственный тип учетной записи — *Система*, в ином случае учетная запись будет активна и на других указанных в данном параметре модулях, что может привести к некорректному изменению ее параметров пользователями данных модулей.

8. После нажатия **Продолжить** появится окно для редактирования параметров учетной записи пользователя (см. [«Параметры пользователей»](#)).

Изменить параметры учетной записи можно, используя кнопку **Свойства** на панели инструментов *Операции с пользователями* или выбрав данное действие из контекстного меню.

9. Завершающей операцией по созданию учетной записи пользователя является назначение пароля (см. [«Назначение пароля»](#)). Назначение пароля предлагается после заполнения всех необходимых параметров в окне создания учетной записи и нажатия кнопки **Сохранить**.

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

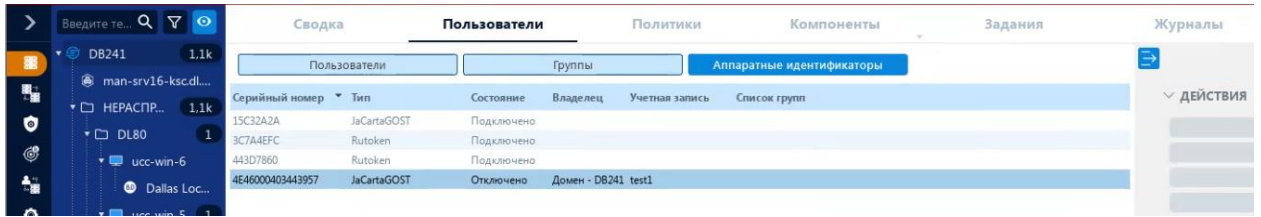
5.2.4 Параметры аппаратного идентификатора

Категория **Аппаратные идентификаторы** на уровне ДБ содержит список аппаратных идентификаторов подключенных к ДБ (рис. 84).

Рабочая область категории **Аппаратные идентификаторы** представляет собой таблицу с полями:

1. «Серийный номер» — содержит информацию о серийном номере идентификатора;
2. «Тип» — содержит информацию, о том какой тип данный идентификатор;
3. «Состояние» — показывает статус подключения АИ в режиме реального времени. Допустимые значения:
 - Подключено – отображается, если идентификатор подключен;
 - Не подключено – отображается, если идентификатор не подключен, но назначен пользователю.
4. «Владелец» — указывает на каком уровне дерева **ЕЦУ Dallas Lock** была создана группа пользователей;

5. «Учетная запись» — имя пользователя, которому назначен АИ. Допустимые значения:
 - Если АИ назначен, то пользователю отображается *Имя пользователя*;
 - Не определено.
6. «Список групп» — название групп, в которые включена учетная запись пользователя.



Сводка						
Пользователи						
Пользователи Группы Аппаратные идентификаторы						
Серийный номер	Тип	Состояние	Владелец	Учетная запись	Список групп	
15C32A2A	JaCartaGOST	Подключено				
3C7A4EFC	Rutoken	Подключено				
443D7860	Rutoken	Подключено				
4E46000403443957	JaCartaGOST	Отключено	Домен - DB241	test1		

Рис. 84. Список аппаратных идентификаторов



По умолчанию подключенные аппаратные идентификаторы отображаются выше в списке, чем не подключенные.

Для применения изменений аппаратного идентификатора, на модулях необходима синхронизация. В категории **Аппаратные идентификаторы** на вкладке *Пользователи* доступно только:

- Назначить/Снять назначение;
- Форматировать;
- Сохранить отчет;
- Сменить PIN-код;
- Перейти к учетной записи.

На панели управления в блоке *Фильтры* предусмотрена возможность фильтрации аппаратных идентификаторов в соответствии с выбранными параметрами и категориями.

Просмотр и настройка параметров аппаратного идентификатора доступны:

- по двойному щелчку левой кнопкой мыши по АИ в списке;
- при выборе пункта **Свойства** из контекстного меню, вызванного щелчком правой кнопки мыши на группе в списке;

5.2.5 Назначение аппаратного идентификатора

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



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

Для назначения аппаратного идентификатора пользователю необходимо:

1. Открыть окно **Редактирование полей пользователя**.
2. Выбрать вкладку *Общие*.
3. Дважды щелкнуть левой кнопкой мыши по параметру **Аппаратный идентификатор**.
4. Откроется окно **Назначение аппаратного идентификатора** (рис. 85).

Назначение аппаратного идентификатора пользователю "admin"

Предъявленные идентификаторы: 0 Подключиться к удаленному АРМ

Идентификатор: Апп.идентификатор не выбран ⓘ

Тип:

Серийный номер:

Метка:

Пользователь:

☐ Пароль хранится в идентификаторе ☐ Пароль защищен PIN кодом

Назначение авторизационных данных: Записать Очистить

Действия с идентификатором: Смена PIN кода... Форматировать

Применить Отмена

Рис. 85. Окно назначения аппаратного идентификатора

5. Предъявить аппаратный идентификатор, вставив его в соответствующий USB-порт или прикоснувшись к считывателю (в зависимости от типа идентификатора).
6. В строке состояния *Предъявленные идентификаторы* будет указано количество предъявленных в данный момент идентификаторов, а в списке выпадающего меню *Идентификатор* появятся их наименования.
7. Выбрать необходимый идентификатор из списка.
8. Далее в полях с параметрами АИ появятся: тип, серийный номер, и для некоторых видов

идентификаторов станут доступны дополнительные функции (рис. 86). Кнопка ⓘ позволяет открыть окно с информацией о параметрах выбранного идентификатора.

Назначение аппаратного идентификатора пользователю "user"

Предъявленные идентификаторы: 1 Подключиться к удаленному АРМ

Идентификатор: Rutoken ⓘ

Тип:

Серийный номер:

Метка:

Пользователь:

☐ Пароль хранится в идентификаторе ☐ Пароль защищен PIN кодом

Назначение авторизационных данных: Записать Очистить

Действия с идентификатором: Смена PIN кода... Форматировать

Применить Отмена

Рис. 86. Параметры назначенного идентификатора

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

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



Если аппаратный идентификатор не поддерживается на модулях пользователя, то программа выводит соответствующее предупреждение.



При присвоении пользователю назначенного аппаратного идентификатора **ЕЦУ** выведет сообщение с предложением о переназначении идентификатора этому пользователю.



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

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

Назначение авторизационных данных

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

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

Для этого необходимо выполнить следующее:

- выбрать в выпадающем списке необходимый идентификатор;
- отметить флагом поле *Пароль хранится в идентификаторе*. Поле *Пароль защищен PIN-кодом* выделится автоматически. Далее нажать кнопку **Записать** (рис. 87);

Назначение аппаратного идентификатора пользователю "user"

Предъявленные идентификаторы: 1 Подключиться к удаленному АРМ

Идентификатор: Rutoken i

Тип: Rutoken

Серийный номер: 40DB7352

Метка: Rutoken

Пользователь:

☒ Пароль хранится в идентификаторе ☒ Пароль защищен PIN кодом

Назначение авторизационных данных Действия с идентификатором

Записать Очистить Смена PIN кода... Форматировать

Применить Отмена

Рис. 87. Запись авторизационной информации в идентификатор

- в появившемся окне ввести: PIN-код идентификатора и пароль пользователя с подтверждением (рис. 88), нажать **Применить**;

Рис. 88. Ввод дополнительной информации

- в окне параметров учетной записи системы защиты нажать **Применить** и **ОК**.

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

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

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

Для этого необходимо выполнить следующее:

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

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

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

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

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

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

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

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

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

Действия с идентификатором

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



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

Изменить пароль аппаратного идентификатора можно с помощью утилиты для идентификатора (скачать с сайта производителя), либо используя окно параметров назначенного пользователю идентификатора (рис. 86). Для этого в поле «Действия с идентификатором» необходимо выбрать кнопку **Смена PIN-кода** или кнопку **Форматировать**.

По нажатию кнопки **Смена PIN-кода** откроется окно, в котором необходимо ввести значения PIN-кода пользователя: старое (текущее) значение, новое значение и повтор нового значения. Дополнительные кнопки рядом с полями ввода позволяют изменить скрытые символы на явные, повтор ввода PIN-кода в этом случае не потребуется (рис. 89).

Рис. 89. Окно смены PIN-кода

Для форматирования аппаратного идентификатора нажать **Форматировать** откроется окно (рис. 90), в котором необходимо заполнить следующие поля:

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

Ввести новые данные:

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

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



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

Рис. 90. Окно форматирования идентификатора



Для аппаратных идентификаторов Рутокен:

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

Снятие аппаратной идентификации

Для того, чтобы снять назначение аппаратного идентификатора для учетной записи отдельного пользователя, необходимо в окне параметров учетной записи в поле *Идентификатор* (рис. 86) выбрать значение *Аппаратный идентификатор не назначен*, нажать **Применить** и **ОК**.

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

5.2.6 Удаленная регистрация аппаратных идентификаторов

В **ЕЦУ** реализована возможность удаленной регистрации аппаратных идентификаторов для модулей **СЗИ Dallas Lock 8.0** и **Dallas Lock Linux**. Данная функциональная возможность полезна в распределенных сетях, когда нет возможности физически привезти аппаратный идентификатор к ТС, на котором расположена консоль **ЕЦУ**.

Для того, чтобы подключиться к удаленному АРМ, необходимо:

1. Нажать кнопку **Подключиться к удаленному АРМ** (рис. 91).

Назначение аппаратного идентификатора пользователю "secServer"

Предъявленные идентификаторы: 0

Идентификатор: Апп.идентификатор не выбран

Тип:

Серийный номер:

Метка:

Пользователь:

☐ Пароль хранится в идентификаторе ☐ Пароль защищен PIN кодом

Назначение авторизационных данных: Записать, Очистить

Действия с идентификатором: Смена PIN кода..., Форматировать

Подключиться к удаленному АРМ

Применить, Отмена

Рис. 91. Окно назначения аппаратного идентификатора

2. После нажатия на кнопку **Подключиться к удаленному АРМ** открывается окно, отображающее дерево домена безопасности. В нем нужно выбрать АРМ, к которому будет произведено подключение. Поиск можно осуществлять вручную либо воспользоваться поисковой строкой вверху окна (рис. 92).

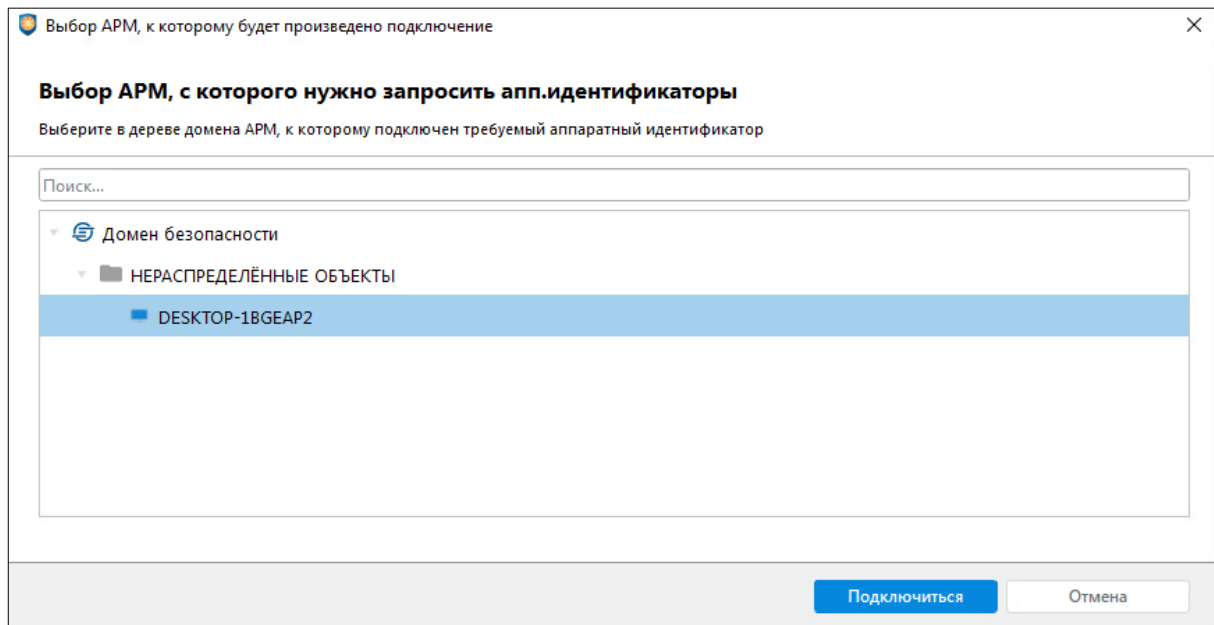


Рис. 92. Окно подключения, удаленного АРМ

- После подключения к удаленному АРМ откроется окно, имеющее вид аналогичный окну локального назначения аппаратного идентификатора. В окне отображается количество подключенных к удаленному АРМ аппаратных идентификаторов, а также имя АРМ, к которому было выполнено подключение (рис. 93).

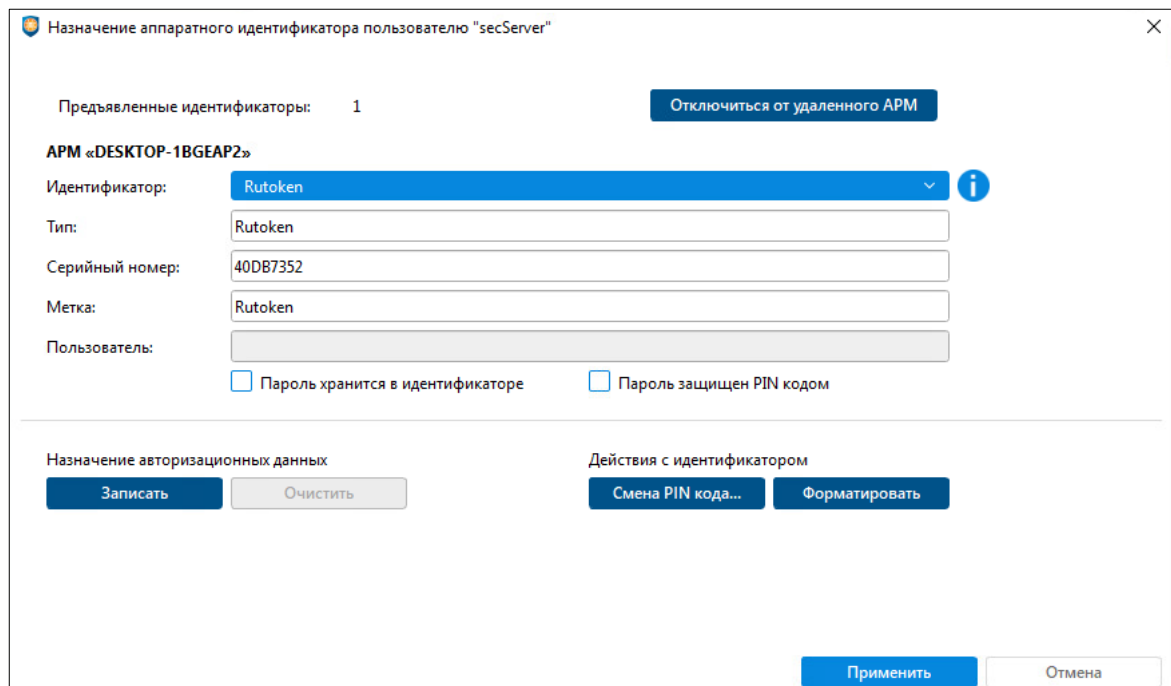


Рис. 93. Окно подключения, удаленного АРМ

Возможна регистрация только тех АИ, которые удовлетворяют политикам настроек АИ на АРМ, то есть должны быть включены соответствующие считыватели. Помимо этого, не должно быть противоречий с настройками доступа **СЗИ НСД Dallas Lock**.



При необходимости внести изменения на удаленный аппаратный идентификатор, который уже был назначен пользователю, требуется заново установить соединение с этим аппаратным идентификатором.

5.2.7 Удаление пользователей ДБ



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

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

5.2.8 Назначение пароля

Для назначения пароля пользователю необходимо выделить его имя в списке и нажать кнопку **Задать пароль**. Появится окно, где требуется ввести новый пароль и подтвердить его (рис. 94).

Рис. 94. 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 политик пароля»](#)).

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

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

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

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

5.2.9 Регистрация доменных пользователей в ДБ

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

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



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

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

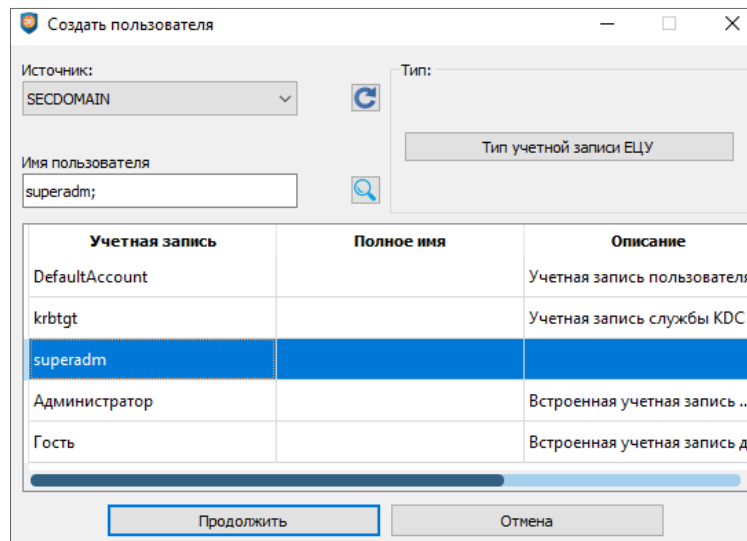
- «*nslookup <имя_домена>*» — убедиться, что выводится IP-адрес;
- «*nslookup <полученный ip-адрес>*» — убедиться, что выводится корректное FQDN-имя контроллера AD.



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

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

1. Убедиться, что Домен безопасности **ЕЦУ Dallas Lock** принадлежит домену (см. [«Менеджер доменов»](#)).
2. Получить список доменных пользователей. Для этого при создании пользователя в выпадающем списке поля *Источник* необходимо выбрать имя домена и нажать кнопку поиска  (рис. 95).



Учетная запись	Полное имя	Описание
DefaultAccount		Учетная запись пользователя
krbtgt		Учетная запись службы KDC
superadm		
Администратор		Встроенная учетная запись ..
Гость		Встроенная учетная запись д

Рис. 95. Заполнение учетной записи пользователя



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

Для получения списка учетных записей домена необходимо дополнительно ввести авторизационные данные администратора домена в появившемся окне (рис. 96).

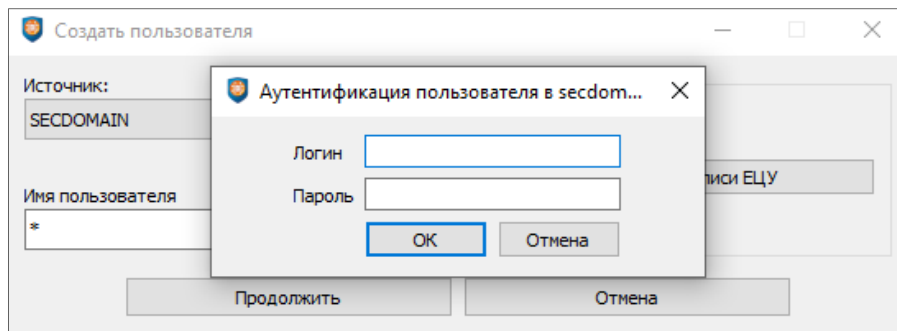


Рис. 96. Авторизационные данные администратора домена AD

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

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

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

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



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

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



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.

5.2.10 Регистрация доменных пользователей по маске в ДБ

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

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

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

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

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



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. 97).

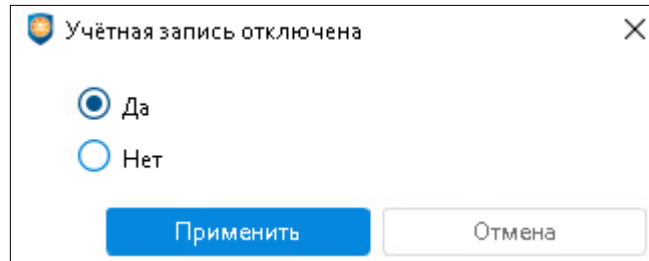


Рис. 97. Учетная запись отключена

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.



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.

5.2.11 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** → **Группы**. В окне Консоли **ЕЦУ** автоматически появляется ряд предварительно сконфигурированных групп в локальной ОС, в которые можно включать глобальных пользователей (рис. 98).



Рис. 98. Группы пользователей

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



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* 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. 99).

Рис. 99. Создание глобальной группы

5. В поле *Название группы* необходимо ввести название регистрируемой группы.



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.



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.

5.2.12 Удаление групп пользователей ДБ

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

5.3 Ролевая модель учетных записей ДБ

Настройки по правам администрирования в ДБ осуществляются в рабочей области для вкладки *Пользователи* в категории *Пользователи* в поле *Роль администрирования* (рис. 100).

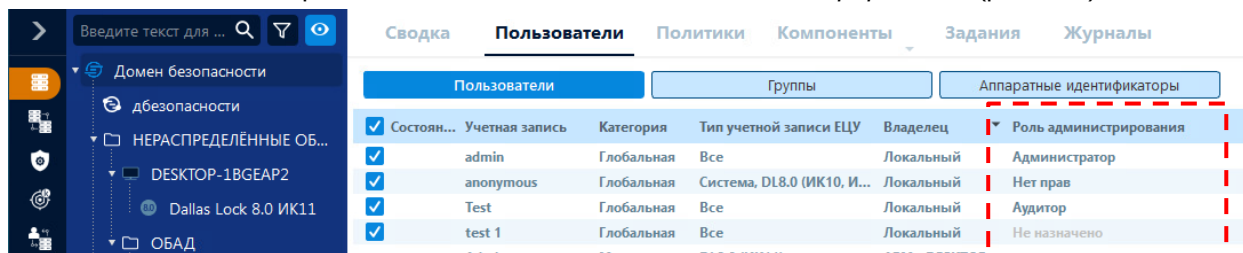


Рис. 100. Роль администрирования

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

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

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

По умолчанию новым пользователям назначается роль «Не назначено».

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

- роль не переопределена (значение «Не назначено»), то пользователь будет наследовать роль с более высокого уровня дерева ДБ;
- роль пользователя переопределена (значение отличное от «Не назначено»), то пользователь будет иметь на этом подчиненном уровне и уровнях ниже этого привилегии в соответствии с назначенной ролью.



Следует внимательно относиться к созданию и удалению назначений ролей пользователей на администрирование ДБ. Если на каком-либо из уровней Домена безопасности не останется ни одного пользователя с ролью «Администратор», доступ к настройкам на этом уровне будет ограничен 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 настройки¹³ (рис. 101).

¹³ Список политик может меняться в зависимости от версии клиента.

Сводка	Пользователи	Политики	Компоненты	Задания	Журналы
Политики паролей	Политики авторизации	Политики аудита	Права пользователей		
Политики контроля целостности	Режим работы СЗИ	Очистка остаточной информации	Политики ДСЧ		
Мандатный доступ	Политики доступа	Сеть	Аппаратная идентификация		

Запрет на изменение	Политика	Значение	Тип модуля
	ESXi: минимальное количество классов символов	Не используется	СЗИ ВИ (ИК4, ИК5, ИК6)
	ESXi: напоминать о смене пароля за	Не используется	СЗИ ВИ (ИК4, ИК5, ИК6)
	oVirt: Количество предыдущих паролей, которые пользователь не может использовать	5	СЗИ ВИ (ИК5, ИК6)
	oVirt: Максимальный срок действия пароля	25 нед. 5 дн.	СЗИ ВИ (ИК5, ИК6)
	oVirt: Минимальная длина пароля	6	СЗИ ВИ (ИК5, ИК6)
	oVirt: Минимальное количество прописных букв	Не используется	СЗИ ВИ (ИК5, ИК6)
	oVirt: Минимальное количество специальных символов	Не используется	СЗИ ВИ (ИК5, ИК6)
	oVirt: Минимальное количество строчных букв	Не используется	СЗИ ВИ (ИК5, ИК6)
	oVirt: Минимальное количество цифр	Не используется	СЗИ ВИ (ИК5, ИК6)
	oVirt: Напоминать о смене пароля за	1 дн.	СЗИ ВИ (ИК5, ИК6)
	vCenter: количество предыдущих паролей, которые пользователь не может использовать	5	СЗИ ВИ (ИК4, ИК5, ИК6)
	vCenter: максимальная длина пароля	20	СЗИ ВИ (ИК4, ИК5, ИК6)

Рис. 101. Вкладка Политики ДБ

Открыть редактор политики можно следующими способами:

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



Если в поле *Запрет на изменение* для политики определен закрытый замок красного цвета, то на данную политику установлен запрет на изменение, политика недоступна для редактирования, при этом на нижележащих уровнях ДБ автоматически установится флаг *Наследуется*, без возможности отключения данного состояния. Открытый зеленый замок обозначает отсутствие запрета на изменение для политики. Закрытый оранжевый замок используется только в заголовке столбца *Запрет на изменение* и устанавливается, если для политик в таблице определены разные значения параметра.

5.4.1 Настройка политик пароля

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.



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 10. Парольные политики

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: 6 символов.
При регистрации новой учетной записи и при изменении старого пароля в ЦУ СЗИ ВИ Dallas Lock контролируется длина вводимого пароля. Если число символов в пароле меньше установленного значения, то на экране появится предупреждение «Ввод пароля: введен слишком короткий пароль».
Следует иметь в виду, что если в процессе работы изменить значение длины пароля (например, увеличить), то у зарегистрированных учетных записей она останется прежней до первой смены пароля.
Политика применяется на модулях СЗИ ВИ Dallas Lock .

ESXi: 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 политика имеет значение: «*Не используется*».

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

vSphere: 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 и 5 дней (180 дней) и «*Не используется*» — максимальный срок действия пароля не установлен. По умолчанию политика имеет значение «180 дн.».

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

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 30 символов и «*Не используется*». По умолчанию политика имеет значение: 8 символов. 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.



При настройке политики для версий модулей, на которых значение политики было ограничено 14 символами, выставленное на **ЕЦУ** значение выше 14 при синхронизации будет заменено для данных модулей на 14. Подробную информацию о диапазоне значений политики можно найти в документации на используемый модуль.

Политика применяется на:

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

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 «*Не используется*».

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 максимального), то **СЗИ** проигнорирует значение минимального срока действия пароля.

Политика применяется на:

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

ESXi: 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 180 дней и «*Не используется*». По умолчанию политика имеет значение «*Не используется*». 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.



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 модулях **СЗИ ВИ Dallas Lock**.

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*».



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 вышеописанной опции количество символов указано 2, то при смене пароля «password1» на «password2» выведется сообщение «Пароль должен сильнее отличаться от предыдущего». Правильной будет смена пароля с «password1» на «Password2».

Политика применяется на модулях:

- **СЗИ Dallas Lock 8.0-K/C;**
- **СДЗ Dallas Lock;**
- **СДЗ УБ Dallas Lock;**
- **СЗИ ВИ Dallas Lock¹⁴.**

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 вышеописанная опция активирована, то при смене пароля на «password2» 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;**
 - **СДЗ УБ Dallas Lock;**
 - **СЗИ НСД Dallas Lock Linux;**
 - **СЗИ ВИ Dallas Lock.**

Необходимо наличие строчных и прописных букв

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

По умолчанию политика имеет значение «Нет».

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

Пример. У пользователя имеется пароль «password1», если вышеописанная опция активирована, то при смене пароля на «password1» выведется сообщение «В пароле должны содержаться и строчные, и прописные буквы». Правильной будет смена пароля с «password1» на «paCsword1».

Политика применяется на:

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

¹⁴ Список параметров может меняться в зависимости от версии клиента.

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 «passwordd» выведется сообщение «В пароле должны содержаться цифры». Правильной будет смена пароля с «password» на «password12».

Политика применяется на:

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

Необходимо отсутствие цифры в первом и последнем символах

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

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

По умолчанию политика имеет значение «Нет».

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

Пример. У пользователя имеется пароль «password», если описанная выше опция активирована, то при попытке смены пароля на «password1», «1password» или «1password1» выведется сообщение «Необходимо отсутствие цифры в первом и последнем символах». Правильной будет смена пароля с «password» на «passwordd».

Политика применяется на:

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

Разрешена генерация пароля

Если данная политика выключена (значение «Нет»), то пользователь не может сгенерировать случайный пароль, ему необходимо самому задавать пароль.

По умолчанию политика имеет значение «Да».

Политика применяется на модулях СДЗ Dallas Lock и СДЗ УБ Dallas Lock.

Разрешена генерация пароля

Если данная политика выключена (значение «Нет»), то пользователь не может сгенерировать случайный пароль, ему необходимо самому задавать пароль.

По умолчанию политика имеет значение «Нет».

Политика применяется на модулях СЗИ ВИ Dallas Lock ИК5.

vCenter: 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: «5».

Политика применяется на модулях СЗИ ВИ Dallas Lock.

vCenter: 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 40 символов и «*Не используется*». По умолчанию значение данной политики: «20».

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

vCenter: 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. По умолчанию значение данной политики: «3».

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

vCenter: минимальное количество прописных букв

Данной политикой устанавливается минимальное количество прописных (больших) букв, которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации в ЦУ **СЗИ ВИ Dallas Lock**.

Политика принимает значения от 1 до 9 символов и «*Не используется*». По умолчанию значение данной политики: «*Не используется*».

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

vCenter: минимальное количество символов алфавита

Данной политикой устанавливается минимальное количество символов алфавита, которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации в ЦУ **СЗИ ВИ Dallas Lock**.

Политика принимает значения от 1 до 15 символов и «*Не используется*». По умолчанию значение данной политики: «*Не используется*».

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

vCenter: минимальное количество специальных символов

Данной политикой устанавливается минимальное количество специальных символов (" ", "~", "!", "@", "#", "\$", "%", "^", "&", "*", "(", ")", "_", "-", "+", "{", "}", "[", "]", "\", "|", ":", ";", ":", ":", ":", "<", ">", "<", ">", "?", "/"), которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации в ЦУ **СЗИ ВИ Dallas Lock**.

Политика принимает значения от 1 до 9 символов и «*Не используется*». По умолчанию значение данной политики: «*Не используется*».

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

vCenter: минимальное количество строчных букв

Данной политикой устанавливается минимальное количество строчных (маленьких) букв, которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации в ЦУ **СЗИ ВИ Dallas Lock**.

Политика принимает значения от 1 до 9 символов и «*Не используется*». По умолчанию значение данной политики: «*Не используется*».

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

vCenter: минимальное количество цифр

Данной политикой устанавливается минимальное количество числовых символов, которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации в ЦУ **СЗИ ВИ Dallas Lock**.

Политика принимает значения от 1 до 9 символов и «*Не используется*». По умолчанию значение данной политики: «*Не используется*».

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

Напоминать о смене пароль 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 «<i>Не используется</i>». По умолчанию политика имеет значение «3 дня». Если выбрано значение «<i>Не используется</i>», 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. Политика применяется на: • службу ЕЦУ; • модулях: • СЗИ Dallas Lock 8.0-K/C; • СДЗ Dallas Lock; • СДЗ УБ Dallas Lock; • СЗИ НСД Dallas Lock Linux; • СЗИ ВИ Dallas Lock ИК4.
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 и 5 дней (180 дней) и «<i>Не используется</i>» — максимальный срок действия пароля не установлен. По умолчанию политика имеет значение «6 недель». Политика применяется на: • службу ЕЦУ; • модулях: • СЗИ Dallas Lock 8.0-K/C; • СДЗ Dallas Lock; • СДЗ УБ Dallas Lock; • СЗИ ВИ Dallas Lock; • СЗИ НСД Dallas Lock Linux.
oVirt: 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: «5». Политика применяется на модулях СЗИ ВИ Dallas Lock ИК5.
oVirt: 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 и 5 дней (180 дней) и «<i>Не используется</i>» — максимальный срок действия пароля не установлен. По умолчанию политика имеет значение «180 дн.». Политика применяется на модулях СЗИ ВИ Dallas Lock Linux ИК5.
oVirt: 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 30 символов и «Не используется». По умолчанию политика имеет значение: 6 символов. 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 модулях **СЗИ ВИ Dallas Lock Linux ИК5**.

oVirt: Минимальное количество прописных букв

Данной политикой устанавливается минимальное количество прописных (больших) букв, которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации в ЦУ **СЗИ ВИ Dallas Lock**.

Политика принимает значения от 1 до 9 символов и «Не используется». По умолчанию значение данной политики: «Не используется».

Политика применяется на модулях **СЗИ ВИ Dallas Lock ИК5**.

oVirt: Минимальное количество специальных символов

Данной политикой устанавливается минимальное количество специальных символов (" ", "~", "!", "@", "#", "\$", "%", "^", "&", "*", "(", ")", "_", "-", "+", "{", "}", "[", "]", "\", "|", ":", ";", ":", ":", ":", "<", ">", ":", ":", "?", "/"), которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации в ЦУ **СЗИ ВИ Dallas Lock**.

Политика принимает значения от 1 до 9 символов и «Не используется». По умолчанию значение данной политики: «Не используется».

Политика применяется на модулях **СЗИ ВИ Dallas Lock ИК5**.

oVirt: Минимальное количество строчных букв

Данной политикой устанавливается минимальное количество строчных (маленьких) букв, которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации в ЦУ **СЗИ ВИ Dallas Lock**.

Политика принимает значения от 1 до 9 символов и «Не используется». По умолчанию значение данной политики: «Не используется».

Политика применяется на модулях **СЗИ ВИ Dallas Lock ИК5**.

oVirt: Минимальное количество цифр

Данной политикой устанавливается минимальное количество числовых символов, которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации в ЦУ **СЗИ ВИ Dallas Lock**.

Политика принимает значения от 1 до 9 символов и «Не используется». По умолчанию значение данной политики: «Не используется».

Политика применяется на модулях **СЗИ ВИ Dallas Lock ИК5**.

oVirt: 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 180 дней и «Не используется». По умолчанию политика имеет значение «Не используется». 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.

Политика применяется на модулях **СЗИ ВИ Dallas Lock ИК5**.

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 11. Политики авторизации

KVM: Блокировать доступ к Cockpit Web Interface
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Да». Данная политика позволяет настроить разрешения входа на Web-клиент Cockpit Web Interface. Политика применяется на модулях СЗИ ВИ Dallas Lock .
KVM: Блокировать протокол SSH
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Да». Значение «Да» данной политики блокирует удаленный доступ к Серверу виртуализации по протоколу SSH. Политика применяется на модулях СЗИ ВИ Dallas Lock .
vCSA: Блокировать протокол SSH
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Политика контролирует удаленный доступ в vCSA по протоколу SSH. Политика применяется на модулях СЗИ ВИ Dallas Lock .
vCSA: Разрешить вход на Web-клиент vCSA Management Interface
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет настроить разрешение входа на Web-клиент VCSA Management Interface. Политика применяется на модулях СЗИ ВИ Dallas Lock .
vCSA: Разрешить локальный вход с консоли
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Да». Данная политика позволяет настроить разрешение локального входа с консоли. Политика применяется на модулях СЗИ ВИ 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 СЗИ ВИ Dallas Lock .
Автоматический выбор аппаратного идентификатора при авторизации
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Включение данной политики позволит автоматически выбрать подключенный аппаратный идентификатор при авторизации. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СДЗ Dallas Lock; • СДЗ УБ Dallas Lock; • СЗИ ВИ Dallas Lock.
Автоматическое блокирование неактивных учетных записей
Политика принимает значения от 1 до 90 дней и «Не используется». По умолчанию значение данной политики: «Не используется».

Данная политика позволяет настроить и выполнить автоматическую блокировку неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования. При активации данной политики на **ЕЦУ** выполняется блокировка неактивной учетной записи пользователей на отдельном модуле **СЗИ Dallas Lock 8.0-K/C**.

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

Блокировать компьютер в случае ввода неправильных паролей

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

Данная политика позволяет настроить блокирование компьютера в случае ввода пользователем неправильных паролей.

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

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»*.



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

Политика применяется на модулях:

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

Время блокировки учетной записи в случае ввода неправильных паролей

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

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

Возможное значение параметра: от 1 минуты до 5 часов и *«Не используется»*. Если выбрано значение *«Не используется»*, то разблокировать учетную запись может только администратор безопасности. По умолчанию значение данной политики: *«10 мин»*.

Политика применяется на:

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

Время ожидания авторизации пользователя

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

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

Политика применяется на модулях **СДЗ Dallas Lock** и **СДЗ УБ Dallas Lock**.

ESXi: Блокировать протокол SSH

Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет».
Если разрешено использование ESXi Shell, то его можно запустить непосредственно на гипервизоре ESXi через DCUI или удаленно по SSH. Данная политика блокирует такую возможность.

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

ESXi: 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.



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

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

ESXi: Время, в течение которого допускается выполнить одну попытку ввода пароля

Политика принимает значения от 1 мин. до 300 минут (5 часов). По умолчанию значение: *1 минута*.

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

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

ESXi: 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: *При удаленном подключении*.

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

ESXi: 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: «3».

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

ESXi: Период неиспользования

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

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

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

Hyper-V: Блокировать SC VMM

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

Данная политика позволяет заблокировать возможность подключиться к серверу VMM.

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

Запретить выход из спящего режима

Данная политика позволяет включить/выключить запрет выхода из спящего режима.

По умолчанию значение данной политики: «Нет».

Политика применяется на модулях **СДЗ УБ Dallas Lock**.

Запретить использование парольного интерфейса входа

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

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

Политика применяется на модулях:

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



Для назначения политики требуется, чтобы компьютер с модулем был введен под управление домена: Active Directory, FreeIPA, ALD PRO, Ред АДМ, Samba.

Запретить повторное использование имени пользователя в течение

Политика принимает значения 1-10 лет, 15 лет, 20 лет, 25 лет, 30 лет, 40 лет, 50 лет, «Навсегда» 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-K/C**.

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**;
- **СЗИ ВИ Dallas Lock**.

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-K/C**.

Максимальное количество ошибок 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: «5».

Политика применяется на:

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

Максимальное количество сессий

Данная политика устанавливает максимальное количество активных сессий на данном ПК. Возможные значения от 1 до 20 сессий и «*Не используется*» — означает, что параметр будет отключен. По умолчанию установлено значение «10».

Политика применяется на модулях **СЗИ НСД Dallas Lock Linux**.

Общее: Включить синхронизацию времени по NTP

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

Данная политика позволяет использовать NTP-сервера из заданного списка для синхронизации времени между сервером УД и агентами **СЗИ ВИ**.

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

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**;
- **СДЗ УБ Dallas Lock**;
- **СЗИ ВИ Dallas Lock**.

Отображать информацию о последнем успешном входе

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

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

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

При значении «*Нет*» — информация не отображается.

Политика применяется на модулях:

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

Принудительное завершение работы по расписанию (Linux)

Данная политика позволяет включить/выключить принудительное завершение работы пользователя по расписанию.

По умолчанию значение данной политики: «*Выкл.*».

Политика применяется на модулях **СЗИ НСД Dallas Lock Linux**.

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, FreeIPA, ALD PRO, Ред АДМ, Samba, для работы с которым настроено **СЗИ НСД Dallas Lock Linux**, пока не зарегистрированные в **СЗИ НСД Dallas Lock Linux**, будут регистрироваться в нем по мере прохождения процесса авторизации в **СЗИ НСД Dallas Lock Linux**.

Политика применяется на модулях **СЗИ НСД Dallas Lock Linux**.

Разрешить использование смарт-карт

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

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

Политика применяется на модулях:

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

vCenter: время, в течение которого подсчитываются ошибки ввода пароля

Политика принимает значения от 1 минуты до 4 часов 59 минут. По умолчанию значение данной политики: *1 минута*.

Данная политика позволяет установить количество времени, в течение которого подсчитываются ошибки ввода пароля на модуле **СЗИ ВИ Dallas Lock**. Если за данный период времени количество неудачных попыток входа достигнет максимального количества ошибок ввода пароля, учетная запись будет заблокирована на время, заданное в политике **Время блокировки учетной записи в случае ввода неправильных паролей**.

В случае, если за установленное время количество неудачных попыток входа не достигло заданного максимального количества ошибок ввода пароля — счетчик неудачных попыток обнуляется.

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

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** и **СДЗ УБ Dallas Lock**.

Текст сообщения при входе

В окне редактирования данной политики имеется возможность проставить флаг *Выводить сообщение при входе*, ввести заголовок и текст предупреждения, которое будет отображаться пользователю до входа в ОС. Смысл данного текста должен предупреждать о реализации мер по обеспечению безопасности информации, и о необходимости соблюдения установленных правил обработки информации. Нажатие **ОК** пользователем будут означать подтверждение ознакомления.

По умолчанию данная политика не используется.

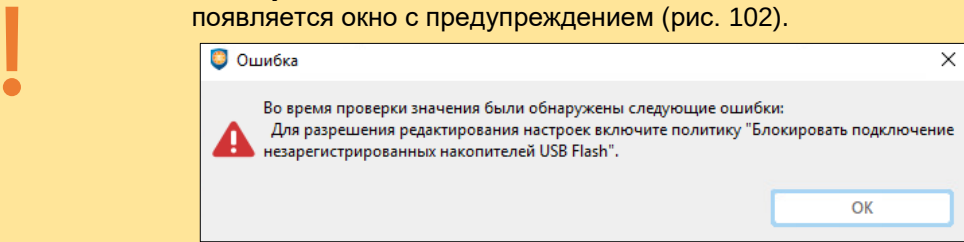
Политика применяется на модулях **СЗИ Dallas Lock 8.0-K/C**.

5.4.3 Настройка политик аудита

На вкладке *Политики* в категории **Политики аудита** 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 12. Политики аудита

Аудит USB-накопителей	
Возможное значение политики: «Не используется», «Зарегистрированные USB-накопители», «Незарегистрированные USB-накопители», «Все USB-накопители». По умолчанию значение данной политики: «Не используется». Данная политика позволяет вести регистрацию событий, связанных с подключаемыми USB-устройствами.	
При попытке изменить значение политики на отличное от «Не используется» проверяется значение политики Блокировать подключение незарегистрированных накопителей USB Flash: - если установлено значение «Да», то изменение производится успешно; - если установлено значение «Нет», то изменения не вносятся, появляется окно с предупреждением (рис. 102).	
	
Рис. 102. Ошибка редактирования политики	
Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C .	
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-K/C; СЗИ ВИ Dallas Lock.	
Аудит событий зачистки	
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Включение данной политики позволяет регистрировать на модуле события зачистки остаточной информации в следующих случаях: - при включенных параметрах зачистки остаточной информации в СЗИ модуля; - при зачистке остаточной информации на модуле по запросу пользователя; - при зачистке накопителя на модуле. Политика применяется на модулях: СЗИ Dallas Lock 8.0-K/C; СЗИ ВИ Dallas Lock.	
Аудит устройств	
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.». Включение данной политики позволяет регистрировать события по доступу к подключаемым на модуле устройствам в Журнале ресурсов (при условии, что журнал ресурсов включен). Сами события настраиваются непосредственно в консоли администрирования СЗИ модуля в окне редактирования параметров дескриптора устройства (класса устройств). Политика применяется на модулях: СЗИ Dallas Lock 8.0-K/C; СЗИ ВИ Dallas Lock.	

Выгрузка журналов

Настройка данной политики в дополнительном окне позволяет:

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

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

По умолчанию политика имеет значение «*Выкл.*»

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

Журнал МЭ

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

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

Политика применяется на модулях **СЗИ ВИ Dallas Lock**.

Журнал аутентификации

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

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

Политика применяется на модулях **Агент ЕЦУ Linux**.

Журнал безопасности

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

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

Политика применяется на модулях **Агент ЕЦУ Windows**.

Журнал доступа к устройствам

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

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

Политика применяется на модулях **СЗИ НСД Dallas Lock Linux**.

Журнал запуска/завершения процессов

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

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

Политика применяется на модулях:

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

Журнал пакетов МЭ

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

Включение журнала позволяет протоколировать в нем информацию о входящих/исходящих пакетах МЭ.

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

Журнал печати Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.». Включение журнала позволяет протолировать 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-K/C; • СЗИ НСД Dallas Lock Linux; • Агент ЕЦУ Dallas Lock Linux.
Журнал пользовательских сообщений Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Вкл.». Включение журнала (значение «Вкл.») позволяет протолировать на модуле в журнале события пользовательских сообщений. Политика применяется на модулях Агент ЕЦУ Linux.
Журнал приложений Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Вкл.». В данном журнале фиксируются события об активности приложений, их целостности и набора загружаемых ими компонентов. Политика применяется на модулях Агент ЕЦУ Windows.
Журнал ресурсов Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Включение журнала позволяет протолировать 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-K/C; • СЗИ НСД Dallas Lock Linux; • СЗИ ВИ Dallas Lock.
Журнал соединений МЭ Настройка данной политики в дополнительном окне позволяет: • указать перечень приложений, для которых будет применяться правило; • указать направление передачи, набор портов; • указать расписание и пользователей. Включение журнала позволяет протолировать в нем информацию о соединениях МЭ. По умолчанию политика имеет значение «Выкл.» Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Журнал гипервизора Hyper-V Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить регистрацию событий, происходящих на гипервизоре Hyper-V. Политика применяется на модулях СЗИ ВИ Dallas Lock.

Журнал трафика фильтрации МЭ
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Включение журнала позволяет протоколировать в нем информацию о трафике фильтрации МЭ. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
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 НСД Dallas Lock Linux; • СЗИ ВИ Dallas Lock.
Журнал управления пользователями и группами
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Журнал содержит события, связанные с настройками, созданием и удалением учетных записей пользователей, групп учетных записей. Включение политики (значение «Вкл.») позволяет протоколировать в журнале данные события. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ НСД Dallas Lock Linux; • СЗИ ВИ Dallas Lock.
Журнал установок
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.». В данном журнале фиксируются события, связанные с инсталляцией обновлений Windows, дополнительных приложений. Политика применяется на модулях Агент ЕЦУ Windows.
Заблокировать выгрузку журналов syslog в SQL
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Значение «Да» данной политики позволяет блокировать выгрузку журналов syslog в SQL для предотвращения передачи служебных данных. Политика применяется на модулях СЗИ ВИ Dallas Lock.
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-K/C; • СЗИ ВИ Dallas Lock.
Заносить в журнал ошибки ОС
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-K/C; • СЗИ ВИ Dallas Lock.
Заносить в журнал события запуска и остановки ОС Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Да». Включение данной политики (значение «Да») позволяет регистрировать на модуле события, связанные с запуском/завершением работы ОС, события запуска/остановки ядра защиты СЗИ Dallas Lock, в журнале управления политиками (при условии, что данный журнал включен). Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Заносить в журнал события запуска и остановки модулей администрирования DL Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Да». Включение данной политики (значение «Да») позволяет регистрировать события, связанные с запуском/завершением работы модулей администрирования СЗИ Dallas Lock в журнале управления политиками (при условии, что данный журнал включен). Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Использовать часы платы СДЗ Dallas Lock Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Включение данной политики (значение «Да») позволяет использовать время из часов СДЗ Dallas Lock. Политика применяется только при установленной на АРМ аппаратной плате. Для работы политики необходимо в ОС модуля установить драйвер для СДЗ. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Максимальное количество записей в журналах Настройка данной политики позволяет установить максимальное количество записей в определенном журнале модуля. Политика может принимать значение «Не используется» или «1000–20 000». По умолчанию в данной политике для каждого журнала задано значение 20 000 записей. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Максимальное количество записей в журналах Настройка данной политики позволяет установить максимальное количество записей в определенном журнале модуля. Политика может принимать значение «Не используется» или «10 000–100 000». По умолчанию в данной политике для каждого журнала задано значение 100 000 записей, выставлен чекбокс <i>Не используется</i>. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
vSphere: ESXi Shell Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить на гипервизоре vSphere регистрацию событий и записей всех введенных команд в ESXi Shell. Политика применяется на модулях СЗИ ВИ Dallas Lock.

vSphere: USB-устройства Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию событий, связанных с подключаемыми USB-устройствами к гипервизору vSphere. Политика применяется на модулях СЗИ ВИ Dallas Lock.
vSphere: Агент ESXi Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию сведений о действиях агента, который управляет и конфигурирует гипервизор vSphere виртуальные машины, а также включить регистрацию событий аутентификации на гипервизоре vSphere. Политика применяется на модулях СЗИ ВИ Dallas Lock.
vSphere: Аутентификация Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию событий, связанных с аутентификацией на гипервизоре. Политика применяется на модулях СЗИ ВИ Dallas Lock.
vSphere: Виртуальные машины Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию событий, связанных с виртуальными машинами и гипервизорами. Политика применяется на модулях СЗИ ВИ Dallas Lock.
vSphere: Зачистка ФС Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию событий, связанных с зачисткой файловой системы гипервизора vSphere. Политика применяется на модулях СЗИ ВИ Dallas Lock.
vSphere: Системные события Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») на гипервизоре vSphere регистрацию общих сообщений журнала (Syslog), которые могут быть использованы для устранения неполадок. Политика применяется на модулях СЗИ ВИ Dallas Lock.
Объем журнала в Мб (100-10000) Политика устанавливает ограничения объема журналов в диапазоне от 100/Мб до 10000/Мб для архивации. По умолчанию политике установлено значение «2800 Мб». Политика применяется на модулях СЗИ НСД Dallas Lock Linux.
Периодическая архивация журнала Границы возможного временного интервала архивации варьируются от 1 часа до 1 года. По умолчанию политике задано значение «Не используется». Включение данной политики позволяет управлять периодами автоматической архивации журналов. После настройки данной политики все журналы по расписанию архивируются, все записи из них сохраняются в файл в системной папке на АРМ с установленным СЗИ Dallas Lock 8.0 «C:\DLLOCK80\Logs», записи журналов очищаются, и они начинают вестись заново. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.

Путь к архивам журналов Возможное значение политики: «<i>Не используется</i>» / «<i>[путь к архивам]</i>». Путь к архиву журналов пишется в одну строку, отделяя каждую папку знаком «/», значение по умолчанию: «<i>/var/log/dll_archive/</i>». Включение данной политики позволяет фиксировать путь к архивам журналов. Политика применяется на модулях СЗИ НСД Dallas Lock Linux.
Системный журнал Возможное значение политики: «<i>Вкл./Выкл.</i>». Значение по умолчанию: «<i>Вкл.</i>». Включение данной политики (значение «<i>Вкл.</i>») позволяет протолировать на модуле в журнале события системного журнала операционной системы (SysLog). Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ НСД Dallas Lock Linux; • Агент ЕЦУ Windows.
Служебный журнал МЭ (пакеты в формате Pcap) Возможное значение политики: «<i>Вкл./Выкл.</i>». Значение по умолчанию: «<i>Выкл.</i>». Включение данной политики позволяет вести учет заблокированных пакетов в формате Pcap. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Собирать только указанные события Возможное значение политики: «<i>Не используется</i>» / «<i>[код события]</i>». Значение по умолчанию: «<i>[код события]</i>». Включение данной политики позволяет фиксировать только те события, коды которых указаны в списке событий. Политика применяется на модулях Агент ЕЦУ Windows.
Собирать только указанные уровни сообщений Возможное значение политики: «<i>Не используется</i>» / «<i>[код события]</i>». Список правил отбора пишется в одну строку, элементы списка разделяются запятыми, значение по умолчанию: «<i>Не используется</i>». Включение данной политики позволяет фиксировать только те события, коды которых указаны в списке событий. Политика применяется на модулях Агент ЕЦУ Linux.
Создавать теньевые копии распечатываемых документов Возможное значение политики: «<i>Да/Нет</i>». По умолчанию значение данной политики: «<i>Нет</i>». Данная политика позволяет включить (значение «<i>Да</i>») сохранение копий распечатываемых документов в отдельную папку на модуле по пути «<i>C:\DLLOCK80\Logs\PrintCopy</i>». В данной папке при каждой печати будут создаваться подпапки с файлами, названия которых состоят из времени печати и имени печатающего устройства. Политика применяется на модулях СЗИ Dallas Lock 8.0.
Срок хранения журналов в месяцах Данная политика позволяет управлять сроком хранения журналов на модулях. По истечению заданного в политике срока, формируется архив, и журналы начинают заполняться новыми данными. Политика принимает значения от 1 до 6 месяцев. По умолчанию для данной политики установлено значение 3 месяца. Политика применяется на модулях СЗИ НСД Dallas Lock Linux.
Уведомления: Журнал событий ВИ Hyper-V (операции VMM) Возможное значение политики: «<i>Да/Нет</i>». По умолчанию значение данной политики: «<i>Нет</i>». Данная политика позволяет включить (значение «<i>Да</i>») регистрацию событий, связанных с управлением хостами, кластерами и облачным сервисом виртуальной инфраструктуры Hyper-V.

Политика применяется на модулях СЗИ ВИ Dallas Lock.
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 Nureg-V. Политика применяется на модулях СЗИ ВИ Dallas Lock.
Уведомления: События управления конфигурацией ВМ
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию событий, связанных с управлением конфигурацией ВМ. Политика применяется на модулях СЗИ ВИ Dallas Lock.
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 Nureg-V. Политика применяется на модулях СЗИ ВИ Dallas Lock.
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 Nureg-V. Политика применяется на модулях СЗИ ВИ Dallas Lock.
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 Nureg-V. Политика применяется на модулях СЗИ ВИ Dallas Lock.
Управление хранилищем теневых копий отчуждаемой информации
По умолчанию значение данной политики «Не используется». Настройка данной политики позволяет: • задать размер хранилища теневых копий (по умолчанию – 150 Мбайт); • задать время жизни теневой копии (по умолчанию 1 месяц); • включить автоматическую перезапись при переполнении хранилища. Политика применяется на модуле СЗИ Dallas Lock 8.0-K/C.
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. ! При значении политики «Да» возникает риск использования информации, содержащейся в столбце <i>Неверный пароль</i>, 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; • СДЗ УБ Dallas Lock; • СЗИ ВИ Dallas Lock.

vSphere: Агент CB vCenter
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет включить (значение «Да») регистрацию сведений о действиях агента, который управляет и конфигурирует гипервизор vSphere виртуальные машины, а также включить регистрацию событий аутентификации на гипервизоре vSphere. Политика применяется на модулях СЗИ ВИ Dallas Lock.
Журнал трафика COB
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Включение журнала позволяет фиксировать проходящий сетевой трафик через контролируемые COB узлы сети. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Заблокировать выгрузку журналов в SQL
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Значение «Да» данной политики позволяет блокировать выгрузку журналов в SQL для предотвращения передачи служебных данных. Политика применяется на модулях СЗИ ВИ Dallas Lock.
Уведомления: Изменение общих настроек сервера виртуализации
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данный параметр позволяет включить регистрацию событий, связанных изменением настроек сервера виртуализации. Политика применяется на модулях СЗИ ВИ Dallas Lock.
Уведомления: Операции с виртуальными машинами
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данный параметр позволяет включить регистрацию событий, связанных виртуальными машинами. Политика применяется на модулях СЗИ ВИ Dallas Lock.
Уведомления: Операции с виртуальными дисками
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данный параметр позволяет включить регистрацию событий, связанных виртуальными дисками. Политика применяется на модулях СЗИ ВИ Dallas Lock.
Уведомления: Операции с объектами виртуальной сети
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данный параметр позволяет включить регистрацию событий, связанных с объектами виртуальной сети. Политика применяется на модулях СЗИ ВИ Dallas Lock.
Уведомления: Операции о снапшотами
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данный параметр позволяет включить регистрацию событий, связанных с созданием снапшотов. Политика применяется на модулях СЗИ ВИ Dallas Lock.
Уведомления: События управления VM
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данный параметр позволяет включить регистрацию событий, связанных с управлением VM. Политика применяется на модулях СЗИ ВИ Dallas Lock.

Фоновое выполнение резервного копирования

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

Включение данного параметра (значение «Вкл.») позволяет понизить для задач резервного копирования приоритет выполнения потоков, обрабатывающих задачи резервного копирования.

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

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.



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

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.

При 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 13. 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-K/C .
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-K/C .
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-K/C .
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-K/C .
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-K/C; • СЗИ ВД Dallas Lock.

Изменение системного времени и часового пояса
С помощью данной политики можно запретить пользователям устройств, входящих в состав ДБ, изменять установленные дату и время. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Интерактивный вход: Запрещен
С помощью данной политики возможно запретить возможность интерактивного входа определенным пользователям и группам в ОС. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Интерактивный вход: Разрешен
С помощью данной политики возможно разрешить возможность интерактивного входа определенным пользователям и группам в ОС. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.
Параметры безопасности: Просмотр
С помощью данной политики можно дать право определенным пользователям или группам на просмотр установленных параметров аудита (в том числе журналов) и доступа. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Параметры безопасности: Управление
С помощью данной политики можно дать определенным пользователям или группам полномочия на управление параметрами безопасности. Если пользователю (группе пользователей) разрешено изменение параметров безопасности, то он может делегировать все свои полномочия другим пользователям с учетом действия контроля за распространением полномочий (см. выше). Если пользователю предоставлено право на управление параметрами безопасности, то право на просмотр установленных настроек предоставляется автоматически. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Печать запрещена
С помощью данной политики можно гибко настроить список учетных записей, которым запрещена печать с данного компьютера. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Печать разрешена
С помощью данной политики можно гибко настроить список учетных записей, которым разрешена печать с данного компьютера. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
Принудительное завершение работы по расписанию
Данная политика позволяет настроить список учетных записей и групп, для которых согласно настройке «<i>Расписание работы</i>» по окончании времени работы ПК пользователя будет заблокирован. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-К/С; • СЗИ ВИ Dallas Lock.

Ресурсы: Управление дискреционным доступом
С помощью данной политики можно назначить учетные записи пользователей для управления дискреционным доступом. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C .
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-K/C .
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-K/C .
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-K/C; • СЗИ ВИ Dallas Lock.
Удаленный вход: Разрешен
С помощью данной политики возможно разрешить возможность удаленного входа определенным пользователям и группам в ОС. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Учетные записи: Принудительная двухфакторная аутентификация
Если в значении данной политики стоит определенная учетная запись или группа, то при регистрации новой учетной записи (в составе данной группы или индивидуально) или редактировании в СЗИ присвоение идентификатора будет обязательным, иначе будет выведено предупреждение об ошибке. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Учетные записи: Управление
Если в значении данной политики стоит учетная запись или группа, то она обладает полномочиями по созданию, удалению и изменению учетных записей пользователей в системе защиты. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C .

5.4.5 Настройка политик контроля целостности

На вкладке *Политики* в категории **Политики контроля целостности** настраиваются параметры проверки целостности отдельно для:

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

По умолчанию проверка целостности установлена только при загрузке модуля.

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

- установить режим проверки (при загрузке, периодичный контроль или контроль по расписанию);
- указать алгоритм расчета контрольной суммы (CRC32, хэш ГОСТ Р34.11-94 или хэш MD5).



Политики контроля целостности программно-аппаратной среды являются общими для модулей **СЗИ Dallas Lock 8.0 К/С** и **СЗИ ВИ Dallas Lock**, но алгоритм расчета контрольной суммы «Хэш ГОСТ Р 34.11-94» не будет работать для модулей **СЗИ ВИ Dallas Lock ИК4**.



Если для проверки объектов программно-аппаратной среды не выбран алгоритм расчета контрольной суммы, то проверка целостности для данного типа объектов выполняться не будет.

Автоматический выбор алгоритма расчета контрольной суммы по умолчанию не предусмотрен.

Таблица 14. Политики контроля целостности

Генерация событий аудита аппаратной целостности
Возможное значение политики: «<i>Да/Нет</i>». По умолчанию значение данной политики: «<i>Нет</i>». Включение данной политики (значение «<i>Да</i>») позволяет отслеживать события нарушения аппаратной целостности. Политика применяется на модулях СЗИ НСД Dallas Lock Linux.
Изменение файлов с назначенным контролем целостности
Данная политика позволяет управлять возможностью изменения файлов с назначенным контролем целостности. Политика может принимать одно из значений: • «Разрешить» — при нарушении целостности СЗИ не блокирует доступ к объекту, для которого назначен контроль целостности; • «Запретить» — при нарушении целостности СЗИ блокирует доступ к объекту, для которого назначен контроль целостности; • «Проверять цифровую подпись исполняемых файлов» — осуществляется проверка электронной подписи для исполняемых файлов (список расширений файлов можно дополнить). По умолчанию значение данной политики: «<i>Разрешить</i>». Политика применяется на модулях СЗИ ВИ Dallas Lock.
Изменение файлов с назначенным контролем целостности
Возможное значение политики «<i>Разрешить</i>»/«<i>Запретить</i>». Значение по умолчанию: «<i>Разрешить</i>». Данная политика позволяет контролировать возможность пользователя изменять файлы с назначенным контролем целостности. При значении «<i>Разрешить</i>» при нарушении целостности СЗИ не блокирует доступ к объекту, для которого назначен контроль целостности. При значении «<i>Запретить</i>» при нарушении целостности СЗИ блокирует доступ к объекту, для которого назначен контроль целостности. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С.
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; • СЗИ ВИ Dallas Lock.

Контроль прогр. апп. среды по расписанию

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

По умолчанию данная политика не используется.

Политика применяется на модулях:

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

Контроль реестра по расписанию

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

По умолчанию данная политика не используется.

Политика применяется на модулях:

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

Контроль целостности прогр. апп. среды: BIOS

Данная политика позволяет включить контроль изменений параметров BIOS.

По умолчанию данная политика выключена.

Политика применяется на модулях:

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

Контроль целостности прогр. апп. среды: USB-устройства

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

По умолчанию данная политика выключена.

Политика применяется на модулях:

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

Контроль целостности прогр. апп. среды: Диски

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

По умолчанию данная политика выключена.

Политика применяется на модулях:

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

Контроль целостности прогр. апп. среды: Драйверы

Данная политика управляет контролем целостности установки и удаления драйверов.

По умолчанию данная политика выключена.

Политика применяется на модулях:

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

Контроль целостности прогр. апп. среды: Кодеки

Данная политика управляет контролем установки или удаления кодеков на ПК.

По умолчанию данная политика выключена.

Политика применяется на модулях:

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

Контроль целостности прогр. апп. среды: Операционная система

Данная политика управляет контролем изменений свойств ОС данного ПК: изменений имени, IP-адреса и пр.

По умолчанию данная политика выключена.

Политика применяется на модулях:

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

Контроль целостности прогр. апп. среды: Папки общего доступа

Данная политика управляет контролем создания или удаления папок общего доступа на данном ПК.

По умолчанию данная политика выключена.

Политика применяется на модулях:

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

Контроль целостности прогр. апп. среды: Принтеры

Данная политика управляет контролем списка всех установленных на ПК принтеров, факсов, МФУ и др. печатающих устройств.

По умолчанию данная политика выключена.

Политика применяется на модулях:

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

Контроль целостности прогр. апп. среды: Программы

Данная политика управляет контролем установки или удаления программ на данном ПК.

По умолчанию данная политика выключена.

Политика применяется на модулях:

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

Контроль целостности прогр. апп. среды: Разделы диска

Данная политика управляет контролем изменений разделов жесткого диска, форматирований диска, подключений новых дисков.

По умолчанию данная политика выключена.

Политика применяется на модулях:

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

Контроль целостности прогр. апп. среды: Сеть

Данная политика управляет контролем сетевых подключений и сетевых карт.

По умолчанию данная политика выключена.

Политика применяется на модулях:

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

Контроль целостности прогр. апп. среды: Система

Данная политика позволяет включить контроль портов, мониторов, шин, звуковых устройств и других системных устройств.

По умолчанию данная политика выключена.

Политика применяется на модулях:

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

Контроль целостности прогр. апп. среды: Список пользователей
Данная политика управляет контролем списка пользователей, созданных в локальной ОС. По умолчанию данная политика выключена. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Контроль целостности прогр. апп. среды: Устройства ввода
Данная политика управляет контролем подключенных устройств ввода на данном ПК: клавиатуры, мыши. По умолчанию данная политика выключена. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Контроль целостности файлов по изменению
Данная политика позволяет выполнять контроль целостности при изменении контролируемых объектов ФС — вычисление контрольной суммы и сравнение с эталоном. По умолчанию данная политика включена. Политика применяется на модулях СЗИ НСД Dallas Lock Linux.
Периодический контроль ФС
Политика принимает значения от 1 минуты до 5 часов и «<i>Не используется</i>». По умолчанию значение данной политики: «<i>Не используется</i>». Данная политика позволяет включить периодический контроль файловой системы и настроить периодичность проверки. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ НСД Dallas Lock Linux; • СЗИ ВИ Dallas Lock.
Периодический контроль прогр. апп. среды
Политика принимает значения от 1 минуты до 5 часов и «<i>Не используется</i>». По умолчанию значение данной политики: «<i>Не используется</i>». Данная политика позволяет включить периодический контроль программно-аппаратной среды и настроить периодичность проверки. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Периодический контроль реестра
Политика принимает значения от 1 минуты до 5 часов и «<i>Не используется</i>». По умолчанию значение данной политики: «<i>Не используется</i>». Данная политика позволяет включить периодический контроль реестра Windows и настроить периодичность проверки. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Проверка цифровой подписи исполняемых файлов
Возможное значение политики: «<i>Вкл./Выкл.</i>». Значение по умолчанию: «<i>Выкл.</i>». Данная политика позволяет определять необходимость проверки цифровой подписи исполняемых файлов. При значении «<i>Вкл.</i>» необходимо указать расширения исполняемых файлов для проверки цифровой подписи.

Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C .
Проверять целостность ФС при загрузке ОС
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Вкл.». Данная политика позволяет управлять включением/отключением автоматической проверки целостности файловой системы при загрузке ОС. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ НСД Dallas Lock Linux; • СЗИ ВИ Dallas Lock.
Проверять целостность прогр. апп. среды при загрузке ОС
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.». Данная политика позволяет управлять включением/отключением автоматической проверки программно-аппаратной целостности при загрузке ОС. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ НСД Dallas Lock Linux; • СЗИ ВИ Dallas Lock.
Проверять целостность реестра при загрузке ОС
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Вкл.». Данная политика позволяет управлять включением/отключением автоматической проверки целостности реестра Windows при загрузке ОС. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Виртуальная машина: Контроль целостности по расписанию
Данная политика позволяет включить контроль целостности виртуальной машины по расписанию и настроить расписание контроля. По умолчанию данная политика не используется. Политика применяется на модулях СЗИ ВИ Dallas Lock.
Виртуальная машина: Периодически проверять целостность дисков
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 целостности дисков и настроить периодичность проверки. Политика применяется на модулях СЗИ ВИ Dallas Lock.
Виртуальная машина: Периодический контроль целостности
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 целостности и настроить периодичность проверки. Политика применяется на модулях СЗИ ВИ Dallas Lock.
Виртуальная машина: Проверять целостность дисков по расписанию
Данная политика позволяет включить контроль целостности дисков по расписанию и настроить расписание контроля. По умолчанию данная политика «Не используется». Политика применяется на модулях СЗИ ВИ Dallas Lock.

Виртуальная машина: Проверять целостность при загрузке ОС
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Включение данной политики (значение «Да») позволяет проверять целостность при загрузке ОС. Политика применяется на модулях СЗИ ВИ Dallas Lock .
Ресурсы: Контроль целостности по расписанию
Данная политика позволяет включить контроль целостности по расписанию и настроить расписание контроля. По умолчанию данная политика не используется. Политика применяется на модулях СЗИ ВИ Dallas Lock .
Ресурсы: Периодический контроль целостности
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 целостности и настроить периодичность проверки. Политика применяется на модулях СЗИ ВИ Dallas Lock .
Ресурсы: Проверять целостность при загрузке ОС
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Включение данной политики (значение «Да») позволяет проверять целостность при загрузке ОС. Политика применяется на модулях СЗИ ВИ Dallas Lock .

5.4.6 Настройка политик режима работы СЗИ

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

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

Таблица 15. Политики режима работы СЗИ

Неактивный режим
С помощью данной политики можно управлять включением/выключением Неактивного режима СЗИ в СЗИ Dallas Lock 8.0 , а также произвести гибкую (точечную) настройку неактивного режима. В окне настройки находится чекбокс <i>Неактивный режим включен</i> и список функций СЗИ , для которых доступна блокировка. Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С .
Неактивный режим СЗИ ВИ Dallas Lock
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.». Данная политика позволяет управлять включением/выключением Неактивного режима СЗИ в СЗИ ВИ Dallas Lock . Политика применяется на модулях СЗИ ВИ Dallas Lock .
Система обнаружения вторжений
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Вкл.». Данная политика позволяет управлять включением/выключением модуля Система обнаружения вторжений СЗИ Dallas Lock 8.0 . Политика применяется на модулях СЗИ Dallas Lock 8.0-К/С .

5.4.7 Настройка политик очистки остаточной информации

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

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

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

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

Таблица 16. 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-K/C; • СЗИ ВИ Dallas Lock.
Количество циклов затирания
Политика Количество циклов затирания позволяет выбрать от одного до четырех циклов затирания информации на модуле. Значение по умолчанию: «1». Установленное количество циклов затирания используется при всех установленных видах очистки остаточной информации: по команде администратора, в автоматическом режиме, и при зачистке накопителя. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Очищать освобождаемое дисковое пространство
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Включение данной политики (значение «Да») позволяет автоматически затирать всю остаточную информацию при освобождении областей на дисках, то есть при удалении файлов или при уменьшении размеров файлов на модуле. Затирание производится записью маскирующей последовательности (политика Затирающая последовательность) поверх освобождаемого пространства заданным количеством циклов затирания (политика Количество циклов затирания). Включение данного параметра может заметно снизить скорость выполнения файловых операций, особенно при количестве циклов затирания больше единицы. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ ВИ Dallas Lock.
Очищать данные в конфиденциальных сеансах доступа
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 освобожденное дисковое пространство**.

Политика применяется на модулях **СЗИ Dallas Lock 8.0-С**.

Очищать файл подкачки виртуальной памяти

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

Включение данной политики (значение «Да») позволяет автоматически затирать всю остаточную информацию в файле подкачки Windows на модуле. Затирание производится записью маскирующей последовательности поверх файла подкачки. Очистка производится при завершении работы (закрытии файла подкачки) и, если очистка была прервана, при старте системы (открытии файла подкачки).

Политика применяется на модулях:

- **СЗИ Dallas Lock 8.0-К/С;**
- **СЗИ ВД Dallas Lock.**

Проверять очистку информации

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

Если данная политика включена, то после проведения очистки объектов ФС на модуле, дополнительно выполняется проверка того, что очистка действительно осуществлена. В том случае, если проверка выявила, что очистка не осуществлена или завершена с ошибкой, то в журнал ресурсов модуля заносится соответствующее событие.

Проверка осуществляется при очистке остаточной информации, выполняемой по команде администратора, в автоматическом режиме, и при зачистке накопителя целиком (функция «Зачистка диска»).

Политика применяется на модулях:

- **СЗИ Dallas Lock 8.0-К/С;**
- **СЗИ ВД Dallas Lock.**

5.4.8 Настройка политик ДСЧ

На вкладке *Политики* в категории **Политики ДСЧ** настраиваются параметры работы датчика случайных чисел для модулей **СДЗ Dallas Lock**.



Категория политик **Политики ДСЧ** не применима для вариантов исполнения **СДЗ Dallas Lock** ПФНА.26.20.40.140.001-04 и ПФНА.26.20.40.140.001-05 (платы **СДЗ Dallas Lock** формата USB «КТ-600-PLS» и USB «КТ-600-Type A»).

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

Таблица 17. Политики ДСЧ

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-С** 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 18. Политики мандатного доступа

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-С.
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.



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-С**.

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-С**.

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**.

Добавлять штамп при печати под уровнями

Настройка данного параметра в дополнительном окне позволяет выбрать уровни мандатного доступа пользователей, при работе под которыми на распечатываемые документы будет добавляться штамп.

Политика применяется на модулях **СЗИ Dallas Lock 8.0-С ИК11**.

Разрешить печать из-под уровней доступа

Настройка данного параметра в дополнительном окне позволяет выбрать уровни мандатного доступа, работая под которыми, пользователи могут осуществлять печать документов.

Политика применяется на модулях **СЗИ Dallas Lock 8.0-С ИК11**.

5.4.10 Настройка политик доступа

На вкладке *Политики* в категории **Политики доступа** 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 19. 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.
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; • СЗИ ВИ Dallas Lock.

Блокировать компьютер при подключении незарегистрированных накопителей USB Flash

Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Данная политика позволяет блокировать ПК при подключении незарегистрированных USB-Flash накопителей.

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

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.

При попытке изменить значение политики на «Нет» проверяется значение политики **Аудит USB-накопителей**:

- если установлено значение «Не используется», то изменение производится успешно;
- если установлено значение, отличное от «Не используется», то изменения не вносятся, появляется окно с предупреждением (рис. 103).

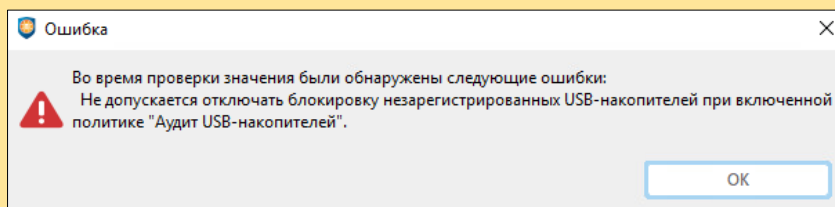


Рис. 103. Ошибка редактирования политики

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

Блокировать файл-диски при отключении аппаратного идентификатора

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

Если при создании файл-диска помимо пароля используется аппаратный идентификатор, то при отключении идентификатора от ПК, файл-диск также будет отключен. Стоит учитывать, что при изменении настроек аппаратного идентификатора необходимо начать новый сеанс работы пользователя для выполнения корректной блокировки. Политика не распространяется на идентификаторы, предъявляемые по касанию.

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

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.



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-K/C**.

Время ожидания подключения по VNC (секунд)

Политика позволяет установить время ожидания удаленного подключения к рабочему столу компьютера по сети. Возможные значения параметра от 5 до 600 секунд. Значение

по умолчанию: «120».

По истечении установленного времени запрос прерывается.



При инициировании подключения по VNC консоль ЕЦУ блокируется до момента подключения/отказа в подключении.

Политика применяется на модулях **Агент ЕЦУ Windows**.

Исключения для приложений

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

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

Список исключений:

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

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

По умолчанию значение — «Не используется».

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

Принудительное завершение сеанса пользователя при отключении аппаратного идентификатора

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

Данная политика завершает сеанс при отключении аппаратного идентификатора.

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 20. 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-K/C**.

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:

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

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

5.5 Межсетевой экран

После настройки системы управления, необходимо произвести настройку межсетевого экрана. Под настройкой межсетевого экрана понимается установка значений политик для межсетевого экрана, удовлетворяющих политикам безопасности организации.

Более подробно о межсетевом экране в Руководстве по эксплуатации **СЗИ Dallas Lock 8.0** глава 15, в Руководстве по эксплуатации **Dallas Lock Linux** раздел 4.12 и в Руководстве по эксплуатации **СЗИ ВИ Dallas Lock** глава 8.

Для перехода к разделу настроек **Управление компонентом МЭ** необходимо на вкладке *Компоненты* выбрать *Межсетевой экран*. На странице **Управление компонентом МЭ** можно редактировать параметры политик на уровне всего ДБ, после синхронизации на всех подчиненных объектах в ДБ применяются установленные настройки (рис. 104).

Сводка	Пользователи	Политики	Компоненты	Задания	Журналы
Управление компонентом МЭ					
Настройки МЭ		Правила МЭ Dallas Lock 8.0			
Политика					
Аварийный режим: Автоматическая активация при нарушении КЦ МЭ		Выкл.		СЗИ ВИ (ИК6)	
Аварийный режим: Автоматическая активация при недоступности Агента ВИ со ст		Выкл.		СЗИ ВИ (ИК6)	
Аварийный режим: Автоматическая активация при провале самотестирования		Выкл.		СЗИ ВИ (ИК6)	
Аварийный режим: Запрет внешнего трафика к гипервизору/CB		Выкл.		СЗИ ВИ (ИК6)	
Аварийный режим: Запрет трафика между Агентом ВИ и ЦУ		Выкл.		СЗИ ВИ (ИК6)	
Аварийный режим: Запрет трафика между ВМ		Выкл.		СЗИ ВИ (ИК6)	
Белый и черный списки приложений		Выкл.		DLL (ИК4, ИК5)	
Блокировать протокол QUIC		Да		DL8.0 (ИК11, ИК12)	
Блокировка адресов		10 срабатываний в течении 60 минут		DLL (ИК4, ИК5)	
Включить уведомление в трей при блокировке соединения		Да		DL8.0 (ИК11, ИК12)	
Включить фильтрацию		Нет		DL8.0 (ИК11, ИК12)	
Доверенные правила МЭ		Вкл.		DL8.0 (ИК11, ИК12)	

Межсетевой экран

Система контроля накопителей

Контроль ресурсов

Система обнаружения вторжений

Безопасная среда COB (песочница)

Средство обнаружения и реагирования

Рис. 104. Вкладка «Межсетевой экран»

Открыть редактор политики можно следующими способами:

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

5.5.1 Настройка политик МЭ

Настройки, касающиеся значений политик МЭ, регулируются в категории **Настройки МЭ** на вкладке **Компоненты** → **Межсетевой экран**.

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

Таблица 21. Настройки МЭ

Аварийный режим: Автоматическая активация при нарушении КЦ МЭ
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.».
Если данная политика включена, то при нарушении контроля целостности автоматически сработает аварийный режим.
Политика применяется на модулях СЗИ ВИ Dallas Lock .
Аварийный режим: Автоматическая активация при недоступности Агента ВИ со стороны ЦУ
Возможное значение политики: «5 минут», «10 минут», «30 минут», «1 час», «1 день» и «Не используется». По умолчанию значение данной политики: «Не используется».
Данная политика позволяет управлять автоматической активацией аварийного режима при потере связи с Агентом ВИ со стороны Центра управления СЗИ ВИ Dallas Lock .
Политика применяется на модулях СЗИ ВИ Dallas Lock .
Аварийный режим: Автоматическая активация при провале самотестирования
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.».
Если данная политика включена, то при провале самотестирования сработает аварийный режим.
Политика применяется на модулях СЗИ ВИ Dallas Lock .
Аварийный режим: Запрет внешнего трафика к гипервизору/СВ
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.».
Данная политика позволяет управлять запретом всех входящих и исходящих соединений между гипервизором/СВ и внешними сетями (Интернетом).
Политика применяется на модулях СЗИ ВИ Dallas Lock .
Аварийный режим: Запрет трафика между Агентом ВИ и ЦУ
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.».
Данная политика позволяет управлять запретом всех входящих и исходящих соединений между Агентом ВИ и Ядром ЦУ СЗИ ВИ .
Политика применяется на модулях СЗИ ВИ Dallas Lock .
Аварийный режим: Запрет трафика между ВМ
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.».
Данная политика позволяет управлять запретом входящих и исходящих соединений между виртуальными интерфейсами ВМ в пределах виртуальной сети.
Политика применяется на модулях СЗИ ВИ Dallas Lock .
Белый и черный списки приложений
Данная политика используется для включения/выключения белого и черного списков приложений. Одновременно включить и чёрный, и белый список невозможно. Значение по умолчанию «Выключить белый и черный списки». Доступные значения: «Включить белый список», «Включить черный список».
Политика применяется на модулях СЗИ НСД Dallas Lock Linux .

Блокировать протокол QUIC
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». При включении данной политики МЭ блокирует протокол QUIC. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Блокировка адресов
Политика позволяет осуществить блокировку адресов при установленном количестве срабатываний правил межсетевого экрана в течении установленного периода времени. Принимает значение количества срабатываний: от 2 до 10; принимает значение срабатываний правил МЭ: от 5 до 60 минут. По умолчанию политика осуществляет блокировку адресов при 10 срабатываниях правил МЭ в течение 60 минут. Политика применяется на модулях СЗИ НСД Dallas Lock Linux.
Включать уведомление в трей при блокировке соединения
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Если включить данную политику при блокировке соединения будут приходить уведомления. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Включить фильтрацию
Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Да». Включение данной политики включает фильтрацию SSL(TLS) трафика. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Доверенные правила МЭ
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.». Включение данной политики разрешает использование доверенных правил МЭ. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Использовать безопасный веб-серфинг
Данная политика используется для настройки безопасного веб-серфинга. По умолчанию данная политика не используется. В ней можно произвести установить, что делать с вредоносным ПО, контентом для взрослых и фишингом (блокировать, журналировать, отключить). Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Максимальный размер http-заголовка
Политика позволяет установить максимальный размер http-заголовка. Возможные значения параметра от 128 до 16384. Значение по умолчанию: «2048». Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Межсетевой экран
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.». Включение данной политики включает работу МЭ. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ НСД Dallas Lock Linux; • СЗИ ВД Dallas Lock.
Отключать GZIP для анализа HTTP трафика
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Вкл.». Выключение данной политики разрешает использовать GZIP для анализа HTTP трафика. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.

Отключать локальные правила МЭ при автопереключении профиля МЭ Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Да». Выключение данной политики разрешает использовать локальные правила МЭ при автопереключении профиля МЭ. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Отображать сообщение о заблокированном соединении (сайте) Возможное значение политики: «Да/Нет». По умолчанию значение данной политики: «Нет». Включение данной политики разрешает уведомления о том, что данный сайт заблокирован. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Периодичность проверки защищенности системы Данная политика используется для настройки периодической проверки защищенности системы. Периодичность проверки по умолчанию 1 раз в час. Доступные значения от 10 мин до 1 дня. Также можно настроить оповещение об отсутствии обновлений для таких объектов, как ОС (по умолчанию 20 дней), антивирусы и сетевые сигнатуры (по умолчанию 20 дней). Для ОС и сетевых сигнатур доступные значения от 1 до 60 дней. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Протоколирование событий МЭ Данная политика используется для настройки протоколирования событий МЭ. По умолчанию в этой политике выбраны все элементы. Для того чтобы выбрать события необходимо зайти в окно протоколируемых событий и выбрать из детерминированного списка (установка параметров неактивного режима, изменение настроек МЭ и пр.) Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Протоколирование событий МЭ Данная политика используется для настройки протоколирования событий МЭ. По умолчанию в этой политике выбраны все элементы. Для того чтобы выбрать события необходимо зайти в окно протоколируемых событий и выбрать из детерминированного списка (установка параметров неактивного режима, изменение настроек МЭ и пр.) Политика применяется на модулях СЗИ НСД Dallas Lock Linux.
Режим обучения МЭ Данная политика используется для настройки режима обучения МЭ. Значение по умолчанию: «Выключено». В окне настройки политики можно выбрать автоматический или интерактивный режим обучения. Для автоматического необходимо настроить период обучения, время и дату окончания обучения, а также режим после обучения: пропускать или запрещать пакеты. Кроме того, в этом окне настраивается максимальное количество портов в одном правиле (10-100), максимальное количество адресов в одном правиле (5-100) и максимальное количество создаваемых правил (10-1000). Если в КУ ЕЦУ ввести меньшее значение в поле ввода, то при сохранении значение не сохранится, а вернется к исходному. Если это сделать на клиенте DL8.0, то поле примет минимально возможное значение (с максимальным значением поведение аналогично). Для интерактивного режима необходимо выбрать действие по умолчанию для соединения: разрешать или блокировать соединение. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.
Режим работы фильтрации Данная политика используется для настройки режима работы фильтрации. По умолчанию в этой политике ничего не выбрано. Доступные значения: «Фильтровать все, кроме исключений», «Фильтрация активна только для хостов-исключений». Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.

Сохранять локальные правила МЭ при синхронизации с ЕЦУ

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

Выключение данной политики отключает сохранение локальных правил МЭ при синхронизации с ЕЦУ.

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

Список перехватываемых исходящих портов

Политика позволяет управлять списком исходящих портов, работа с которыми будет фильтроваться. Значение по умолчанию: «80,8080,3128,443».

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

Уведомления по событиям отсутствия антивируса и обновлений ОС и DL

Данная политика используется для определения места, куда будут приходить уведомления по событиям отсутствия антивируса и обновлений ОС и DL. Значение по умолчанию: «Уведомление в журнал». Доступные значения: «Уведомление в системный tray», «Уведомление в ЕЦУ», «Уведомление в журнал».

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

Фильтрация SSL

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

Включение данной политики включает фильтрацию SSL.

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

Частота регистрации события НСД 'Нарушение правила МЭ'

Возможное значение политики: «5 минут», «10 минут», «15 минут», «30 минут», «1 час» и «1 день». По умолчанию значение данной политики: «5 минут».

Данная политика позволяет задавать диапазон, в течение которого должно срабатывать событие НСД. Действует на запрещающие правила.

Политика применяется на модулях **СЗИ ВД Dallas Lock**.

5.5.2 Настройка правил МЭ СЗИ Dallas Lock

На вкладке *Межсетевой экран* в категории **Правила МЭ Dallas Lock 8.0** производится настройка правил МЭ для модулей **СЗИ Dallas Lock 8.0-К/С** (рис. 105).

Управление компонентом МЭ

Настройки МЭ **Правила МЭ Dallas Lock 8.0** Правила МЭ Dallas Lock Linux

№	Имя правила	Направление передачи	Тип правила	Параметры протоколов
1	DNS клиент	Любое	TCP/UDP-правило	Локальные TCP-порты: Все; Внешние TC
2	ARP	Любое	ARP-правило	IP-адрес отправителя: Все; IP-адрес полу
3	DHCP клиент	Любое	TCP/UDP-правило	Локальные TCP-порты: Все; Внешние TC
4	HTTP/HTTPS клиент	Исходящие пакеты	TCP/UDP-правило	Локальные TCP-порты: Все; Внешние TC
5	Internet Explorer HTTP/HTTPS	Любое	TCP/UDP-правило	Локальные TCP-порты: Все; Внешние TC
6	IGMP	Любое	IGMP-правило	Отсутствуют; Локальный IP-адрес: Все; Е
7	yandex.ru	Исходящие пакеты	IP-правило	Локальный IP-адрес: Все; Внешний IP-адр
8	Внешние сетевые папки	Любое	TCP/UDP-правило	Локальные TCP-порты: Все; Внешние TC
9	Локальные сетевые папки	Любое	TCP/UDP-правило	Локальные TCP-порты: 139,445,135; Внел
10	DL удаленное управление (входящее)	Исходящие пакеты	TCP/UDP-правило	Локальные TCP-порты: 17490; Внешние TC
11	DL удаленное управление (исходящее)	Исходящие пакеты	TCP/UDP-правило	Локальные TCP-порты: Все; Внешние TC
12	DL проверка доступности клиентов (ICMP ping)	Любое	ICMP-правило	ICMP-сообщения: 0,8; Локальный IP-адр
13	DL СБ (входящее)	Входящие пакеты	TCP/UDP-правило	Локальные TCP-порты: 17490,17491,1749
14	DL СБ (исходящее)	Исходящие пакеты	TCP/UDP-правило	Локальные TCP-порты: Все; Внешние TC
15	DL СЛ (входящее)	Входящие пакеты	TCP/UDP-правило	Локальные TCP-порты: 17498,17499; Внел
16	Dallas Lock ECU	Любое	TCP/UDP-правило	Локальные TCP-порты: 17490,17900,1790
17	ICMP по умолчанию (исходящее)	Исходящие пакеты	ICMP-правило	ICMP-сообщения: 3,8,10; Локальный IP-
18	ICMPv6 по умолчанию (исходящее)	Исходящие пакеты	ICMPv6-правило	ICMP-сообщения: 1,141,142,136; Локаль
19	ICMP по умолчанию (входящее)	Входящие пакеты	ICMP-правило	ICMP-сообщения: 3,8,10,11; Локальный
20	ICMPv6 по умолчанию (входящее)	Входящие пакеты	ICMPv6-правило	ICMP-сообщения: 3,133,135,129,136; Лок
21	MSRPC	Любое	TCP/UDP-правило	Локальные TCP-порты: 135; Внешние TC
22	LDAP	Любое	TCP/UDP-правило	Локальные TCP-порты: 389; Внешние TC

✓ По умолчанию Действие с пакетами, не попавшими ни под од... Любое

ДЕЙСТВИЯ

- Создать
- Редактировать
- Удалить
- Активировать
- Деактивировать
- Копировать
- Увеличить приоритет
- Уменьшить приоритет
- Сохранить
- Загрузить
- Скрыть столбцы таблицы

ОПЕРАТИВНОЕ УПРАВЛЕНИЕ

- Синхронизировать

Рис. 105. Категория «Правила МЭ Dallas Lock 8.0»

Необходимо настроить все правила, расположенные в списке правил МЭ, в соответствии с требованиями политики безопасности организации.

В этой категории можно создавать, редактировать, удалять, активировать, деактивировать, копировать, повысить или понизить приоритет, сохранять и загружать правила МЭ. Также можно скрывать отображение некоторых столбцов настройки правил.

По умолчанию пропускаются все пакеты. Но в окне дан список основных правил МЭ, которые находятся в деактивированном состоянии.

Список предустановленных деактивированных правил МЭ:

- DNS клиент;
- ARP;
- DHCP клиент;
- HTTP /HTTPS клиент;
- Internet Explorer HTTP /HTTPS;
- IGMP;
- yandex.ru;
- Внешние сетевые папки;
- Локальные сетевые папки;
- DL удаленное управление (входящее);
- DL удаленное управление (исходящее);
- DL проверка доступности клиентов (ICMP ping);
- DL СБ (входящее);
- DL СБ (исходящее);
- DL СЛ (входящее);
- ICMP по умолчанию (исходящее);
- ICMPv6 по умолчанию (исходящее);
- ICMP по умолчанию (входящее);
- ICMPv6 по умолчанию (входящее);
- MSRPC;
- LDAP.

Список правил МЭ для модулей **СЗИ Dallas Lock 8.0** на уровне ДБ представляет собой таблицу с полями:

1. «№» — столбец с идентификационным номером строки правила и с индикатором активности правила. Поле № принимает следующий вид:

 — разрешающее правило активно;

 — запрещающее правило активно;

 — запрещающее или разрешающее правило неактивно.

2. «Имя правила» — заданное АИБ произвольное имя правила МЭ при создании.
3. «Направление передачи» — отображается направление сетевого трафика, для которого действует правило.
4. «Тип правила» — отображается тип протокола, на основании которого осуществляется фильтрация сетевых пакетов.
5. Основные данные по ресурсам и пользователям, для которых они назначены: маски пути, пользователи, уровень доступа и т.д.

Для применения изменений списка учетных записей на модулях необходима синхронизация.

В категории **Правила МЭ Dallas Lock 8.0** можно назначить действия, которые будут выполняться с пакетами, не попавшими ни под одно правило (пропускать или запрещать пакеты). Также можно указать, куда будут приходить уведомления о действиях с такими пакетами: «Уведомление в системный tray», «Уведомление в ЕЦУ», «Уведомление в журнал пакетов».

5.5.3 Настройка правил МЭ Dallas Lock Linux

На вкладке *Межсетевой экран* в категории **Правила МЭ Dallas Lock Linux** производится настройка правил МЭ для модулей **СЗИ НСД Dallas Lock Linux** (рис. 106).

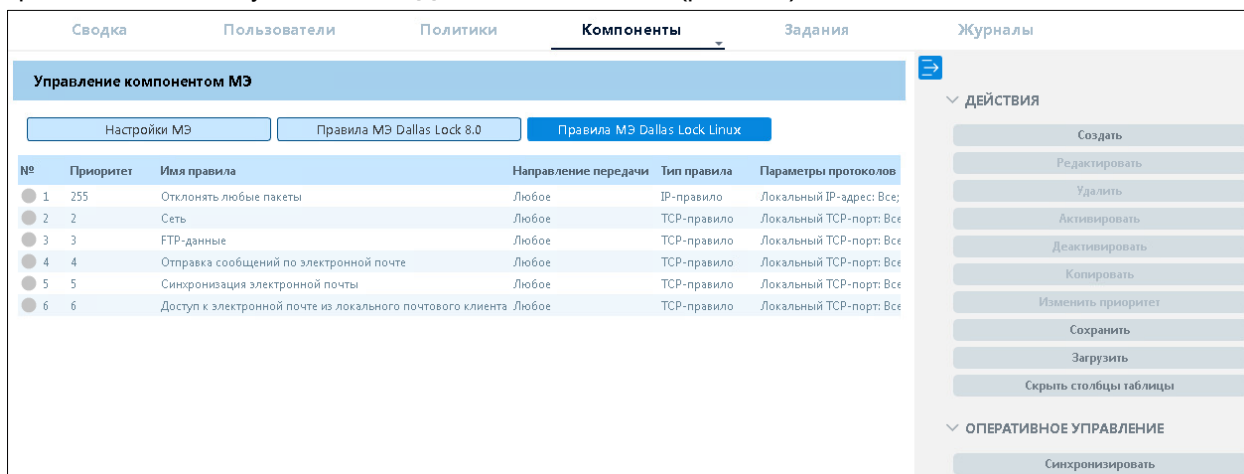


Рис. 106. Категория «Правила МЭ Dallas Lock Linux»

Необходимо настроить все правила, расположенные в списке правил МЭ, в соответствии с требованиями политики безопасности организации.

Список предустановленных деактивированных правил МЭ:

- Сеть;
- FTP-данные;
- Отправка сообщений по электронной почте;
- Синхронизация электронной почты;
- Доступ к электронной почте из локального почтового клиента;
- Отклонять любые пакеты.

Список правил МЭ для модулей **СЗИ НСД Dallas Lock Linux** на уровне ДБ представляет собой таблицу с полями:

1. «№» — столбец с идентификационным номером строки правила и с индикатором активности правила. Поле № принимает следующий вид:

- ✓ — разрешающее правило активно;
- ✗ — запрещающее правило активно;
- — запрещающее или разрешающее правило неактивно.

2. «Приоритет» — столбец с номером приоритета правила.
3. «Имя правила» — заданное АИБ произвольное имя правила МЭ при создании.
4. «Направление передачи» — отображается направление сетевого трафика, для которого действует правило.
5. «Тип правила» — отображается тип сетевого или транспортного протокола, на основании которого осуществляется фильтрация сетевых пакетов.
6. «Профиль Safe Mode» — столбец содержит информацию о состоянии (включена/выключена), добавлено ли правило в профиль «Safe Mode».



Правила, созданные на **ЕЦУ** с включенным модулем «Safe Mode», не могут быть удалены пользователем на модуле **СЗИ НСД Dallas Lock Linux**. Для удаления правила МЭ на модуле, администратору необходимо отключить данный параметр на **ЕЦУ**.



Не рекомендуется удалять все правила из профиля «*Safe Mode*», поскольку он необходим для корректной обработки трафика в случае критического сбоя работы МЭ.

7. Основные данные по ресурсам: фильтрация, аудит, автоблокировка и т.д.

Для применения изменений списка учетных записей на модулях необходима синхронизация.

В этой категории можно создавать, редактировать, удалять, активировать, деактивировать, копировать, повысить или понизить приоритет, сохранять и загружать правила МЭ. Также можно скрывать отображение некоторых столбцов настройки правил.

Реализована возможность экспорта правил МЭ в файл по кнопке **Сохранить** (рис. 107). После нажатия **Сохранить**, в появившемся окне, нужно указать путь для сохранения отчета с данными из таблицы с правилами МЭ. Файл сохраняется в формате *.fwconf.

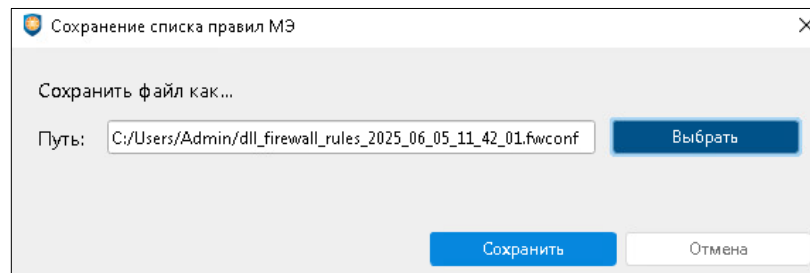


Рис. 107. Экспорт правил МЭ в файл

Для применения правил МЭ на модулях необходимо на панели действий нажать кнопку **Загрузить**.

В появившемся окне, необходимо указать путь к файлу, для этого нужно:

- нажать кнопку **Выбрать**;
- найти и выбрать сохраненный ранее файл правил МЭ;
- нажать кнопку **Применить**.



Применение правил МЭ из конфигурационного файла приведет к удалению всех текущих правил МЭ.

5.5.4 Создание правил МЭ

Для создания нового правила МЭ на уровне ДБ необходимо:

1. Выбрать ДБ в дереве консоли и перейти на вкладку *Межсетевой экран*.
2. Перейти в категорию правил **Dallas Lock 8.0** или **Dallas Lock Linux** и на панели инструментов нажать кнопку **Создать**.
3. На экране появится окно мастера создания правил МЭ (рис. 108). Выбрать на какие модули будет распространяться данное правило, можно создать универсальное правило или правило для конкретного модуля. После нажать кнопку **Далее**.

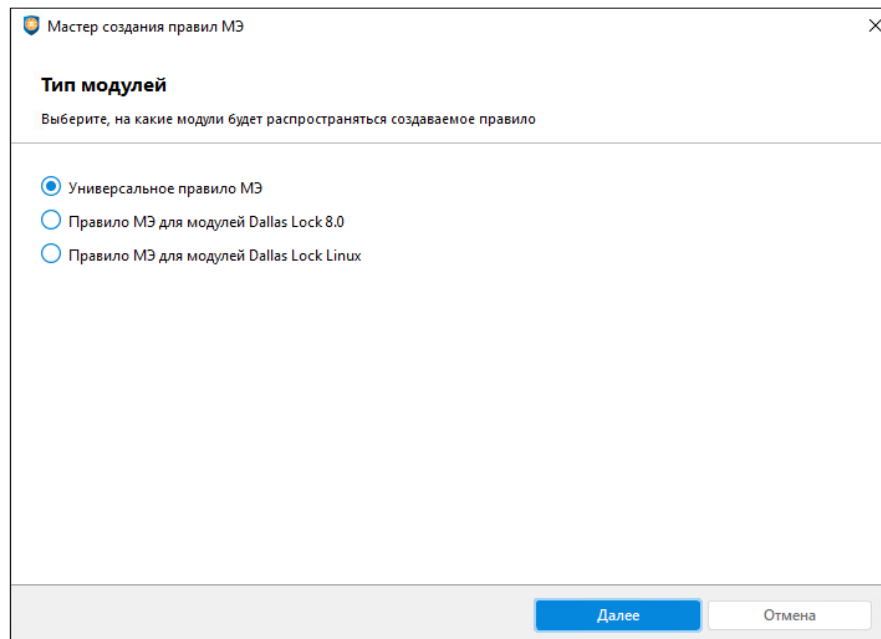


Рис. 108. Мастер создания правил МЭ

4. Ввести название правила и тип действия. После нажать кнопку **Далее**.
5. Выбрать объекты дерева домена, для которых правило будет активно либо оставить правило выключенным и нажать **Далее**.
6. Выбрать направления передачи и указать параметры правила. После нажать **Далее**.
7. Выбрать тип правила, определяющий набор протокол для дальнейшей настройки и нажать **Далее**. Заполнить необходимые поля и нажать **Далее**.
8. После откроется окно значений параметров создаваемого правила. Для завершения нажать кнопку **Готово**.

Созданное правило появится в таблице правил модулей, для которых оно было назначено. Открыть редактор правила можно следующими способами:

- дважды щелкнуть левой кнопкой мыши по изменяемому правилу;
- вызвать контекстное меню изменяемой политики и выбрать **Свойства**;
- нажать кнопку **Свойства** на панели *Действия*.

5.6 Система контроля накопителей

Для перехода к разделу настроек **Управление компонентом СКН** необходимо на вкладке *Компоненты* выбрать *Система контроля накопителей*. На странице **Управление компонентом СКН** можно редактировать параметры политик на уровне всего ДБ, после синхронизации на всех подчиненных объектах в ДБ применяются установленные настройки (рис. 109).

Более подробно о Системе контроля накопителей в Руководстве по эксплуатации **СЗИ Dallas Lock 8.0** глава 13 и в Руководстве по эксплуатации **Dallas Lock Linux** раздел 4.5.

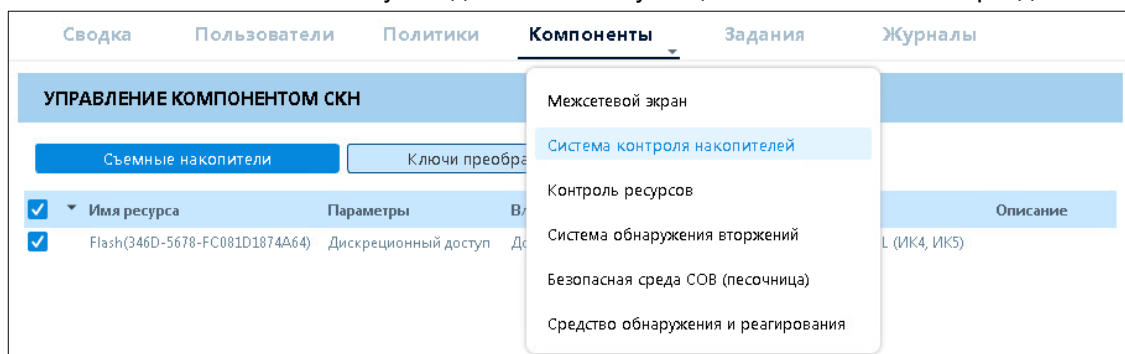


Рис. 109. Вкладка «Система контроля накопителей»

5.6.1 Съёмные накопители

В категории **Съёмные накопители** на вкладке **Управление компонентом СКН** формируется список всех установленных дескрипторов на сменные накопители, в том числе права доступа и назначенный аудит (рис. 110).

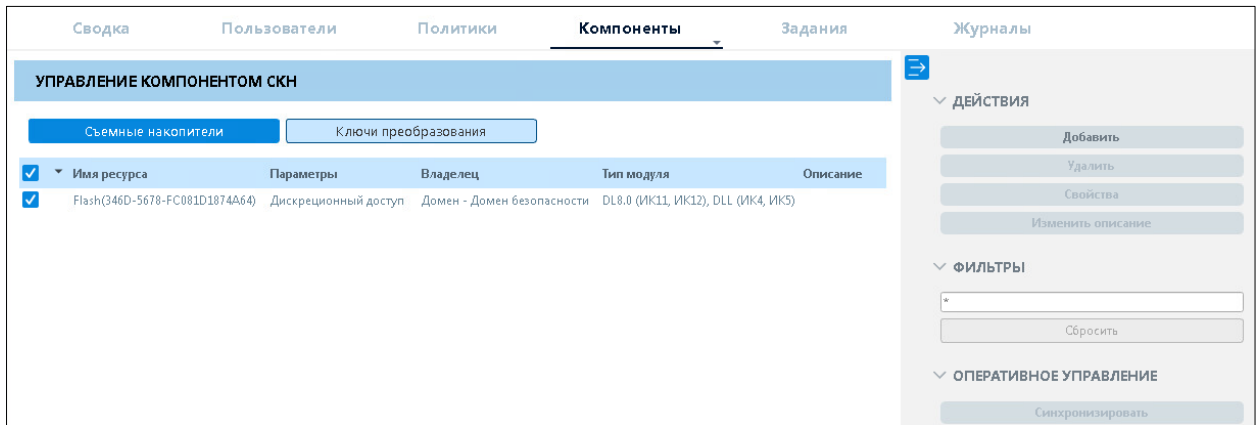


Рис. 110. Вкладка «Съёмные накопители»

Чтобы назначить права доступа к конкретному накопителю, необходимо:

1. Подключить этот накопитель к соответствующему порту ПК.
2. На панели действий нажать кнопку **Добавить**.
3. На экране появится окно мастера добавления съёмных накопителей (рис. 111).

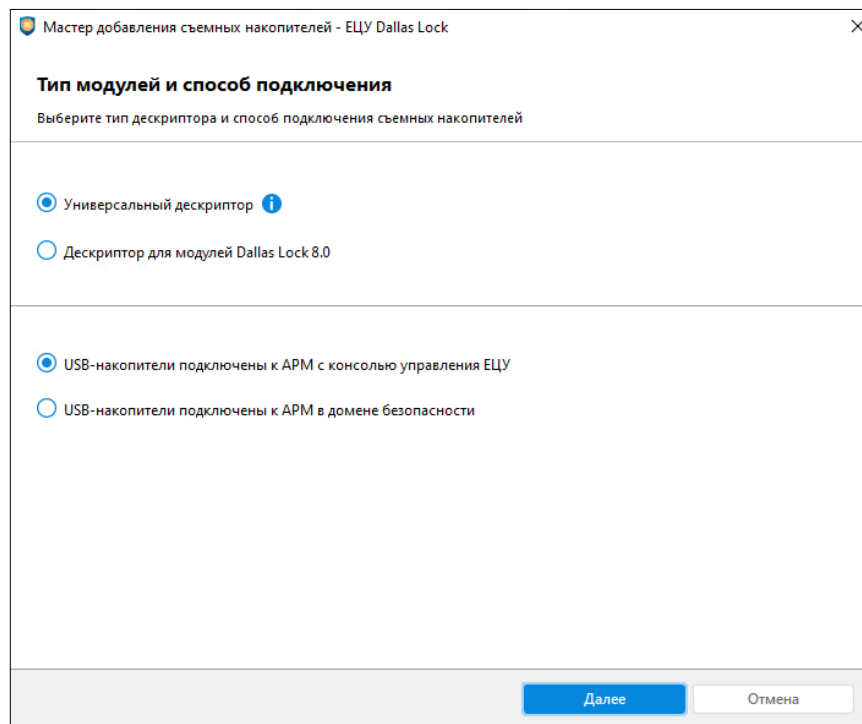


Рис. 111. Мастер добавления съёмных накопителей

4. Выбрать тип дескриптора и способ подключения съёмных накопителей. Нажать **Далее**.



Если накопитель подключен к **ЕЦУ**, работающему на ОС Linux, и доступ к его файловой системе отсутствует, необходимо установить недостающий пакет ntfs-3g.

5. Выбрать съёмный накопитель и объект файловой системы.

6. Настроить права доступа и аудит. Для завершения нажать **Готово**.

Добавленный накопитель появится в списке. Открыть редактор параметра можно следующими способами:

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



Для В список контролируемых объектов накопители занесутся в специальном формате, в который входит тип накопителя и его уникальный номер («Flash(XXXX-XXXX-XXXXXXXXXXXXXXXXXXXX):\»).

Для USB-Flash накопителей номер высчитывается как: идентификатор производителя (VendorID), идентификатор продукта (ProductID) и серийный номер (Serial Number).

5.6.2 Ключи преобразования

В категории **Ключи преобразования** на вкладке **Управление компонентом СКН** осуществляется централизованное управление ключами преобразования съемных накопителей (рис. 112).

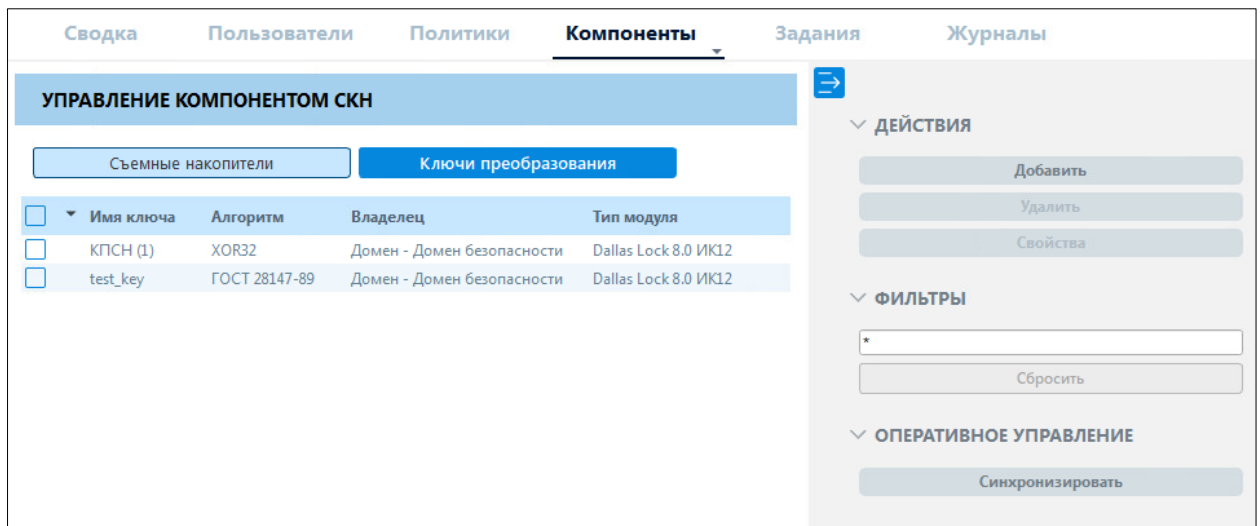


Рис. 112. Категория «Ключи преобразования»

В этой категории можно создавать, редактировать, удалять, активировать и деактивировать КПСН. Справа расположены панель инструментов *Фильтры* и панель инструментов *Действия* (кнопки данной панели также дублируются в контекстном меню).

Для создания КПСН необходимо нажать кнопку **Добавить** на панели инструментов *Действия* (или выбрать данную команду в контекстном меню таблицы КПСН), после чего откроется окно **Ключ преобразования съемных накопителей** (рис. 113).

Рис. 113. Окно «Ключ преобразования съемных накопителей»

Окно ввода параметров ключа преобразования содержит следующие параметры:

- «Имя ключа» — поле ввода имени КПСН.



Имя ключа должно быть уникальным, создание двух ключей с одинаковыми именами невозможно.

- «Ключ отключен» — чекбокс, который определяет активность ключа преобразования.
- «Доступ к накопителю по паролю» — чекбокс, который определяет необходимость предоставления пароля для доступа к накопителю.



Функциональная возможность «Доступ к накопителю по паролю» доступна только при наличии лицензии на модуль «СКН уровня отчуждения (переноса) информации».

- «Алгоритм» — выпадающий список для выбора алгоритма преобразования. Допустимые значения: XOR32 (значение по умолчанию), ГОСТ 28147-89 и Внешний криптопровайдер. При выборе значения *Внешний криптопровайдер* также становятся активными параметры *Криптопровайдер*, *Выбор алгоритма преобразования* и *Выбор алгоритма хеширования*.
- «Идентификатор».
- «Пароль ключа» и «Подтверждение» — поля для ввода и подтверждения пароля КПСН.

Для применения введенных настроек и создания ключа преобразования необходимо нажать на кнопку **Применить**. При нажатии на кнопку **Отмена** окно **Ключ преобразования съемных накопителей** закрывается, ключ преобразования не создается.

Редактирование параметров КПСН производится на аналогичной странице «Ключ преобразования съемных накопителей» (рис. 113) для выбранного КПСН. Открыть редактор КПСН можно следующими способами:

- дважды щелкнуть левой кнопкой мыши по изменяемому КПСН;
- вызвать контекстное меню изменяемого КПСН и выбрать «Свойства»;
- нажать кнопку **Свойства** на панели *Действия*.



Редактирование параметров КПСН доступно только на уровне дерева ДБ, на котором был создан КПСН, или на уровне ДБ. На нижележащих уровнях ДБ возможность редактирования параметров КПСН исключена, разрешен только просмотр свойств.

Для удаления КПСН необходимо использовать команду **Удалить**, после чего подтвердить удаление нажатием кнопки **Да** (рис. 114). За раз возможно удаление как одного ключа преобразования, так и нескольких сразу при множественном выделении.

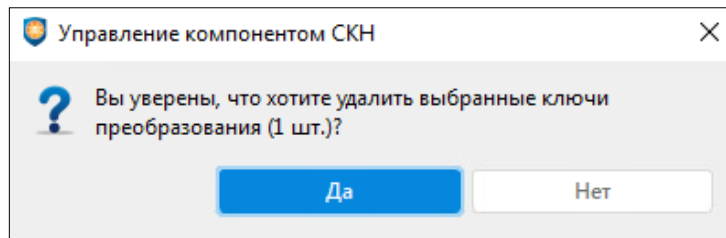


Рис. 114. Подтверждение удаления КПСН

Для удобства работы со списком КПСН можно воспользоваться сортировкой и фильтрацией:

- Сортировка производится нажатием на поле, содержащее название столбца, по которому необходима сортировка. Сортировка может быть выполнена как по убыванию, так и по возрастанию.
- Фильтрация настраивается на панели инструментов *Фильтры*, доступна фильтрация по всему содержимому списка КПСН. Сброс настроенного фильтра осуществляется по команде **Сбросить**.

5.7 Контроль ресурсов

Для перехода к разделу настроек **Управление контролем ресурсов** необходимо на вкладке *Компоненты* выбрать *Контроль ресурсов*. На странице **Управление контролем ресурсов** можно редактировать параметры политик на уровне всего ДБ, после синхронизации на всех подчиненных объектах в ДБ применяются установленные настройки (рис. 115).

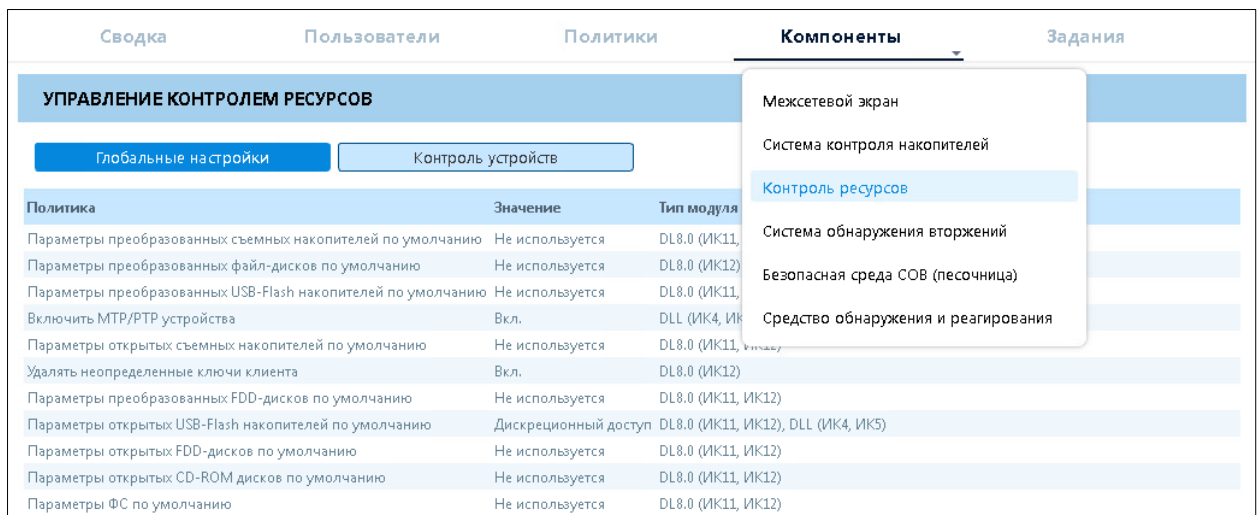


Рис. 115. Вкладка «Контроль ресурсов»

5.7.1 Глобальные настройки

Настройки, касающиеся значений политик СКН, регулируются в категории **Глобальные настройки** на вкладке **Управление контролем ресурсов**.

Таблица 22. Настройки СКН

Включить MTP/PTP устройства	
Возможное значение политики: «Вкл./Выкл.». Значение по умолчанию: «Выкл.». Данная политика позволяет настроить разрешение для включения MTP/PTP устройств. Политика применяется на модулях СЗИ Dallas Lock Linux.	
Параметры ФС по умолчанию	
Политика позволяет настроить доступ к параметрам ФС, предоставляя определенным пользователям или группам право на работу. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.	
Параметры CD-ROM дисков по умолчанию	
Политика позволяет настроить доступ к параметрам CD-ROM дисков, предоставляя определенным пользователям или группам право на работу. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.	
Параметры открытых FDD-дисков по умолчанию	
Политика позволяет настроить доступ к параметрам открытых FDD-дисков, предоставляя определенным пользователям или группам право на работу. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.	
Параметры открытых USB-Flash накопителей по умолчанию	
Политика позволяет настроить доступ к параметрам открытых USB-Flash накопителей, предоставляя определенным пользователям или группам право на работу. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ НСД Dallas Lock Linux.	
	В случае, если на клиентском АРМ с СЗИ Dallas Lock Linux не применились корректно разрешающие правила для USB-накопителей (можно проверить в оболочке администрирования Dallas Lock Linux на вкладке <i>Контроль ресурсов</i> в категории Блочные устройства в поле <i>Тип контроля</i>), необходимо проделать следующие действия:
	В консоли ЕЦУ для данного АРМ (или для группы, или для всего домена безопасности) настроить данную политику следующим образом: Дискреционный доступ – Все – установить значение <i>Полный доступ</i>. На панели инструментов <i>Оперативное управление</i> использовать кнопку Синхронизировать, дождаться сообщения «Команда синхронизации инициирована для вложенных модулей». В консоли ЕЦУ для данного АРМ (или для группы, или для всего домена безопасности) настроить данную политику следующим образом: Дискреционный доступ – Все – установить значение <i>Запретить всё</i>. На панели инструментов <i>Оперативное управление</i> использовать кнопку Синхронизировать, дождаться сообщения «Команда синхронизации инициирована для вложенных модулей». Проверить на АРМ корректность установленных настроек.
Параметры открытых съемных накопителей по умолчанию	
Политика позволяет настроить доступ к параметрам открытым съемным накопителям, предоставляя определенным пользователям или группам право на работу. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C.	

Параметры преобразованных FDD-дисков по умолчанию

Политика позволяет настроить доступ к параметрам преобразованных FDD-дисков, предоставляя определенным пользователям или группам право на работу.

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

Параметры преобразованных USB-Flash накопителей по умолчанию

Политика позволяет настроить доступ к параметрам преобразованных USB-Flash накопителей, предоставляя определенным пользователям или группам право на работу.

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

Параметры преобразованных съемных накопителей по умолчанию

Политика позволяет настроить доступ к параметрам преобразованных съемных накопителей, предоставляя определенным пользователям или группам право на работу.

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

Параметры преобразованных файл-дисков по умолчанию

Политика позволяет настроить доступ к параметрам преобразованных файл-дисков, предоставляя определенным пользователям или группам право на работу.

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

Удалять неопределенные ключи клиента

Политика позволяет настроить удаление неопределенных ключей клиента.

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

Если на клиенте имеются локально созданные ключи преобразования, которые не совпадают с ключами, созданными в ДБ для данного клиента:

- если политика включена, то в процессе синхронизации клиентов эти ключи будут удалены;
- если политика отключена, то в процессе синхронизации клиентов эти ключи заблокируются (будут переведены в неактивное состояние).



Если имя локального ключа совпадает с именем ключа, присланного с **ЕЦУ**, то приоритетным является ключ, присланный с **ЕЦУ**, и, соответственно, локальный ключ будет заменен на ключ, присланный с **ЕЦУ**.

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

5.7.2 Контроль устройств

Централизованное управление контролем устройств осуществляется в категории **Контроль устройств** на странице **Управление контролем ресурсов** (рис. 116).

Имя и параметры	Тип контроля	Тип модуля
Хост-контроллер...		DL 8.0 (ИК12)
Съемные накопит...		DL 8.0 (ИК12)
Другие устрой...	Дискреционные...	DLL (ИК5)
USB-Flash диски	Дискреционные...	DL 8.0 (ИК12), DLL (ИК5)
FDD-диски	Дискреционные...	DL 8.0 (ИК12), DLL (ИК5)
CD-ROM диски	Дискреционные...	DL 8.0 (ИК12), DLL (ИК5)
Считыватели сма...		DL 8.0 (ИК12)
Сканеры и цифро...		DL 8.0 (ИК12)
Сетевые адаптеры		DL 8.0 (ИК12)
Сенсоры		DL 8.0 (ИК12)
Радиоинтерфейсы	Дискреционные...	DLL (ИК5)
PCMCIA устройства		DL 8.0 (ИК12)
Принтеры		DL 8.0 (ИК12), DLL (ИК5)
Преобразованн...		DL 8.0 (ИК12)
USB-Flash диски		DL 8.0 (ИК12)
FDD-диски		DL 8.0 (ИК12)

Рис. 116. Категория «Контроль устройств»

Управление контролем устройств осуществляется при помощи кнопок на панели *Действия*, а также при помощи кнопок, дублируемых в контекстном меню таблицы, содержащей дерево классов устройств.

5.8 Система обнаружения вторжений

Для перехода к разделу настроек **Управление компонентом СОВ** необходимо на вкладке *Компоненты* выбрать *Система обнаружения вторжений*. На странице **Управление компонентом СОВ** можно редактировать параметры на уровне всего ДБ, после синхронизации на всех подчиненных объектах в ДБ применяются установленные настройки (рис. 117).

Более подробно о Системе обнаружения вторжений описано в Руководстве по эксплуатации **СЗИ Dallas Lock 8.0** глава 16 и в Руководстве по эксплуатации **Dallas Lock Linux** раздел 4.13.

Рис. 117. Вкладка «Система обнаружения вторжений»



Управление системой обнаружения вторжений в **ЕЦУ** реализовано для модулей **СЗИ НСД Dallas Lock 8.0** и **СЗИ НСД Dallas Lock Linux**, переключение управления между модулями осуществляется в рабочей области вкладки с помощью выпадающего списка. Состав допустимых категорий и параметров для управления будет варьироваться в зависимости от модуля, для которого производится настройка.

5.8.1 Сводка СОВ

На вкладке **Управление компонентом СОВ** в категории **Сводка СОВ** отображаются информация об обновлении СОВ и журналы событий СОВ с клиентов (рис. 118).

На вкладке **Управление компонентом СОВ** в категории **Сводка СОВ** выделено 2 раздела:

- Основная информация;
- Журнал событий.

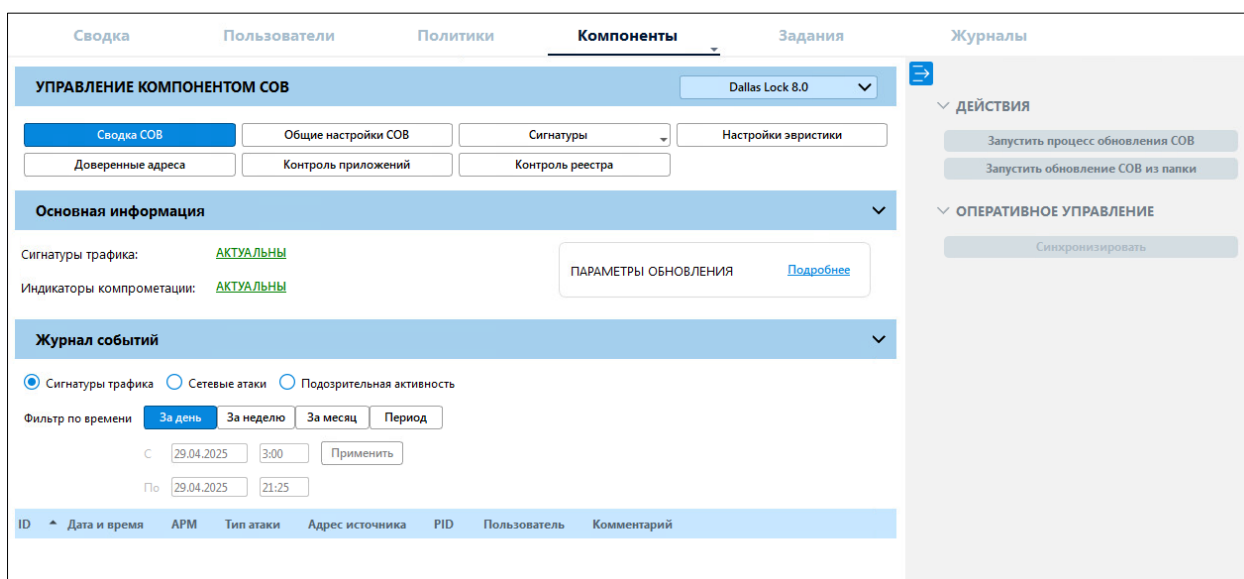


Рис. 118. Категория «Сводка COB»

! Раздел *Основная информация*, а также действия **Запустить процесс обновления COB** и **Запустить обновление COB** из папки панели инструментов доступны только на уровне корня Домена безопасности.

С помощью команды оперативного управления **Синхронизировать** в категории **Сводка COB** производится синхронизация всех произведенных на вкладке **Управление компонентом COB** настроек.

На панели *Действия* доступны следующие команды оперативного управления:

- **Запустить процесс обновления COB** — позволяет загрузить обновления с FTP-сервера или из локальной папки для баз решающих правил (далее — БРП) компонента COB в БД ЕЦУ согласно заданным параметрам обновления (рис. 120). При иницировании команды появляется окно **Обновление базы решающих правил компонента COB** (рис. 119).

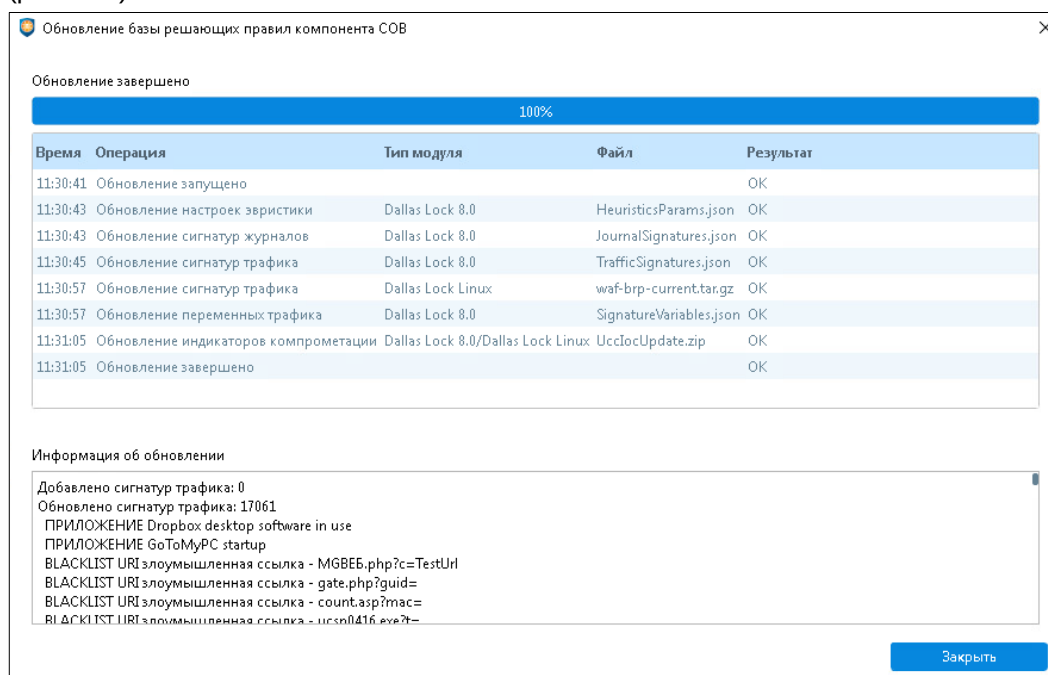


Рис. 119. Обновление базы решающих правил компонента COB

- **Загрузить обновления COB из папки** — позволяет выбрать локальную директорию для разовой загрузки обновления БРП COB в БД ЕЦУ. При инициировании команды открывается окно для выбора директории с файлами обновления.

В рабочей области раздела *Основная информация* выделены поля *Сигнатуры трафика* и *Индикаторы компрометации*, которые позволяют получить информацию об актуальности сигнатур трафика и индикаторов компрометации, имеющихся в БД ЕЦУ. Поля имеют два состояния:

- «АКТУАЛЬНЫ» — набор сигнатур трафика / индикаторов компрометации обновился, с момента обновления прошло меньше, чем две недели;
- «УСТАРЕЛИ» — с момента последнего обновления набора сигнатур трафика / индикаторов компрометации прошло больше, чем две недели. При нажатии на кнопку **УСТАРЕЛИ** иницируется команда оперативного управления **Запустить процесс обновления COB**.

При нажатии кнопки **Подробнее** поля *Параметры обновления* в разделе *Основная информация* открывается окно **Состояние обновления базы решающих правил COB** (рис. 120), в котором можно настроить параметры обновления БРП компонента COB в БД ЕЦУ, а также посмотреть информацию о последнем обновлении БРП.

Состояние обновления базы решающих правил COB

Информация об обновлении базы решающих правил для модулей Dallas Lock 8.0

Название модуля COB	Время и дата	Версия	Состояние	Комментарий
Обновление настроек эвристики	27.05.2025 10:22:15	1	Включено	Базовое
Обновление сигнатур журналов	27.05.2025 10:22:15	10	Включено	Значимые обновления
Обновление сигнатур трафика	27.05.2025 10:22:15	197	Включено	Регулярное обновление
Обновление переменных трафика	27.05.2025 10:22:15	1	Включено	Базовое
Обновление индикаторов компрометации	27.05.2025 10:22:16	1	Включено	Базовое

Информация об обновлении базы решающих правил для модулей Dallas Lock Linux

Название модуля COB	Время и дата	Версия	Состояние	Комментарий
Обновление сигнатур трафика	27.05.2025 10:22:15	101	Включено	Базовое
Обновление индикаторов компрометации	27.05.2025 10:22:16	1	Включено	Базовое

Настройки обновления базы решающих правил COB, и в том числе базы индикаторов компрометации

Регулярность обновления

☐ Вручную
☐ Раз в сутки
☒ Раз в две недели

Источники обновления:

HTTPS

Применить Закрыть

Рис. 120. Окно «Состояние обновления базы решающих правил COB»

Рабочая область раздела *Журнал событий* содержит список событий по сработавшим сигнатурам и произошедшим сетевым атакам, а также зарегистрированные события подозрительной активности. Выбор отображаемого списка событий осуществляется с помощью переключателя:

- если для управления компонентом **Система обнаружения вторжений** выбран модуль **СЗИ НСД Dallas Lock 8.0** — доступны журналы категорий *Сигнатуры трафика*, *Сетевые атаки* и *Подозрительная активность*;
- если для управления компонентом **Система обнаружения вторжений** выбран модуль **СЗИ НСД Linux** — доступны журналы категорий *Сигнатуры* и *Сетевые атаки*.

5.8.2 Общие настройки СОВ

На вкладке **Управление компонентом СОВ** в категории **Общие настройки СОВ** регулируются настройки, касающиеся значений политик СОВ, а также некоторых параметров обновления СОВ для системы **ЕЦУ**.



Параметры, которые управляют обновлением БРП в БД **ЕЦУ**, отображается только на уровне корне ДБ.

Таблица 23. Общие настройки СОВ

Анализ журналов ОС
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Политика позволяет включать и отключать сигнатурный и эвристический анализ, использующий журналы ОС и приложений. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ НСД Dallas Lock Linux.
Анализ сигнатур атак в сетевом трафике
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Политика позволяет включать и отключать сигнатурный эвристический анализ, использующий Журнал трафика. Политика применяется на модулях: • СЗИ Dallas Lock 8.0-K/C; • СЗИ НСД Dallas Lock Linux.
Аудит: IoC
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Политика применяется на модулях СЗИ НСД Dallas Lock Linux .
Аудит: изменение параметров СОВ
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Политика применяется на модулях СЗИ НСД Dallas Lock Linux .
Аудит: срабатывание журнальных сигнатур
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Политика применяется на модулях СЗИ НСД Dallas Lock Linux .
Аудит: срабатывание сигнатур трафика
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Политика применяется на модулях СЗИ НСД Dallas Lock Linux .
Аудит: срабатывание эвристик
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Политика применяется на модулях СЗИ НСД Dallas Lock Linux .
Блокировать снятие скриншотов по клавише PrintScreen
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Выкл.». Включение политики позволяет блокировать процесс копирования изображения текущего состояния экрана в буфер обмена при нажатии клавиши Print Screen. Политика применяется на модулях СЗИ Dallas Lock 8.0-K/C .
Блокировка отправки телеметрии Windows
Возможное значение политики: «7 суток», «10 суток», «30 суток» и «Не используется». По умолчанию значение данной политики: «Не используется». Политика предназначена для ограничения сбора диагностических данных и их отправки на серверы Microsoft, с выбором периодичности автоматического обновления файлов.

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

Включить систему обнаружения вторжений

Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Политика позволяет включать и отключать COB.

Политика применяется на модулях:

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

Заносить в журнал политик проверки наличия обновлений

Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Выкл.». Включение политики позволяет вести учет проверок на наличие обновлений в журнале управления политиками.

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

Защита от вирусов шифровальщиков

Возможное значение политики: «Режим аудита», «Активный режим», «Активный режим с очисткой», «Активный режим с восстановлением» и «Не используется». По умолчанию значение данной политики: «Активный режим».

Политика позволяет осуществлять настройку механизма защиты от вирусов-шифровальщиков, который нацелен на обнаружение неизвестных антивирусным базам вредоносных программ по их поведению.

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

Источник обновлений

Для управления политикой доступны следующие элементы (рис. 121):

- таблица с источниками обновления с сайта или из папки:
 - столбец *Используется* — содержит чекбоксы для включения/выключения источника обновления. По умолчанию чекбокс активирован у источника с типом *HTTPS*;
 - столбец *Тип* — содержит фиксированные значения *HTTPS* и *Папка*;
 - столбец *Источник* — содержит адрес источника для обновления. Для типа *HTTPS* значение по умолчанию *updates.dallaslock.ru/Update*, для типа *Папка* по умолчанию адрес источника не задан;
- кнопка **Изменить**, позволяющая изменять адрес выбранного источника;
- кнопки **Вверх** и **Вниз**, позволяющие изменять местами строки с источниками в таблице для установления приоритета обновления.

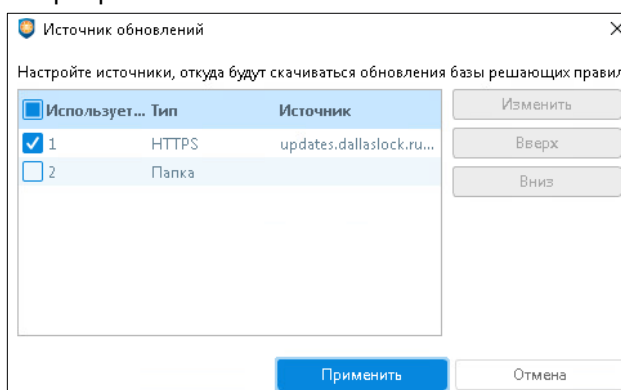


Рис. 121. Окно настройки политики «Источник обновлений» для модулей СЗИ Dallas Lock 8.0

Политика позволяет задать источник обновления БРП.

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

Источник обновлений

Для управления политикой доступны следующие элементы (рис. 122):

- таблица с источниками обновления с сайта или из папки:
 - столбец *Используется* — содержит чекбоксы для включения/выключения источника обновления. По умолчанию чекбокс активирован у источника с типом *HTTPS*;

- столбец *Тип* — содержит фиксированные значения *HTTPS* и *Архив*;
- столбец *Источник* — содержит адрес источника для обновления. Для типа *HTTPS* значение по умолчанию `updates.dallaslock.ru/WafUpdate/waf-brp-current.tag.gz`, для типа *Архив* по умолчанию адрес источника не задан;
- кнопка **Изменить**, позволяющая изменять адрес выбранного источника;
- кнопки **Вверх** и **Вниз**, позволяющие изменять местами строки с источниками в таблице для установления приоритета обновления.

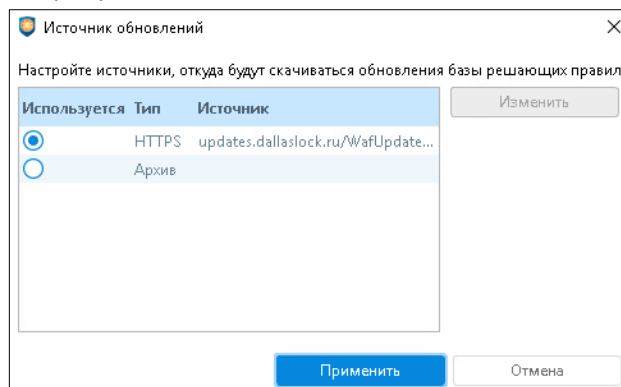


Рис. 122. Окно настройки политики «Источник обновлений» для модулей СЗИ Dallas Lock Linux

Политика позволяет задать источник обновления БРП.

Политика применяется на модулях **СЗИ НСД Dallas Lock Linux**.

Контроль приложений

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

Политика позволяет включать и отключать функционирование контроля приложений.

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

Маскирование датчика COB

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

Политика позволяет скрыть наличие датчика COB для пользователей, не имеющих прав на просмотр и изменение настроек COB. Для таких пользователей не будут появляться уведомления COB, а также в меню значка блокировки скроется пункт COB.

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

Настройки оповещения контроля приложений

Для управления доступны следующие элементы (рис. 123):

- чекбокс *Включить оповещение контроля приложений* — включает настройку оповещения в таблице ниже (при отключенном чекбоксе остальные параметры политики недоступны для редактирования). По умолчанию чекбокс не активирован;
- таблица с правилами для контроля приложений и пороговыми значениями:
 - столбец *Системные функции приложения* — содержит фиксированный список системных функций, а также чекбоксы для включения/выключения оповещения. По умолчанию все чекбоксы выключены;
 - столбец *Порог для информационного оповещения в день* — поле для ввода числового значения, допустимые значения: от «0» до «9997». Значение по умолчанию для всех функций: «50»;
 - столбец *Порог для оповещений об опасной активности в день* — поле для ввода числового значения, допустимые значения: от «1» до «9998». Значение по умолчанию для всех функций: «100»;
 - столбец *Порог для информационного оповещения в неделю* — поле для ввода числового значения, допустимые значения: от «2» до «99999». Значение по умолчанию для всех функций: «350»;
 - столбец *Порог для оповещений об опасной активности в неделю* — поле для ввода числового значения, допустимые значения: от «3» до «10000». Значение по умолчанию для всех функций: «700».

Редактирование пороговых значений осуществляется по двойному клику на ячейку.

Правила для контроля приложений	Порог для инф...	Порог для опо...	Порог для инф...	Порог для опове...
☐ Модификация памяти ядра с помощью ...	50	100	350	700
☐ Вызов функции SetWinEventHook для внедрени...	50	100	350	700
☐ Вызов функции SetWindowsHook для внедрени...	50	100	350	700
☐ Вызов функции SetThreadContext для внедрени...	50	100	350	700
☐ Вызов функции для работы с памятью чужого ...	50	100	350	700
☐ Вызов функции DupHandles для работы с ...	50	100	350	700
☐ Вызов функции для создания потока в чужом ...	50	100	350	700
☐ Вызов функции потока в чужом процессе	50	100	350	700
☐ Управление чужим процессом с помощью ...	50	100	350	700
☐ Установка драйвера	50	100	350	700
☐ Запуск драйвера	50	100	350	700
☐ Установка службы	50	100	350	700

Рис. 123. Настройка оповещения контроля приложений



Значения в столбцах с пороговыми значениями зависят друг от друга: значение в каждом столбце должно превышать значение левого столбца, но не превышать значение правого столбца. Нарушение данного правила при вводе значений приведет к ошибке.

Политика позволяет произвести настройку оповещений для контроля приложений.

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

Настройки списка блокировок

Для управления доступны следующие элементы (рис. 124):

- чекбокс *Включить использование файлов блокировки* — включает настройку использования файлов блокировок (при отключенном чекбоксу параметры политики недоступны для редактирования). По умолчанию чекбокс не активирован;
- выпадающий список *Частота опроса* — содержит значения «1 час», «2 часа», «3 часа», «6 часов», «8 часов», «12 часов», «1 сутки» и «2 суток». Значение по умолчанию «1 сутки»;
- таблица с адресами файлов блокировки:
 - столбец *Адрес файла* — содержит адреса файлов блокировки, а также чекбоксы для активации;



Можно добавлять следующие типы адресов файлов:

- для файлов на сервере в сети Интернет `http(s)://<Site>/<fileName>.txt`;
- для файлов на жестком диске `<Drive>:\<Path>\<fileName>.txt`;
- для файлов на сетевом диске `\\<Server>\<Path>\<fileName>.txt`.

- столбец *Аудит* — позволяет включать аудит с помощью чекбоксов для указанных файлов блокировок;
- кнопка **Изменить**, позволяющая изменить адрес выбранного файла;
- кнопки **Удалить** и **Удалить все**, позволяющие удалить один или сразу все адреса;
- кнопки **Добавить URL** и **Добавить файл**, позволяющие добавлять новый адрес в таблицу.

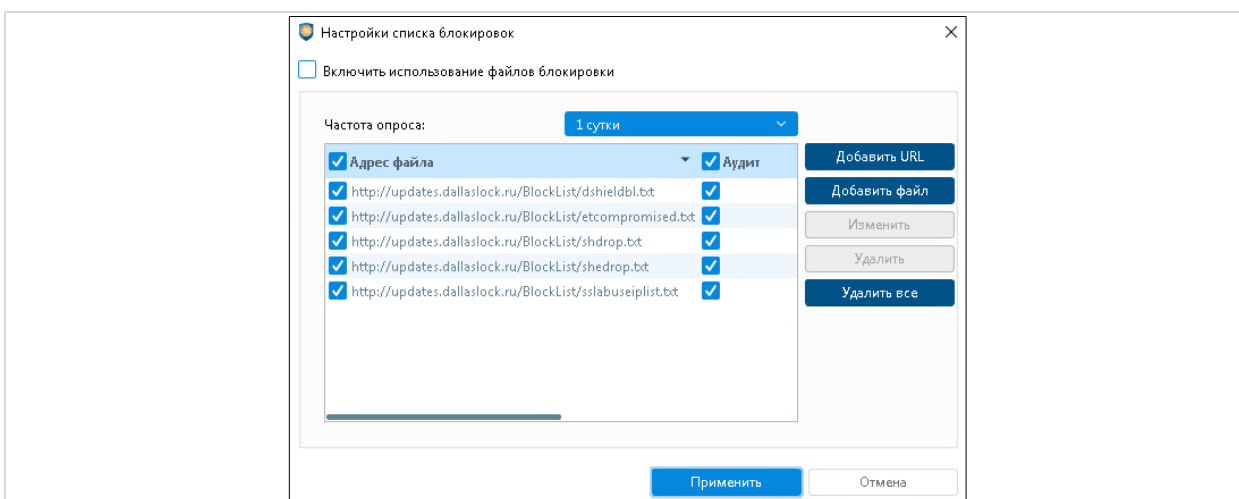


Рис. 124. Настройка списка блокировок

Политика позволяет включать и отключать использование файлов блокировки, управлять составом файлов блокировки и частотой их опроса.

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

Не заносить повторы в журнал контроля приложений

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

Включение политики позволяет фильтровать повторяющиеся однотипные события в журнале контроля приложений.

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

Обновление детектора атак

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

Включение и отключение обновления детектора атак (настройки эвристики) при ручном или автоматическом обновлении.

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

Обновление настроек эвристики

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

Включение и отключение обновления глобальных настроек эвристики при ручном или автоматическом обновлении.

Политика применяется на:

- службу **ЕЦУ**;
- модулях **СЗИ Dallas Lock 8.0-K/C**.

Обновление переменных трафика

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

Включение и отключение обновления переменных трафика при ручном или автоматическом обновлении.

Политика применяется на:

- службу **ЕЦУ**;
- модулях **СЗИ Dallas Lock 8.0-K/C**.

Обновление сигнатур журналов

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

Включение и отключение обновления сигнатур журналов при ручном или автоматическом обновлении.

Политика применяется на:

- службу **ЕЦУ**;
- модулях **СЗИ Dallas Lock 8.0-K/C**.

Обновление сигнатур трафика

Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Включение и отключение обновления сигнатур трафика при ручном или автоматическом обновлении.

Политика применяется на:

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

Период блокировки

Для управления доступны следующие элементы: переключатели *Заблокировать на время* и *Заблокировать навсегда*. При выборе *Заблокировать на время* доступна настройка времени блокировки в формате ЧЧ:ММ, значение по умолчанию *Заблокировано на время* — 15 минут.

Политика отвечает за время блокировки обнаруженного источника атаки.

Политика применяется на модулях:

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

Протоколирование событий СОВ

Для управления доступны следующие элементы: Список событий для протоколирования с чекбоксами.

Политика позволяет выбрать регистрируемые события об изменении конфигурации СОВ.

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

Расширенное определение атак подмены адресов

Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Выкл.». Включение политики позволяет минимизировать ложные срабатывания обнаружения некоторых атак при получении сетевым адаптером пакетов, адресованных не только непосредственно данному адаптеру.

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

Регулярность обновлений

Возможное значение политики: «Вручную», «Раз в сутки» и «Раз в две недели». По умолчанию значение данной политики: «Вручную».

Политика отвечает за регулярность автоматического обновления БРП.

Политика применяется на модулях:

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

Синхронизировать список доверенных адресов

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

Политика позволяет включать/отключать синхронизацию списка доверенных адресов между ЕЦУ и модулями.

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

Уровень блокировки

Возможное значение политики: от 1 до 10. По умолчанию значение данной политики: «10».



Значение данной политики должно быть не ниже установленного значения для политики Уровень журналирования. При нарушении данного условия будет выведено соответствующее сообщение об ошибке.

Политика отвечает за количество баллов, при наборе которых произойдет реагирование на атаку.

Политика применяется на модулях:

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

Уровень журналирования

Возможное значение политики: от 1 до 10. По умолчанию значение данной политики: «7».



Значение данной политики не должно превышать установленное значение для политики Уровень блокировки. При нарушении данного условия будет выведено соответствующее сообщение об ошибке.

Политика отвечает за количество баллов, при которых произойдет реагирование на атаку.

Политика применяется на модулях:

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

Эвристический анализ COB

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

Политика позволяет включать и отключать блокировку атак на протоколы и сканирование портов.

Политика применяется на модулях:

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

5.8.3 Сигнатуры

На вкладке **Управление компонентом COB** в категории *Сигнатуры* регулируются настройки, касающиеся сигнатур COB модулей **СЗИ Dallas Lock 8.0-K/C** и **СЗИ НСД Dallas Lock Linux**.

Категория реализована в виде выпадающего списка, состоящего из следующих вложенных категорий:

- *Сигнатуры журналов* — предназначены для анализа журналов Windows и журналов антивируса Kaspersky Endpoint Security;
- *Сигнатуры трафика*;
- *Сигнатуры: переменные трафика* (для модулей **СЗИ Dallas Lock 8.0-K/C**) — предназначены для настройки переменных в сигнатурах трафика.



Полное управление сигнатурами (создание, удаление, редактирование и т.д.) доступно только на уровне корня ДБ.

На уровне группы, подгруппы, АРМ и модулей доступен только просмотр списка сигнатур с их значениями, а также управление состоянием сигнатур (активация / деактивация) и наследованием состояния.

Рабочая область категории *Сигнатуры* содержит списки сигнатур домена с установленными значениями. Списки сигнатур являются едиными для всего домена.

Управление списком сигнатур осуществляется командами на панели *Действия* или через контекстное меню рабочей области списка сигнатур.

Для списка сигнатур доступен поиск по ключевым словам посредством панели *Фильтры*. Для сигнатур трафика также доступна фильтрация по параметрам.

При инициировании команды *Запустить процесс обновления COB* на вкладке *Сводка COB* происходит обновление типовых шаблонов сигнатур COB для всего ДБ, предоставляемых компанией ООО «Конфидент». Обновление производится следующим образом:

- новые типовые шаблоны сигнатур, пришедшие с обновлением, добавляются;
- созданные пользователем сигнатуры не удаляются и остаются без изменений;
- для существующих типовых шаблонов сигнатур трафика — обновляется только информация скрытого раздела *Содержимое*. Настройки раздела *Общие* и состояние сигнатуры (активна/деактивирована) не изменяются;
- для существующих типовых шаблонов сигнатур журналов — добавляются только новые типовые сигнатуры, для уже существующих сигнатур настройки не изменяются;
- для существующих типовых шаблонов переменных трафика — добавляются новые переменные, для уже существующих переменных настройки не изменяются.



Типовые шаблоны сигнатур — шаблоны типовых сигнатур, поставляемые компанией ООО «Конфидент», которые были загружены при установке **ЕЦУ** или получены с сервера при обновлении (имеют уникальный идентификатор менее 100 000).
Пользовательские сигнатуры — сигнатуры, созданные пользователем (имеют уникальный идентификатор более 100 000).

Сигнатуры журналов для модулей **СЗИ НСД Dallas Lock 8.0-С/К**

В рабочей области вложенной категории *Сигнатуры журналов* список сигнатур журналов и сведения о них отображаются в виде древовидной структуры (рис. 125).

Описание	ID сигнатуры	Статус события	Уровень тревоги	Частота сра
Группа правил Windows	1	Все	1	
Группа правил KES	116	Все	1	
Базы устарели	117	Все	1	
Базы сильно устарели	118	Все	1	
Запуск обновления	119	Все	1	
Завершение обновления	120	Все	1	
Самозащита программы выключена	121	Все	1	
Важные компоненты защиты выключе...	122	Все	1	
Обнаружен вредоносный объект (лока...	124	Все	8	
Обнаружена активная угроза. Требуе...	125	Все	8	
Открыта опасная ссылка	126	Все	8	
Сработал компонент Предотвращение ...	127	Все	8	
Сетевое соединение заблокировано	128	Все	8	
Обнаружена сетевая атака	129	Все	8	
Обновлены не все компоненты	130	Все	1	

Рис. 125. Категория «Сигнатуры журналов» для модулей **СЗИ НСД Dallas Lock 8.0**

Для сигнатур журналов для модулей **СЗИ НСД Dallas Lock 8.0** определены следующие индикаторы состояния:



— сигнатура активирована, состояние не наследуется с верхнего уровня домена;



— сигнатура деактивирована, состояние не наследуется с верхнего уровня домена;



— сигнатура активирована, состояние наследуется с верхнего уровня домена;



— сигнатура деактивирована, состояние наследуется с верхнего уровня домена;



— сигнатура активирована, но не функционирует, так как родительская сигнатура деактивирована.

Для других столбцов значения сигнатур отображаются в соответствии с заданными АИБ значениями.

В данной вложенной категории можно добавлять, редактировать, удалять, активировать, деактивировать, сохранять и загружать сигнатуры журналов. Также для таблицы сигнатур возможно сворачивать и разворачивать все вложенные элементы дерева сигнатур журналов с помощью кнопок **Свернуть все** / **Развернуть все** соответственно.

Для просмотра настроенных параметров сигнатур необходимо нажать кнопку **Просмотр** на панели *Действия*.

Для добавления новой сигнатуры журналов на уровне ДБ необходимо:

1. Выбрать ДБ в дереве консоли и перейти на вкладку *Система обнаружения вторжений*. Рядом с наименованием страницы выбрать модуль *Dallas Lock 8.0*.
2. Перейти во вложенную категорию *Сигнатуры* → *Сигнатуры журналов* и на панели *Действия*

нажать кнопку **Добавить**.

3. На экране появится окно мастера добавления сигнатур журналов (рис. 126). Ввести краткую информацию и выбрать родительские сигнатуры:

- текстовое поле *ID сигнатуры* — уникальный числовой идентификатор сигнатуры. Поле недоступно для редактирования, номер присваивается автоматически, начиная со значения 100 001;
- текстовое поле *Описание сигнатуры* — имя создаваемой сигнатуры. Параметр может быть не уникальным;
- текстовое поле *Информация* — комментарий для создаваемой сигнатуры. Параметр может быть не уникальным;
- поле поиска *Родительские сигнатуры* с выпадающим списком результатов поиска — поле позволяет искать по именам всех существующих сигнатур журналов;
- поле с перечнем имен добавленных родительских сигнатур — параметр определяет, в какие существующие сигнатуры журналов будет добавлена дочерней создаваемая сигнатура. Может содержать несколько значений. По умолчанию поле:
 - пустое, если перед нажатием кнопки **Добавить** (на панели действий категории *Сигнатуры журналов*) не было выбрано ни одной сигнатуры из списка;
 - содержит имена сигнатур, которые были выбраны из списка перед нажатием кнопки **Добавить** (на панели действий категории *Сигнатуры журналов*).

Рис. 126. Мастер добавления сигнатур журналов

Для продолжения процесса добавления сигнатур нажать кнопку **Далее**.

4. Установить необходимые параметры сигнатуры (рис. 127) и нажать кнопку **Далее**.

Мастер добавления сигнатур журналов

Общие настройки сигнатуры
Установите необходимые параметры сигнатуры

Статус события: Успех Уровень тревоги: 0

Частота срабатывания: Интервал времени:

Коды событий журнала:

Параметры

☐ Принудительная сигнализация

Назад Далее Отмена

Рис. 127. Мастер добавления сигнатур журналов

5. Выбрать объекты дерева, для которых создаваемая сигнатура будет активна, либо оставить сигнатуру выключенной. Нажать кнопку **Далее**.
6. Добавить ключевые слова (маску), которые должны содержаться в тексте описания события для срабатывания. Нажать кнопку **Далее**.
7. После откроется окно значений параметров создаваемого правила. Для завершения нажать кнопку **Готово**.

Для редактирования сигнатуры необходимо выбрать сигнатуру в рабочей области категории и нажать кнопку **Редактировать** на панели *Действия*.

Для удаления сигнатур необходимо выбрать одну или несколько существующих пользовательских сигнатур из таблицы и нажать кнопку **Удалить** на панели *Действия*, после чего подтвердить удаление.



Удаление типовых шаблонов сигнатур журналов недоступно, при необходимости их можно только деактивировать.

Для загрузки сигнатур журналов из файла необходимо нажать кнопку **Загрузить** на панели *Действия*, после чего в появившемся окне выбрать необходимый файл сигнатур журналов.



При загрузке сигнатур журналов из файла все текущие сигнатуры журналов будут удалены.

Сигнатуры журналов для модулей СЗИ НСД Dallas Lock Linux

В рабочей области вложенной категории *Сигнатуры журналов* список сигнатур журналов и сведения о них отображаются в виде таблицы (рис. 128).

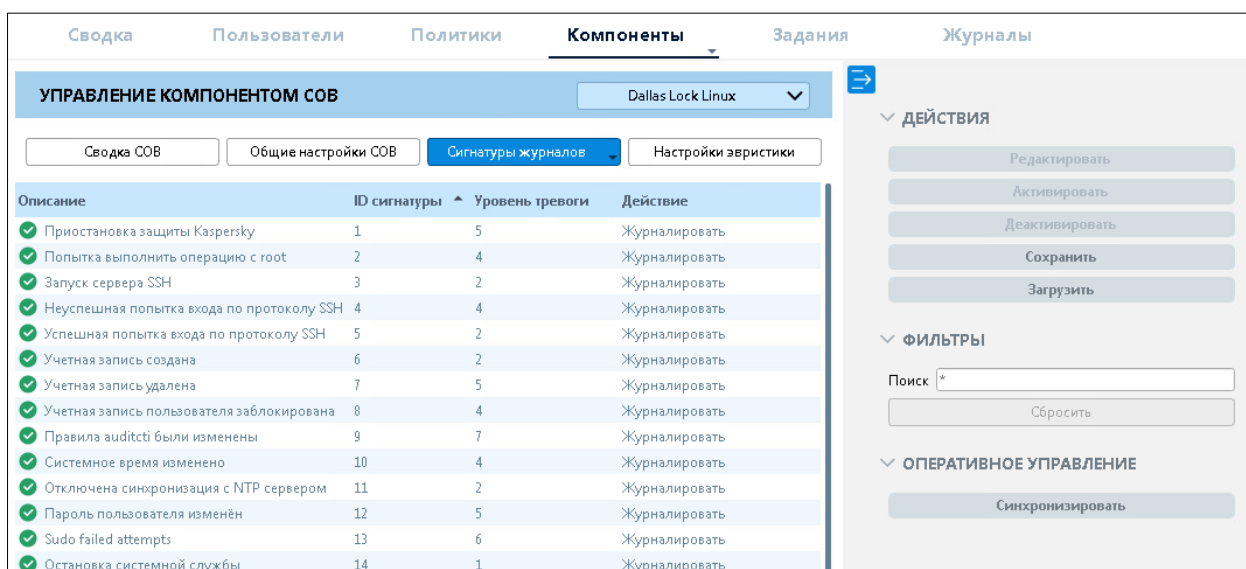


Рис. 128. Категория «Сигнатуры журналов» для модулей CЗИ Dallas Lock Linux

Для сигнатур также определены следующие индикаторы состояния:



— сигнатура активирована;



— сигнатура деактивирована.

Для других столбцов значения сигнатур отображаются в соответствии с заданными АИБ значениями.

В данной вложенной категории можно редактировать, активировать, деактивировать, сохранять и загружать сигнатуры журналов.

Для активации / деактивации сигнатуры или нескольких сигнатур необходимо на панели *Действия* нажать кнопку **Активировать** / **Деактивировать** соответственно.

Для просмотра настроенных параметров сигнатур необходимо нажать кнопку **Просмотр** на панели *Действия*, после чего откроется окно редактора сигнатур.

Редактирование сигнатур осуществляется по нажатию кнопки **Редактировать** на панели *Действия*. В открывшемся окне **Редактирование сигнатуры журналов** (рис. 129) можно активировать / деактивировать сигнатуру с помощью тумблера *Активная сигнатура*, а также выставить уровень угрозы для сигнатуры с помощью ползунка *Уровень тревоги* (содержит значения от 1 до 10). Текстовые поля *ID сигнатуры* и *Описание сигнатуры* недоступны для редактирования. Поле *Действие* содержит действие, выполняемое при срабатывании сигнатуры, и содержит единственное значение — *Журналировать*.

Рис. 129. Редактирование сигнатуры журналов для модулей СЗИ Dallas Lock Linux

Для сохранения внесенных изменений необходимо нажать кнопку **Применить**, по нажатию кнопки **Отмена** окно редактора сигнатуры будет закрыто без сохранения внесенных изменений.

Для экспорта сигнатур журналов в файл на панели *Действия* необходимо нажать кнопку **Сохранить**, после чего в появившемся системном окне выбрать директорию для сохранения файла сигнатур журналов.



При сохранении сигнатур в файл экспортируются все сигнатуры с учетом установленного состояния активности и наследования.

Для загрузки сигнатур журналов из файла необходимо нажать кнопку **Загрузить** на панели *Действия*, после чего в появившемся окне выбрать необходимый файл сигнатур журналов.



При загрузке сигнатур журналов из файла все текущие сигнатуры журналов будут удалены, после чего будут применены новые сигнатуры из файла.

Сигнатуры трафика для модулей СЗИ НСД Dallas Lock 8.0-С/К

В рабочей области вложенной категории *Сигнатуры трафика* отображается перечень сигнатур трафика и сведения о них в виде двухуровневого списка (рис. 130): первый уровень списка — фиксированный набор групп сигнатур; второй уровень списка — сигнатуры, входящие в группу.

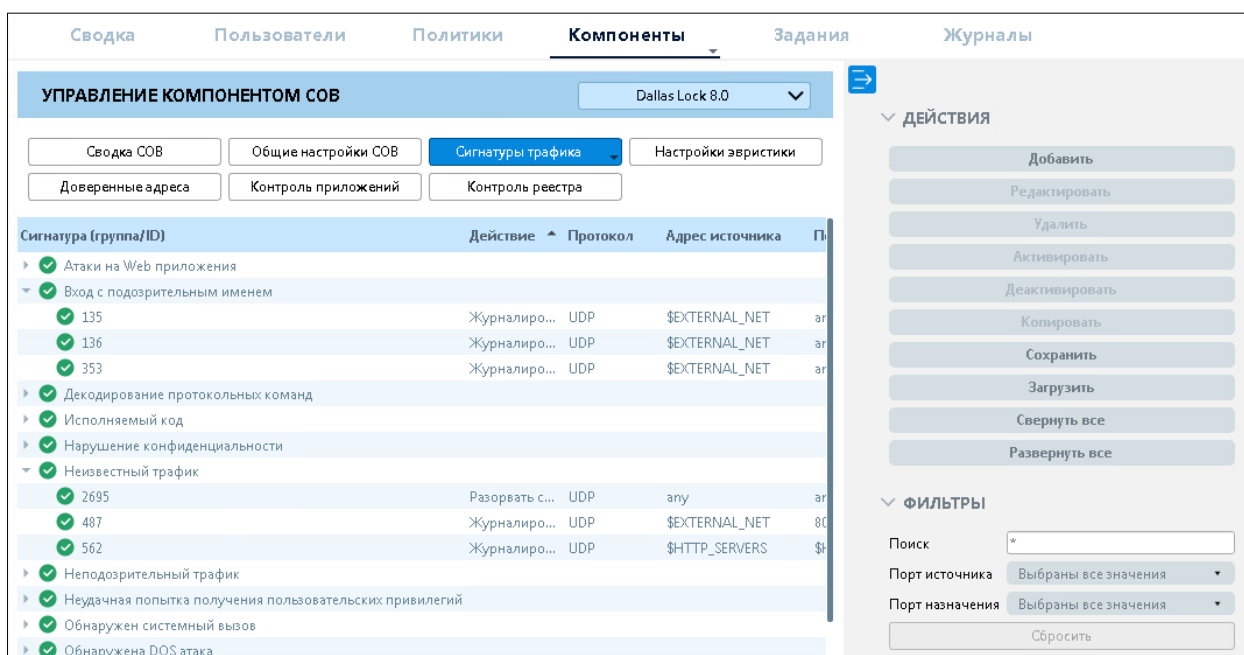


Рис. 130. Категория «Сигнатуры трафика» для модулей СЗИ Dallas Lock 8.0

В столбце *Сигнатура (группа/ID)* помимо названия группы сигнатур или идентификатора сигнатуры отображается также индикатор состояния сигнатур / групп сигнатур. Возможные индикаторы состояния:

-  — сигнатура или вся группа сигнатур активирована;
-  — сигнатура или вся группа сигнатур деактивирована;
-  — активированы не все сигнатуры, входящие в группу.



Столбец *Информация об уязвимости* содержит информацию только для типовых шаблонных сигнатур, недоступен для редактирования.

В данной вложенной категории можно добавлять, редактировать, удалять, активировать, деактивировать, сохранять и загружать сигнатуры трафика с помощью соответствующих кнопок на панели *Действия*. Также для таблицы сигнатур возможно сворачивать и разворачивать все вложенные элементы дерева сигнатур журналов с помощью кнопок **Свернуть все** / **Развернуть все** соответственно.

Для добавления новой сигнатуры трафика на уровне ДБ необходимо:

1. Выбрать ДБ в дереве консоли и перейти на вкладку *Система обнаружения вторжений*. Рядом с наименованием страницы выбрать модуль *Dallas Lock 8.0*.
2. Перейти в категорию *Сигнатуры* → *Сигнатуры трафика* и на панели *Действия* нажать кнопку **Добавить**.
3. На экране появится окно мастера добавления сигнатур трафика (рис. 131). Ввести краткую информацию и выбрать родительские сигнатуры:
 - текстовое поле *ID сигнатуры* — уникальный числовой идентификатор сигнатуры. Поле недоступно для редактирования, номер присваивается автоматически, начиная со значения *100 001*;
 - текстовое поле *Сообщение* — текст, который будет содержаться в инциденте при срабатывании создаваемой сигнатуры. Параметр может быть неуникальным;
 - выпадающий список *Действие* — содержит следующие значения: *Журналировать*, *Разорвать соединение*, *Разорвать соединение и заблокировать адрес*. По умолчанию установлено значение *Журналировать*;
 - выпадающий список *Направление* — содержит следующие значения: *Входящий трафик*

соединения, *Входящий и исходящий трафик соединения*. По умолчанию установлено значение *Входящий трафик соединения*;

- выпадающий список *Группа* с возможностью поиска и выпадающим списком результатов поиска — поле позволяет найти или выбрать из выпадающего списка родительскую группу для создаваемой сигнатуры (набор групп сигнатур фиксированный). Поле обязательно для заполнения, по умолчанию поле содержит следующие значения:
 - *Прочие атаки* — если перед нажатием кнопки **Добавить** на панели действий категории *Сигнатуры трафика* не было выбрано ни одной группы сигнатур из списка;
 - имя группы сигнатур, которая была выбрана из списка перед нажатием кнопки **Добавить** на панели действий категории *Сигнатуры трафика*.

Рис. 131. Мастер добавления сигнатур трафика

4. Выбрать протокол и установить необходимые порты и IP-адреса, после чего нажать кнопку **Далее**.
5. Выбрать объекты дерева, для которых создаваемая сигнатура будет активна. Нажать кнопку **Далее**.
6. Добавить ключевые слова, байтовую последовательность или маску, которые должны содержаться в проходящем сетевом трафике для срабатывания. Для перехода на следующий шаг мастера добавления сигнатуры нажать кнопку **Далее**.
7. После откроется окно значений параметров создаваемого правила. Для завершения нажать кнопку **Готово**.

Для редактирования сигнатур требуется выбрать в рабочей области сигнатуру / группу сигнатур и нажать на панели *Действия* кнопку **Редактировать**, после в открывшемся окне **Редактирование сигнатуры трафика** (рис. 132) произвести необходимые настройки и нажать кнопку **Применить**.

Рис. 132. Окно редактора сигнатур трафика для модулей СЗИ Dallas Lock 8.0



Редактировать можно как пользовательские сигнатуры, так и типовые шаблоны сигнатур, но для типовых шаблонов сигнатур раздел *Содержимое* для редактирования недоступен.

Сигнатуры трафика для модулей СЗИ НСД Dallas Lock Linux

В рабочей области вложенной категории *Сигнатуры трафика* отображается перечень сигнатур трафика и сведения о них в виде таблицы со столбцами *Описание*, *ID сигнатуры*, *Уровень тревоги* и *Действие* (рис. 133).

Описание	ID сигнатуры	Уровень тревоги	Действие
✓ A03:2021 HTML инъекция - Отражение (GET) (WAFDL)	2001	2	
✓ A03:2021 SQL Инъекция (GET/Search) (WAFDL)	2002	2	
✓ A03:2021 Внедрение Комманд ОС (WAFDL)	2003	2	
✓ A03:2021 PHP Инъекция Кода (WAFDL)	2004	2	
✓ Внедрение На Стороне Сервера (SS) Тестовая-Инъекция (WAFDL)	2005	2	
✓ XXS - Отражение (GET) (WAFDL)	2006	2	
✓ A01:2021 Обход Каталогов — Каталоги (WAFDL)	2007	2	
✓ A01:2021 Удаленное и Локальное Включение Файлов (RFI/LFI) (WAFDL)	2008	2	
✓ A05:2021 XML-Атаки на внешние объекты (XXE) (WAFDL)	2009	2	
✓ Уязвимость Shellshock (CGI) (WAFDL)	2010	2	
✗ RCE 1.1 bypass (WAFDL)	25000	2	
✗ RCE 1.2 bypass (WAFDL)	25001	2	
✗ RCE 2.1 bypass (WAFDL)	25002	2	
✗ RCE 2.2 bypass (WAFDL)	25003	2	
✗ RCE 3.1 bypass (WAFDL)	25004	2	

Рис. 133. Категория «Сигнатуры трафика» для модулей СЗИ Dallas Lock Linux

В столбце *Описание* помимо описания сигнатуры отображается также индикатор состояния сигнатуры. Возможные индикаторы состояния:

-  — сигнатура активирована;
-  — сигнатура деактивирована.

В данной вложенной категории можно редактировать, активировать, деактивировать, сохранять и загружать сигнатуры трафика.

Для активации / деактивации сигнатуры или нескольких сигнатур необходимо на панели *Действия* нажать кнопку **Активировать / Деактивировать** соответственно.

Для просмотра настроенных параметров сигнатур необходимо нажать кнопку **Просмотр** на панели *Действия*, после чего откроется окно редактора сигнатур.

Редактирование сигнатур осуществляется по нажатию кнопки **Редактировать** на панели *Действия* или по двойному щелчку на выбранной сигнатуре. В открывшемся окне **Редактирование сигнатуры трафика** (рис. 134) можно активировать / деактивировать сигнатуру с помощью тумблера *Активная сигнатура*, выставить уровень угрозы для сигнатуры с помощью ползунка *Уровень тревоги* (содержит значения от 1 до 10), а также выбрать при помощи выпадающего списка *Действие* действие, выполняемое при срабатывании сигнатуры. Текстовые поля *ID сигнатуры* и *Описание сигнатуры* недоступны для редактирования.

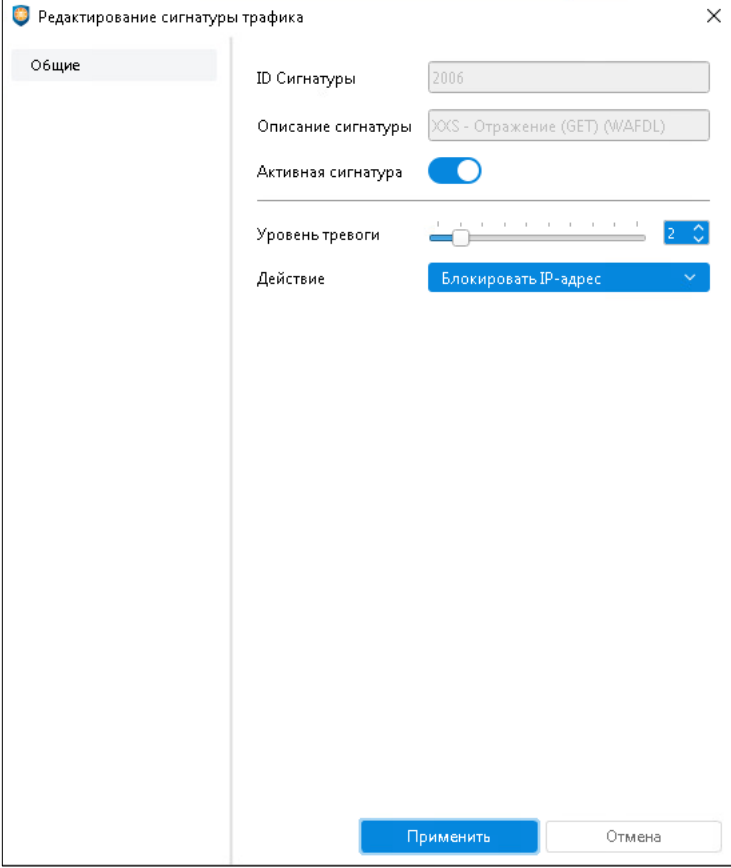


Рис. 134. Окно редактора сигнатуры трафика для модулей СЗИ Dallas Lock Linux

Для сохранения внесенных изменений необходимо нажать кнопку **Применить**, по нажатию кнопки **Отмена** окно редактора сигнатуры будет закрыто без сохранения внесенных изменений.

Для экспорта сигнатур журналов в файл на панели *Действия* необходимо нажать кнопку **Сохранить**, после чего в появившемся системном окне выбрать директорию для сохранения файла сигнатур журналов.



При сохранении сигнатур в файл экспортируются все сигнатуры с учетом установленного состояния активности и наследования.

Для загрузки сигнатур журналов из файла необходимо нажать кнопку **Загрузить** на панели *Действия*, после чего в появившемся окне выбрать необходимый файл сигнатур журналов.



При загрузке сигнатур журналов из файла все текущие сигнатуры журналов будут удалены, после чего будут применены новые сигнатуры из файла.

Сигнатуры: переменные трафика

В рабочей области вложенной категории *Сигнатуры: переменные трафика* список переменных трафика и их значений отображается в виде таблицы. Данный список представлен следующими столбцами **Переменная** и **Значение**.



Категория *Сигнатуры: переменные трафика* позволяет задать сетевые адреса внутренней и внешней сети, серверы, TCP- и UDP-порты, используемые в сети, а также группировать эти переменные, чтобы затем использовать в настройках сигнатур трафика. При изменении значения переменной любая сигнатура, которая использует данную переменную, обновится в соответствии с новым значением переменной.

Переменные бывают двух типов — переменные диапазона адресов и переменные диапазона портов.

Переменные диапазона адресов отображаются зеленым цветом текста, переменные диапазона портов — синим цветом текста.

Список переменных по умолчанию содержит типовые шаблоны переменных трафика:

- HOME_NET — в данной переменной задается диапазон внутренних IP-адресов. Переменная находится первой в списке.
- EXTERNAL_NET — в данной переменной задается диапазон внешних IP-адресов. Переменная находится второй в списке.
- Переменные SERVERS — группа переменных для настройки IP-адресов серверов.
- Переменные PORTS — в данной переменной задаются порты.
- DL_SUSPICIOUS_PORTS — переменная эвристики Сканирование подозрительных TCP портов, находится в конце списка.
- DL_UNUSED_SERVICE_PORTS — переменная эвристики Сканирование неиспользуемых служебных TCP портов, находится в конце списка.

В данной категории можно добавлять, редактировать и удалять переменные трафика, а также восстанавливать список переменных трафика по умолчанию.



Нельзя удалять переменные, которые используются в значениях других переменных, а также переменные эвристики **DL_SUSPICIOUS_PORTS** и **DL_UNUSED_SERVICE_PORTS**. При попытке удаления подобных переменных будет выведено соответствующее сообщение об ошибке.



Для восстановления списка переменных трафика по умолчанию следует нажать кнопку **По умолчанию** на панели *Действия*, после чего для шаблонов переменных будут выставлены значения по умолчанию, все пользовательские переменные будут удалены.

Для добавления переменной трафика следует нажать кнопку **Добавить** на панели *Действия*, после чего откроется окно **Создание переменной трафика** (рис. 135), содержащее следующие параметры для настройки:

- текстовое поле *Переменная* — название переменной, является уникальным параметром. По умолчанию присваивается имя «USER_VARIABLE#№», где № — порядковый номер, начинающийся с 1;
- переключатель *Тип* — выбор типа переменной трафика, содержит значения *Адрес* и *Порт*;

- переключатель *Список переменных*;
- текстовое поле *Значение* с выпадающим списком — предназначено для ввода значения переменной или для выбора значения из списка переменных.

Рис. 135. Окно создания переменной трафика

Для сохранения новой переменной трафика необходимо нажать кнопку **Применить**, при нажатии на кнопку **Отмена** окно создания пользовательской переменной трафика будет закрыто без создания новой переменной.



Добавленные новые переменные попадают в конец списка, но перед переменными эвристики.

Редактирование переменных трафика осуществляется через окно **Редактирование переменной трафика**. Редактор запускается нажатием кнопки **Редактировать** на панели *Действия* или двойным кликом по выбранной переменной трафика.



Редактировать можно любые переменные трафика, кроме переменных эвристик *DL_SUSPICIOUS_PORTS* и *DL_UNUSED_SERVICE_PORTS*.

5.8.4 Настройки эвристики

На вкладке **Управление компонентом COB** в категории **Настройки эвристики** регулируются настройки эвристического анализа. Рабочая область категории содержит в виде таблицы список атак и глобальные настройки эвристики, а также их значения (рис. 136).

Политика	Значение	Тип модуля
Атака: ARP spoofing/poisoning	Выкл	DL 8.0 (IK12)
Атака: DHCP-атаки	Выкл	DL 8.0 (IK12)
Атака: ICMP flood	Выкл	DL 8.0 (IK12)
Атака: IP spoofing	Выкл	DL 8.0 (IK12)
Атака: Open Tear	Выкл	DL 8.0 (IK12)
Атака: Short Headers	Выкл	DL 8.0 (IK12)
Атака: Smurf	Выкл	DL 8.0 (IK12)
Атака: Teardrop (для ICMP протокола)	Выкл	DL 8.0 (IK12)
Атака: Аномальная сетевая активность	Выкл	DL 8.0 (IK12)
Атака: Защита от DDoS-атаки (защита от флуда)	Выкл	DL 8.0 (IK12)
Атака: Перекрытие заголовков	Выкл	DL 8.0 (IK12)
Атака: Сканирование неиспользуемых служебных TCP портов	Выкл	DL 8.0 (IK12)
Атака: Сканирование подозрительных TCP портов	Выкл	DL 8.0 (IK12)
Атака: Сканирование портов	Выкл	DL 8.0 (IK12)
Исключения для сканирования портов (перечень)	138, 139, 445	DL 8.0 (IK12)
Объем трафика за 10 мин., для определения аномальной сетевой активности	2.0 Гб	DL 8.0 (IK12)
Продолжительность атаки (сек)	20	DL 8.0 (IK12)
Сканирование неиспользуемых TCP портов (перечень)	80, 53, 21, 25, 110, 3306, 22, 4899, 443	DL 8.0 (IK12)
Сканирование подозрительных TCP портов (перечень)	1080, 12345, 2773, 2774, 5877, 6713, 8787, 16959, 30003, 31337, 54283, 54321, 60000	DL 8.0 (IK12)
Чувствительность сканирования портов	5	DL 8.0 (IK12)

Рис. 136. Категория «Настройки эвристики»

Список настроек эвристики меняется в зависимости от того, управление каким модулем было выбрано.

Для редактирования настроек эвристики необходимо для выбранной в таблице политики нажать кнопку **Свойства** на панели **Действия**.



При инициировании команды *Запустить процесс обновления COB* на вкладке **Сводка COB** происходит обновление настроек эвристики (все политики, кроме атак) COB модулей **СИ Dallas Lock 8.0-К/С** для всего ДБ, предоставляемых компанией ООО «Конфидент».

При этом на уровне ДБ меняются значения политик, которые не были настроены пользователем.

5.8.5 Доверенные адреса

На вкладке **Управление компонентом COB** в категории **Доверенные адреса** для модулей **СИ Dallas Lock 8.0-К/С** отображаются доверенные IP- и MAC-адреса, а также сведения о них (рис. 137).

Адреса	Комментарий	Отметка в журнале
✓ 10.10.100.90	test_1	Выкл
✓ 10.10.100.91		Выкл

Рис. 137. Категория «Доверенные адреса»

Для добавления доверенного адреса в таблицу необходимо нажать кнопку **Добавить** на панели **Действия**, после чего в открывшемся окне **Добавление доверенного адреса COB** заполнить необходимые данные (рис. 138).

Рис. 138. Окно добавления доверенного адреса

Редактирование выбранного адреса из списка осуществляется по нажатию кнопки **Редактировать** на панели *Действия* или по двойному клику на выбранный адрес. Окно редактора доверенных адресов аналогично окну добавления (рис. 138).

Для удаления адреса необходимо выбрать адрес в таблице и нажать кнопку **Удалить** на панели *Действия*, после чего подтвердить удаление. Можно выбрать несколько адресов одновременно.

5.8.6 Контроль приложений

На вкладке **Управление компонентом COB** в категории **Контроль приложений** для модуля **СЗИ Dallas Lock 8.0-K/C** регулируются настройки контроля приложений для обнаружения аномалий в поведении приложений и ОС для всего ДБ (рис. 139).

В рабочей области категории отображается список правил контроля приложений и сведения о них в виде таблицы.

Сводка Пользователи Политики Компоненты Задания Журналы						
УПРАВЛЕНИЕ КОМПОНЕНТОМ COB						
Dallas Lock 8.0						
Сводка COB Общие настройки COB Сигнатуры Настройки эвристики						
Доверенные адреса Контроль приложений Контроль реестра						
№	Описание	Маски пути	Пользователи и группы	Уровень доступа	Уровень журналирования	
1	Системные приложения	%systemroot%\System32\lsass.exe; %systemroot%\System32\conhost.exe; %systemroot%\...		Все уровни	Наследуется	
2	Web-браузеры	%SystemDrive%\Users\AppData\Local\Programs\Opera\Opera.exe; %SystemDrive%\Users\...		Все уровни	Наследуется	
3	Офисный пакет приложений	%PROGRAMFILES%\Microsoft Office\root\Office10\EXCEL.exe; %PROGRAMFILES%\Micros...		Все уровни	Наследуется	
4	Программное обеспечение	%PROGRAMFILES%\totalcmd\TOTALCMD64.EXE; %PROGRAMFILES%\Adobe\Acrobat ...		Все уровни	Наследуется	
По умолчанию	Подписанные приложения				Уровни: 5; Аудит успеха; Аудит отказа	
По умолчанию	Неподписанные приложения				Уровни: 5; Аудит успеха; Аудит отказа	
По умолчанию	Приложения по умолчанию				Уровни: 5; Аудит успеха; Аудит отказа	

Рис. 139. Категория «Контроль приложений»

Список правил контроля приложений содержит следующие типы правил:

- глобальные правила — правила, задающее глобальные настройки по умолчанию для приложений;
- пользовательские правила — правила, созданные администратором безопасности, имеющие точечные настройки. Могут наследовать параметры глобальных правил по умолчанию и имеют самый высокий приоритет. В группу пользовательских правил также входят четыре предустановленных правила, необходимые для корректной работы операционной системы и прикладного программного обеспечения: системные приложения, web-браузеры, офисный пакет приложений, программное обеспечение.



В столбце № для пользовательских правил отображается номер приоритета и индикатор активности правила. Индикаторы состояния могут принимать следующий вид:

-  — правило активировано и все значения для системных функций установлены в *Разрешено*;
-  — правило активировано и все значения для системных функций установлены в *Запрещено*;
-  — правило активировано, но не все значения для системных функций выставлены в *Разрешено* или *Запрещено*;
-  — правило деактивировано.



Номер приоритета присваивается каждому новому правилу автоматически, добавляя его в конец списка, где 1 — наивысший приоритет правила. Поменять приоритет правила можно при помощи кнопок **Увеличить приоритет** и **Уменьшить приоритет** на панели *Действия*.

Для глобальных правил столбец № отображает состояние правила.

Для остальных столбцов таблицы значения отображаются в соответствии с заданными администратором безопасности значениями.

Для применения изменений на модулях необходима синхронизация.

В данной категории можно добавлять, редактировать, удалять, активировать, деактивировать, понижать или повышать приоритет правил контроля приложений.



Приоритеты правил контроля приложений представляют собой следующую иерархию:

- пользовательские правила имеют самый высокий приоритет;
- глобальные правила по умолчанию для подписанных и неподписанных приложений имеют средний приоритет;
- глобальное правило для приложений по умолчанию имеет самый низкий приоритет.

При нажатии кнопки **Добавить** открывается окно для добавления пользовательского правила контроля приложений **Добавление правила контроля приложений** (рис. 140).

Рис. 140. Окно «Добавление правила контроля приложений»

На вкладке *Общие* предлагается заполнить основные данные и параметры, относящиеся к правилам контроля приложений:

- текстовое поле *Описание правила* — название правила (параметр является обязательным, может быть неуникальным);

- тумблер *Активное правило*;
- таблица для добавления приложений, на которые распространяется правило — содержит следующие столбцы: **Путь**, **Параметры запуска**. Обязательна для заполнения, в рамках одного правила в таблице не может содержаться одинаковых директорий приложений;
- кнопки **Добавить**, **Изменить** и **Удалить** — позволяют управлять таблицей с приложениями:
 - кнопка **Добавить** — открывает окно для добавления пути и параметров запуска приложения;
 - кнопка **Изменить** — открывает окно для изменения пути и параметров запуска выбранного приложения;
 - кнопка **Удалить** — позволяют удалять указанное приложение;
- таблица с настройкой системных функций приложений — позволяет для перечисленных системных функций приложения управлять доступом. Содержит следующие столбцы:
 - столбец с чекбоксами — управляет значениями в столбце **Доступ**. В шапке таблицы для данного столбца содержится высокоуровневый чекбокс, позволяющий управлять значениями всех чекбоксов таблицы;
 - столбец **Доступ** — отображает значения в зависимости от установленного состояния чекбокса. Содержит следующие значения:
 - «Разрешено» — для системной функции приложения доступ разрешен, ячейка окрашена в зеленый цвет;
 - «Запрещено» — для системной функции приложения доступ запрещен, ячейка окрашена в красный цвет;
 - «Наследуется» — для системной функции приложения значение доступа наследуется одновременно от глобального правила для подписанных приложений и от глобального правила для неподписанных приложений;

Если в столбце **Доступ** определено значение *Наследуется*, ячейка со значением может быть окрашена в следующие цвета:



- зеленый — от глобальных правил для подписанных и неподписанных приложений одновременно наследуется значение *Разрешено*;
- красный — от глобальных правил для подписанных и неподписанных приложений одновременно наследуется значение *Запрещено*;
- синий — от глобальных правил для подписанных и неподписанных приложений наследуются разные значения.

- *Системные функции приложения* — столбец с фиксированным набором системных функций приложения.

На вкладке *Аудит* предлагается заполнить параметры, относящиеся к аудиту событий безопасности:

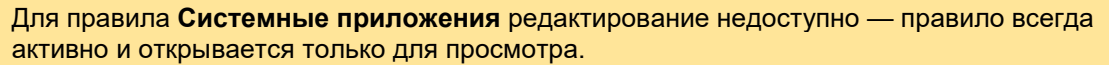
- чекбокс *Наследовать* — позволяет одновременно наследовать параметры Аудита от глобального правила для подписанных приложений и от глобального правила для неподписанных приложений. При включенном чекбоксе остальные параметры Аудита недоступны для редактирования. По умолчанию чекбокс активирован;
- ползунок *Уровень журналирования* — установленный уровень журналирования для событий успеха и отказа при срабатывании правила. Содержит значения от 1 до 10, значение по умолчанию: 5;
- чекбоксы *Аудит успеха* и *Аудит отказа* — позволяют выбрать, какие события подлежат аудиту. По умолчанию чекбоксы активированы.

На вкладке *Пользователи* отображается список пользователей, к которым будет применяться созданное правило. Реализована возможность выбора мандатных уровней доступа пользователей, для которых будет применено правило.

Для сохранения нового правила необходимо нажать кнопку **Применить**, для отмены всех внесенных изменений без сохранения нового правила — **Отмена**.

Функциональная возможность редактирования правил контроля приложений в консоли **ЕЦУ** осуществляется через окно редактора правил контроля приложений. Редактор запускается по нажатию кнопки **Редактировать** на панели *Действия* или по двойному клику на строку с правилом.

Интерфейс и набор параметров редактора пользовательского правила аналогичны интерфейсу и набору параметров окна **Добавление правила контроля приложений** (рис. 140).



Для редактирования глобальных правил доступны разделы *Общие* и *Аудит* (рис. 141). В разделе *Общие* можно управлять доступом для перечисленных системных функций приложения. Настройка параметров в разделе *Аудит* производится аналогично настройке параметров для пользовательских приложений.

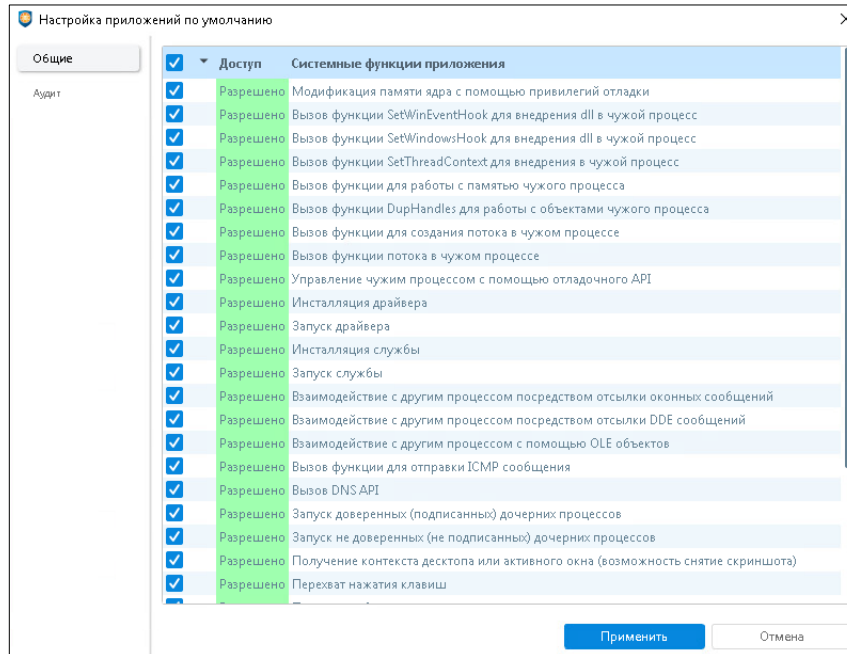
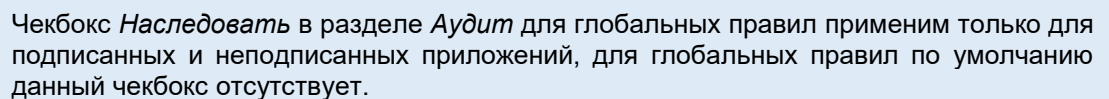


Рис. 141. Редактор глобальных правил по умолчанию



Функциональная возможность редактирования пользовательских правил контроля приложений в консоли **ЕЦУ** осуществляется через окно редактора **Настройки правила контроля приложений**. Редактор запускается по нажатию кнопки **Редактировать** на панели *Действия* или по двойному клику на строку с правилом. Интерфейс и набор параметров редактора пользовательского правила аналогичны интерфейсу и набору параметров окна **Добавление правила контроля приложений** (рис. 140).

Редактирование глобальных правил контроля приложений в консоли **ЕЦУ** осуществляется через отдельное окно редактора (рис. 141), запускаемого при помощи кнопки **Редактировать** или по двойному щелчку на строку с правилом.

5.8.7 Контроль реестра

Категория **Контроль реестра** (рис. 142) на вкладке **Управление компонентом СОВ** позволяет для модулей **СЗИ Dallas Lock 8.0-К/С** ограничивать попытки ПО изменять в системном реестре настройки критических объектов ОС.

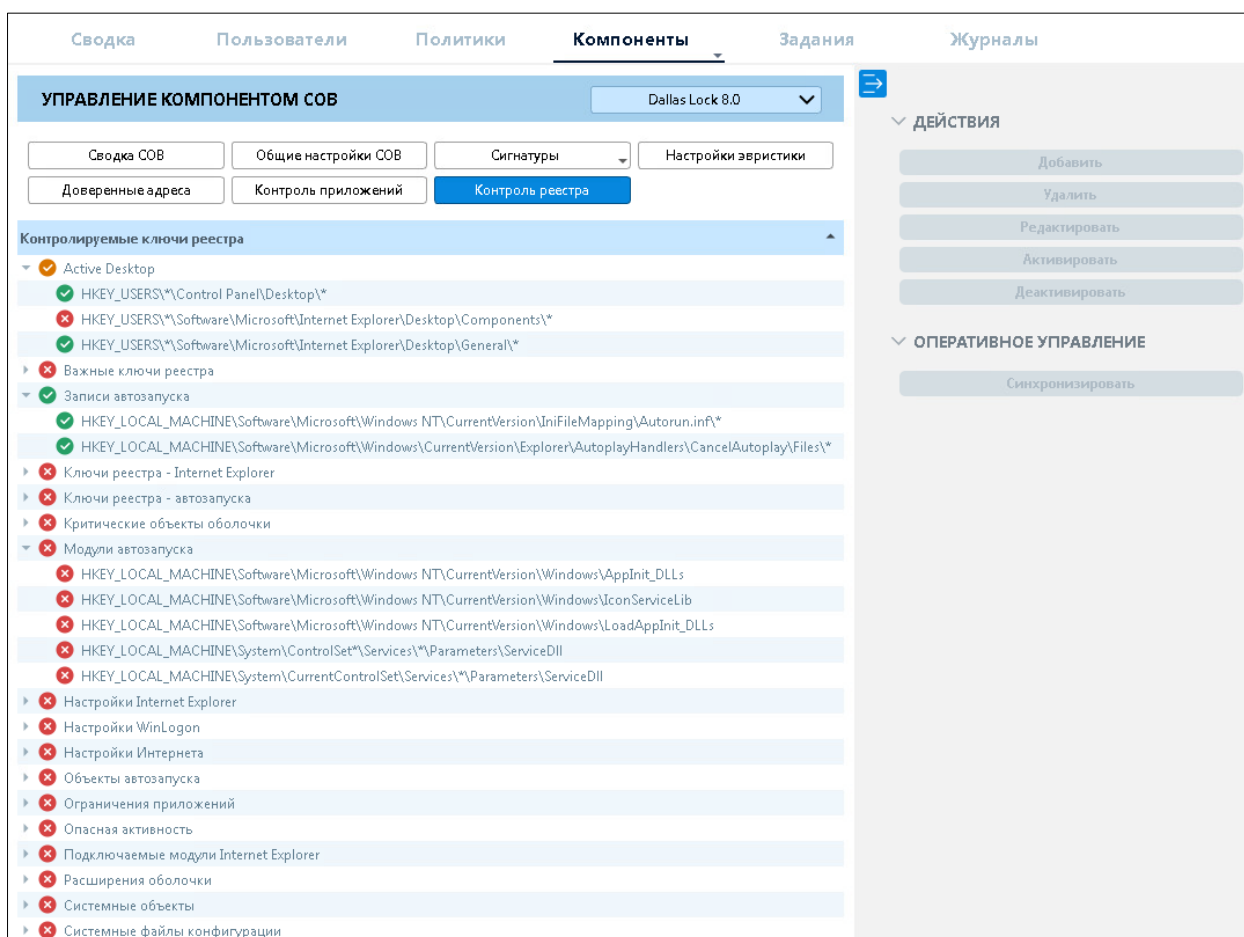


Рис. 142. Категория «Контроль реестра»

Рабочая область категории **Контроль реестра** содержит перечень контролируемых ключей реестра в виде двухуровневого списка: первый уровень списка — фиксированный набор групп контролируемых ключей, второй уровень списка — ключи реестра, входящие в группу. Данный список содержит название группы контролируемых ключей или название одиночного ключа реестра с индикатором состояния. Индикаторы состояния на уровне ДБ могут принимать следующий вид:

-  — ключ реестра или вся группа ключей активирована;
-  — ключ реестра или вся группа ключей деактивирована;
-  — активированы не все ключи, входящие в группу.

В данной категории можно просматривать, добавлять, редактировать, удалять, активировать и деактивировать ключи реестра. Также на уровне группы, подгруппы, АРМ и модулей **СЗИ DallasLock 8.0-К/С** доступна настройка наследования состояния активности ключа реестра с верхнего уровня домена.

При нажатии кнопки **Добавить** открывается окно добавления нового контролируемого ключа реестра, содержащее следующие параметры:

- текстовое поле **Ключ реестра** — ввод маски ключа или ветки реестра;
- тумблер **Активировать ключ**;
- кнопка, позволяющая открыть проводник для выбора ветки реестра;
- кнопка **Применить** — позволяет добавить новый выбранный ключ;
- кнопка **Отмена** — закрывает окно без сохранения.

Редактирование ключа реестра запускается нажатием кнопки **Редактировать** или по двойному клику на ключ реестра, после чего открывается окно, аналогичное окну добавления ключа реестра.

5.9 Безопасная среда COB (песочница)

Для перехода к разделу настроек **Управление параметрами безопасной среды COB** необходимо на вкладке **Компоненты** выбрать **Безопасная среда COB (песочница)**. На странице **Управление параметрами безопасной среды COB** можно настраивать параметры безопасной среды COB для модулей **СЗИ НСД Dallas Lock 8.0** (рис. 143).

Более подробно о Безопасной среде COB (песочнице) описано в Руководстве по эксплуатации **СЗИ Dallas Lock 8.0** раздел 16.6.

Сводка	Пользователи	Политики	Компоненты	Задания	Журналы
УПРАВЛЕНИЕ ПАРАМЕТРАМИ БЕЗОПАСНОЙ СРЕДЫ COB			Межсетевой экран		
Политика ▲ Значение			Система контроля накопителей		
Автоматическая очистка по завершении всех процессов			Контроль ресурсов		
Автоматический запуск приложений в БС			Система обнаружения вторжений		
Безопасная среда			Безопасная среда COB (песочница)		
Возможность перенести изменения из БС в систему			Средство обнаружения и реагирования		
Всегда запускать в Безопасной среде					
Доверенное расположение					
Контроль приложений					
Настройки эвристики БС					
Отчет по завершении работы процесса БС					
Порог срабатывания эвристики					
Файловая система и реестр					
Эвристический анализ для блокировки работы опасных процессов					

Рис. 143. Вкладка «Безопасная среда COB (песочница)»

ЕЦУ позволяет настраивать следующие политики безопасной среды:

Таблица 24. Настройки безопасной среды COB

Автоматическая очистка по завершении всех процессов
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Политика позволяет определить, будет ли производиться автоматическая очистка временных каталогов от содержимого, созданного процессом или процессами, запущенными в безопасной среде.
Автоматический запуск приложений в БС
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Выкл.». Политика позволяет автоматически запускать в безопасной среде исполняемые файлы и приложения, ассоциированные с неисполняемыми файлами, а также файлы, запускаемые из недоверенных источников. Доверенные источники указываются в политике Доверенное расположение .
Безопасная среда
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Политика позволяет управлять включением и отключением Безопасной среды COB на модулях СЗИ Dallas Lock 8.0-K/C .
Возможность перенести изменения из БС в систему
Возможное значение политики: «Вкл./Выкл.». По умолчанию значение данной политики: «Вкл.». Политика позволяет пользователю отключить сохранение результатов работы процесса, запущенного в безопасной среде. Если данный параметр включен, перед сохранением пользователю будет выведено диалоговое окно с вопросом на сохранение изменений, выполненных завершенным процессом.
Всегда запускать в Безопасной среде
Политика позволяет настраивать пути до приложений, которые необходимо принудительно запускать в Безопасной среде. По умолчанию значение данной политики: «Не используется».
 Не рекомендуется добавлять в данный список системные приложения, так как принудительный запуск в Безопасной среде системных приложений или приложений, которые затрагивают критические системные функции, приведет операционную систему к неработоспособности.

Доверенное расположение	
Политика позволяет через соответствующие разделы настраивать список доверенных директорий и список доверенных носителей информации.	
Контроль приложений	
Политика позволяет настроить правила контроля приложений Безопасной среды. При инициировании команды <i>Добавить</i> открывается отдельное окно Добавление правила контроля приложений безопасной среды СОВ , содержащее 2 раздела:	
• Общие — отвечает за управление доступом для системных функций приложения; • Аудит — отвечает за настройку уровня журналирования при срабатывании правила, а также за выбор того, какие события подлежат аудиту (Аудит успеха и Аудит отказа).	
Настройки эвристики БС	
Политика позволяет настраивать весовые значения правил эвристики.	
	Настройка данной политики зависит от установленного значения политики Эвристический анализ для блокировки работы опасных процессов :
	• если для политики Эвристический анализ для блокировки работы опасных процессов установлено значение <i>Включен</i>, то политика Настройки эвристики БС недоступна даже для просмотра;
	• если для политики Эвристический анализ для блокировки работы опасных процессов установлено значение <i>Режим с настройками по умолчанию</i>, то политика Настройки эвристики БС доступна для просмотра;
	• если для политики Эвристический анализ для блокировки работы опасных процессов установлено значение <i>Режим ручной настройки</i>, то политика Настройки эвристики БС доступна для редактирования.
Отчет по завершении работы процесса БС	
Политика позволяет настроить функцию формирования отчета по завершении работы процесса в БС, а также указать каталог для хранения отчетов БС.	
Порог срабатывания эвристики	
Возможное значение политики: от 0 до 1000. По умолчанию значение данной политики: «100».	
Политика является накопительным счетчиком весов срабатываний правил эвристики, по достижении значения которого приложение, запущенное в Безопасной среде СОВ, будет принудительно завершено.	
	Редактирование данного параметра разрешено только в случае, когда для политики Эвристический анализ для блокировки работы опасных процессов установлено значение <i>Режим ручной настройки</i> . В ином случае при попытке открыть редактор политики Порог срабатывания эвристики появится соответствующее сообщение об ошибке.
Файловая система и реестр	
Политика позволяет настраивать недоступные на чтение и запись каталоги, полный доступ к каталогам, недоступные на чтение и запись ветки реестра и полный доступ к веткам реестра путем добавления добавления пути в соответствующий список.	
Эвристический анализ для блокировки работы опасных процессов	
Возможное значение политики: « <i>Выключен</i> », « <i>Режим ручной настройки</i> », « <i>Режим с настройками по умолчанию</i> ». По умолчанию значение данной политики: « <i>Выключен</i> ».	
Политка позволяет разрешить безопасной среде применять эвристический анализ для принудительного завершения работы опасных процессов согласно настройкам эвристического анализа, указанным в политике Настройки эвристики БС .	

5.10 Средство обнаружения и реагирования

Для перехода к разделу настроек **Управление компонентом СОР** необходимо на вкладке **Компоненты** выбрать **Средство обнаружения и реагирования**. На странице **Управление компонентом СОР** можно редактировать параметры на уровне всего ДБ, после синхронизации на всех подчиненных объектах в ДБ применяются установленные настройки (рис. 144).

Более подробно о Средстве обнаружения и реагирования описано в Руководстве по эксплуатации **СЗИ Dallas Lock 8.0** раздел 16.7 и в Руководстве по эксплуатации **Dallas Lock Linux** раздел 4.13.

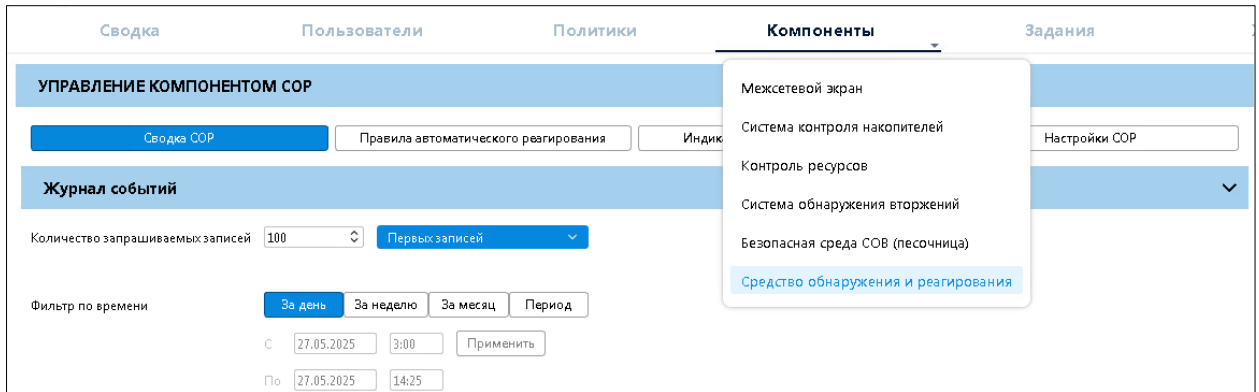


Рис. 144. Вкладка «Средство обнаружения и реагирования»

5.10.1 Сводка СОР

На вкладке **Управление компонентом СОР** в категории **Сводка СОР** отображается информация о событиях по сканированию систем на индикаторы компрометации с клиентов для всего ДБ (рис. 145).

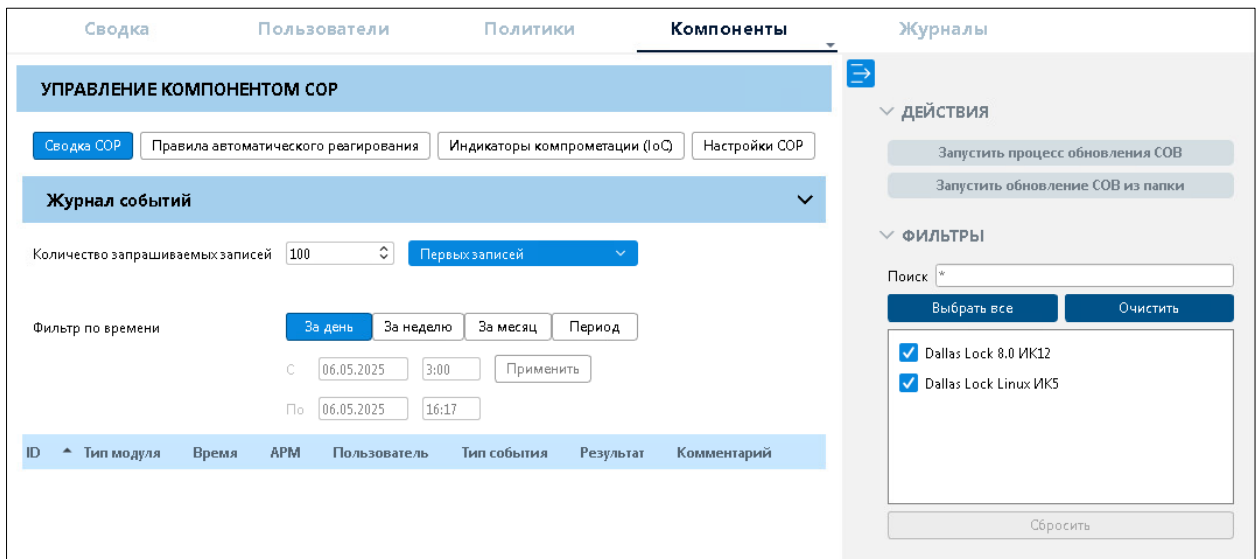


Рис. 145. Категория «Сводка СОР»

На панели **Фильтры** для собираемых записей журналов можно настроить фильтрацию по имени параметра и по типу модулей.

Также для категории **Сводка СОР** предусмотрена возможность обновления базы IoC-объектов через команды **Запустить процесс обновления СОВ** и **Запустить обновление СОВ из папки**.

При запуске команды **Запустить процесс обновления СОВ** открывается окно **Обновление базы решающих правил компонента СОВ** (рис. 119) с добавленной операцией **Обновление базы индикаторов компрометации** (рис. 146).

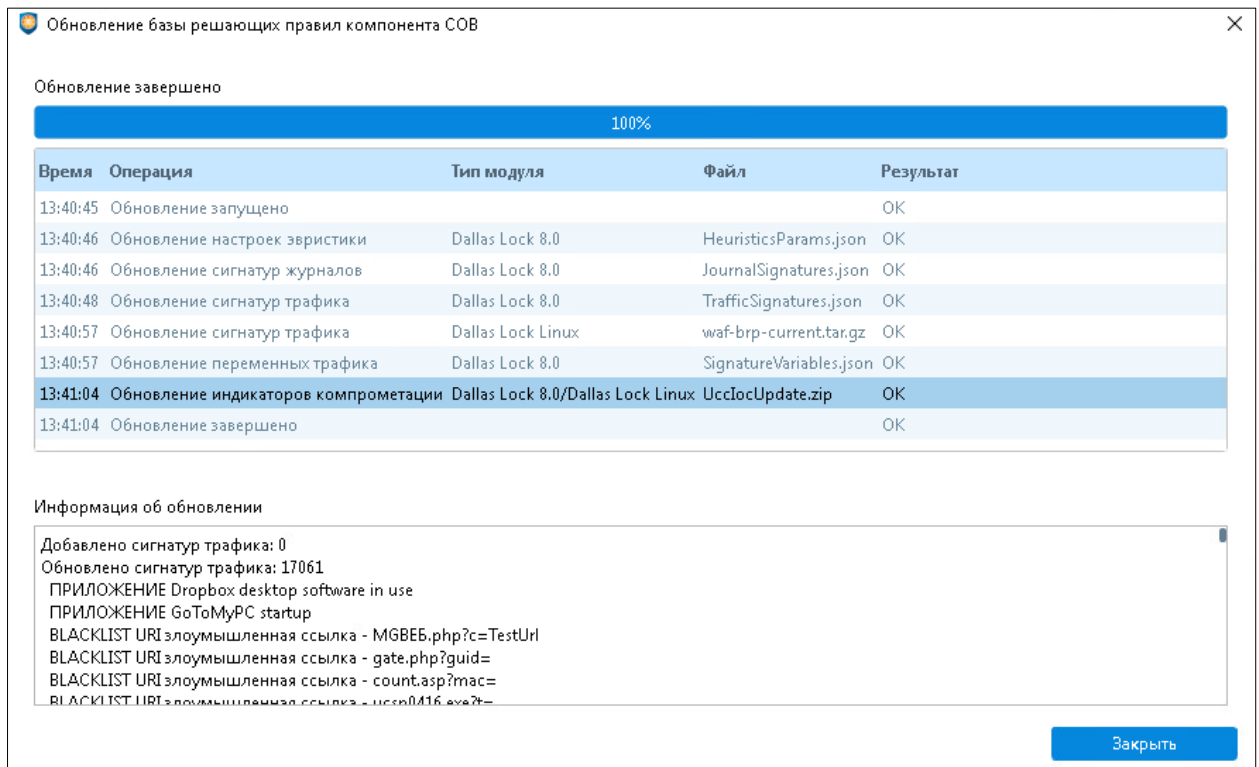


Рис. 146. Обновление базы решающих правил компонента COB для категории «Сводка СОР»

При запуске команды *Запустить обновление COB из папки* открывается системное окно ОС для выбора источника обновления.

Обновление базы IoC-объектов может включать в себя:

- обновление списка IoC-объектов: новые IoC-объекты добавляются, неактуальные — удаляются;
- обновление содержимого IoC-объектов: при необходимости содержимое существующих IoC-объектов может дорабатываться;
- обновление списка IoC-объектов DL8.0 и DLL.



Если при обновлении базы IoC-объектов новый IoC-объект имеет такой же ID, что и уже существующий пользовательский IoC-объект, то новый IoC-объект заменяет собой имеющийся.



IoC-объекты из группы *Стандартные*, которые не были включены в обновление (не были получены с сервера dallaslock.ru/Update при обновлении), будут удалены как неактуальные.

5.10.2 Правила автоматического реагирования

В категории **Правила автоматического реагирования** на вкладке *Система обнаружения и реагирования* производится настройка правил автоматического реагирования СОВ (рис. 147).

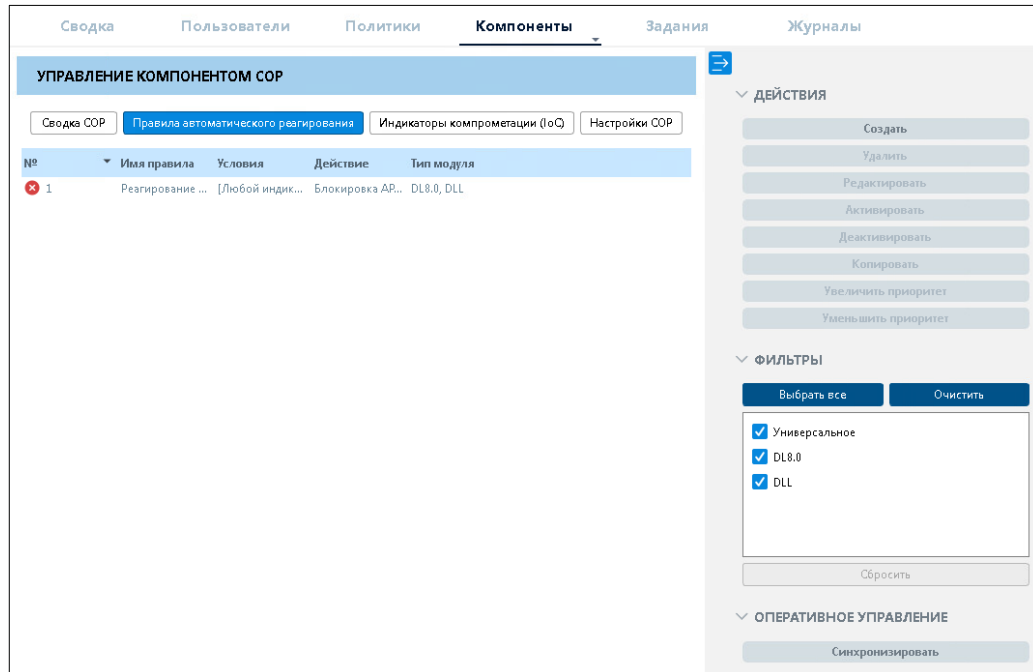


Рис. 147. Категория «Правила автоматического реагирования»

Список правил автоматического реагирования для модулей **СЗИ НСД Dallas Lock 8.0** и **СЗИ НСД Dallas Lock Linux** на уровне ДБ представляет собой таблицу с полями:

1. «№» — столбец с идентификационным номером строки правила и с индикатором активности правила. Может содержать следующие индикаторы активности правила:

- ✓ — правило активно;
- ✗ — правило неактивно.

2. «Имя правила» — заданное АИБ произвольное имя правила при создании.
3. «Условия» — индикатор (список индикаторов, объединенных операторами), указанный при создании правила.
4. «Действие» — действие, указанное при создании правила.
5. «Тип модуля» — тип модуля, для которого создано правило.

В данной категории можно создавать, редактировать, удалять, активировать, деактивировать, копировать, повышать или понижать приоритет правила автоматического реагирования при помощи соответствующих кнопок на панели *Действия* или команд контекстного меню.



Управление списком правил автоматического реагирования доступно только на уровне корня ДБ **ЕЦУ**. На уровне группы (подгруппы), АРМ и модулей возможен только просмотр и активация/деактивация правил.

Для добавления правила автоматического реагирования необходимо:

1. В категории **Правила автоматического реагирования** нажать кнопку **Создать** на панели *Действия*.
2. В открывшемся мастере создания правила выбрать тип модуля, для которого создается правило.
3. Ввести в текстовом поле имя создаваемого правила, указать условие, выбрав индикаторы в открывшемся по нажатию кнопки **Выбрать индикаторы** окне, а также выбрать действие из выпадающего списка.

После выбора индикатора в окне **Выбор индикатора** его имя (или строка «Любой индикатор», если проставлен соответствующий чекбокс) отобразится в кнопке выбора и появится выпадающий список + со следующими значениями:

- «+» — пока выбрано данное значение, окно остается без изменений до выбора одного из операторов «ИИЛИ»;
- «И» / «ИЛИ» — при выборе данных операторов добавляется кнопка выбора нового индикатора и выпадающий список оператора;



Для создания условия в ЕЦУ возможно использовать до 3 индикаторов включительно.

- «Удалить» — удаляет следующий индикатор (индикатор справа от данного блока), выпадающий список выбора оператора принимает значение следующего (при его наличии).
4. Выбрать объекты дерева, для которых создаваемое правило будет активно. Также можно оставить правило выключенным, оставив параметры по умолчанию.
 5. Проверить значения параметров правила, после чего подтвердить создание нажатием кнопки **Готово**. Новое правило будет добавлено в конец списка, с меньшим приоритетом.

Для редактирования правила необходимо нажать кнопку **Редактировать** на панели *Действия* либо выбрать данную команду из контекстного меню, после чего в открывшемся окне **Редактирование правил реагирования ЕЦУ Dallas Lock** (рис. 148) внести необходимые изменения. Для сохранения изменений требуется нажать кнопку **Применить**. При нажатии на кнопку **Отмена** окно редактора правил будет закрыто без сохранения внесенных изменений.

Рис. 148. Редактирование правил реагирования ЕЦУ Dallas Lock

Удаление выбранного правила осуществляется посредством нажатия кнопки **Удалить** на панели *Действия* или выбора данной команды в контекстном меню.

Для копирования правила необходимо нажать кнопку **Копировать** на панели *Действия*, в открывшемся окне ввести имя правила или оставить предложенное по умолчанию, после чего нажать кнопку **Применить**. При нажатии на кнопку **Отмена** окно будет закрыто без применения каких-либо изменений.



После копирования новое правило будет добавлено в таблицу с приоритетом, меньшим на единицу от копируемого правила. Приоритеты последующих правил будут пересчитаны.

5.10.3 Индикаторы компрометации (IoC)

Категория **Индикаторы компрометации (IoC)** на странице **Управление компонентом СОР** предназначена для управления механизмом IoC (рис. 149).

В рабочей области категории располагается таблица, содержащая список существующих правил.

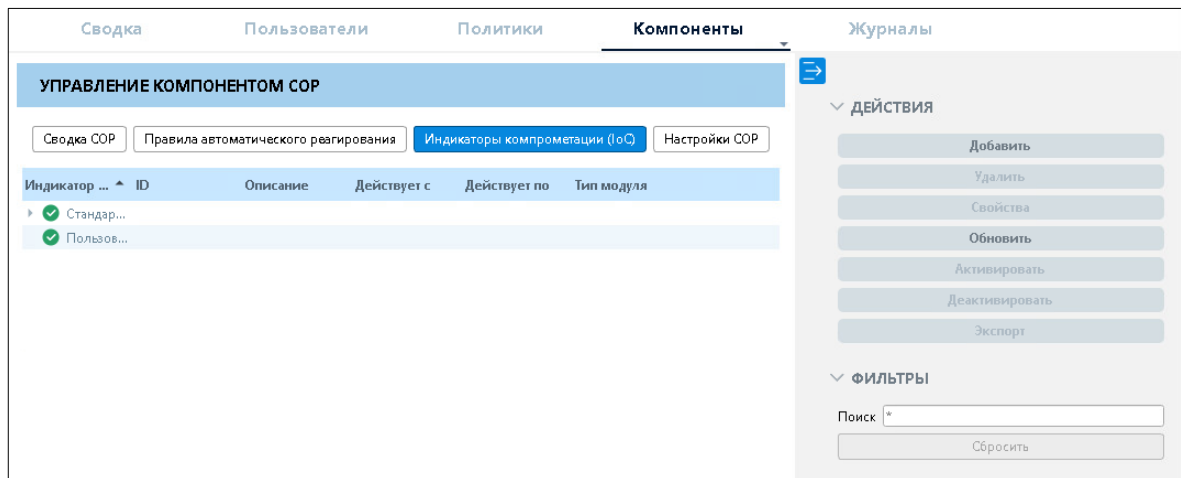


Рис. 149. Категория «Индикаторы компрометации (IoC)»

Для списка IoC-объектов предусмотрена возможность сортировки по столбцам, осуществляемая внутри групп *Стандартные* и *Пользовательские*.



Управление списком правил реагирования осуществляется только на уровне ДБ. На уровне группы, АРМ и модуля доступны только просмотр, активация/деактивация и включение/отключение наследования.

Для просмотра IoC-объекта необходимо нажать на кнопку **Свойства** на панели **Действия** или дважды кликнуть на строку в таблице с выбранным IoC-объектом, после чего откроется окно **Просмотр индикатора компрометации (IoC)**, содержащее json-объект без возможности редактирования и кнопку **Заккрыть**.

Для добавления пользовательских индикаторов компрометации необходимо:

1. Нажать кнопку **Добавить** на панели **Действия**, после чего откроется окно **Добавление пользовательских индикаторов компрометации (IoC) ЕЦУ Dallas Lock** (рис. 150).

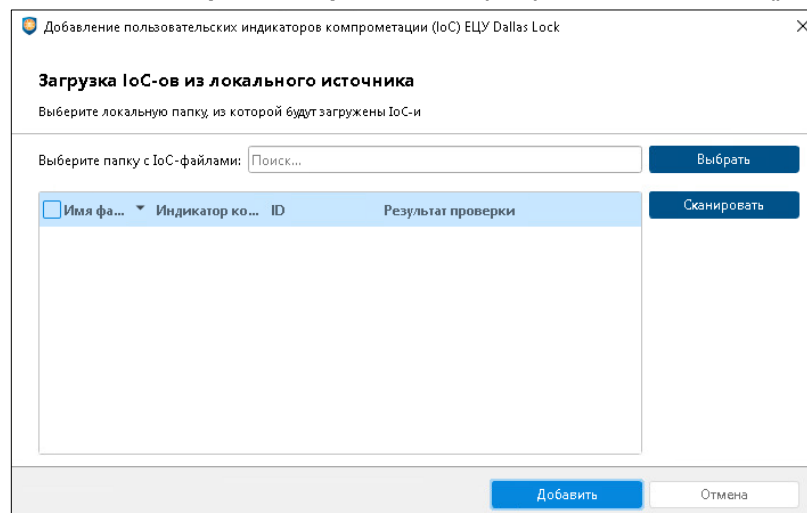


Рис. 150. Добавление пользовательских индикаторов компрометации (IoC)

2. В открывшемся окне указать путь до каталога с IoC-файлами, в которых определены IoC-объекты, прописав путь в поле *Выберите папку с IoC-файлами* или выбрав каталог в проводнике

при помощи кнопки **Выбрать**, после чего нажать кнопку **Сканировать** для проверки наличия в указанном каталоге IoC-файлов и последующей проверки соответствия содержащихся IoC-объектов критериям. Нажать на кнопку **Добавить**.



Критерии того, что файл является IoC-файлом:

- файл имеет расширение .json;
- в файле есть хотя бы один JSON-объект, у которого *type* равен *indicator*.

По результатам сканирования все IoC-объекты, обнаруженные в IoC-файлах, будут добавлены в таблицу.



Если файлы, удовлетворяющие критериям, в процессе сканирования не будут найдены, появится соответствующее сообщение об ошибке.

3. В таблице обнаруженных IoC-объектов установить в столбце *Имя файла* чекбоксы напротив индикаторов компрометации, которые требуется добавить в базу IoC-объектов.

4. Нажать кнопку **Добавить**.

Кнопка **Отмена** позволяет закрыть окно **Добавление пользовательских индикаторов компрометации (IoC) ЕЦУ Dallas Lock** без сохранения любых изменений.

Для удаления необходимо выбрать в таблице один или несколько индикаторов компрометации и нажать кнопку **Удалить** на панели *Действия*, после чего в открывшемся окне подтвердить удаление.



Если для удаления были выбраны и пользовательские, и стандартные IoC-объекты, то при подтверждении удаления выделенные пользовательские IoC-объекты будут удалены, а выделенные стандартные IoC-объекты — деактивированы.

5.10.4 Настройки COP

Настройки, касающиеся значений политик COP, регулируются в категории **Настройки COP** на вкладке **Компоненты** → **Средство обнаружения и реагирования** (рис. 151).

Политика	Значение	Тип модуля
Запрет на изм...		
Расписание сканирования системы на индикаторы компрометации (IoC)	Вкл.	DL8.0 (IK12)
Правила автоматического реагирования	Вкл.	DL8.0 (IK12), DLL (IK5)
Область сканирования IoC	Не используется	DLL (IK5)
Регулярность сканирования IoC	Сканирование выключено	DLL (IK5)
Обновление базы индикаторов компрометации (IoC)	Вкл.	Система, DL8.0 (IK12), DLL (IK5)
Регулярность обновлений	Вручную	DL8.0 (IK12), DLL (IK5)
Источник обновлений	updates.dallaslock.ru/Update	DL8.0 (IK12)
Источник обновлений IoC	updates.dallaslock.ru/Update...	DLL (IK5)

Рис. 151. Категория «Настройки COP»

Таблица 25. Настройки COP

Источник обновлений
Значением для политики может быть HTTPS-адрес и/или адрес папки. По умолчанию для политики выбран тип <i>HTTPS</i> и назначен источник <i>updates.dallaslock.ru/Update</i> .

Активация / деактивация источника обновлений осуществляется при помощи чекбокса в столбце *Используется*. С помощью кнопок **Вверх** и **Вниз** можно управлять приоритетом источника обновлений.

Политика позволяет управлять источником обновления базы IoC-объектов.

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

Источник обновлений IoC

Значением для политики может быть HTTPS-адрес и/или адрес папки. По умолчанию для политики выбран тип *HTTPS* и назначен источник *updates.dallaslock.ru/Update/UcclocUpdate.zip*.

Политика позволяет управлять источником обновления базы IoC-объектов.

Политика применяется на модулях **СЗИ НСД Dallas Lock Linux**.

Область сканирования IoC

Политика используется для настройки области сканирования системы на индикаторы компрометации.

Политика применяется на модулях **СЗИ НСД Dallas Lock Linux**.

Обновление базы индикаторов компрометации (IoC)

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

Политика позволяет управлять возможностью обновления базы индикаторов компрометации: обновление осуществляется только в том случае, если политика включена.

Политика применяется на:

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

Правила автоматического реагирования

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

Политика применяется на модулях:

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

Расписание сканирования системы на индикаторы компрометации (IoC)

Значение политики по умолчанию: «17: 00 Пн Вт Ср Чт Пт». Интерфейс политики представлен на рис. 152.

Политика используется для управления расписанием поиска IoC.

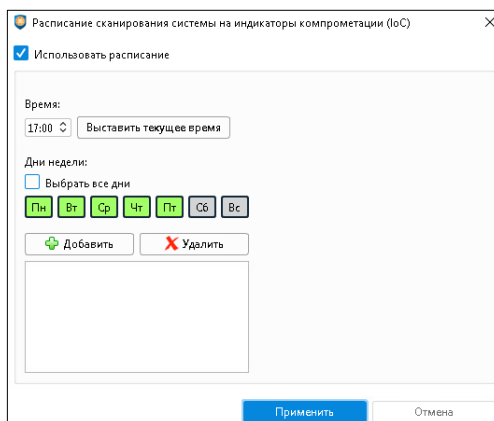


Рис. 152. Настройка политики «Расписание поиска индикаторов компрометации (IoC)»

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

Регулярность обновлений

Возможное значение политики: «Вручную», «Раз в час», «Раз в сутки», «Раз в две недели». Значение по умолчанию: «Вручную».



Политика дублируется из категории **Общие настройки СОВ** вкладки *Компоненты* → *Система обнаружения вторжений*.

Политика применяется на модулях:

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

Регулярность сканирования IoC

Для политики требуется вводить значение в формате «ДД ЧЧ:ММ», но не реже, чем раз в 21 день, и не чаще, чем раз в 15 минут.

Политика используется для настройки регулярности сканирования системы на индикаторы компрометации IoC.

Политика применяется на модулях **СЗИ НСД Dallas Lock Linux**.

5.11 Задания ДБ

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

Управление заданиями осуществляется на вкладке *Задания* (рис. 153).

Сводка		Пользователи		Политики		Компоненты	Задания
Создано	Выполнено	Тип	Автор	АРМ	Модуль	Статус	
05.06.2025 14:49	1 из 2	Проверка целостности	admin	АРМ-DL80-K, A...	Dallas Lock 8.0 ИК12	Ожидание выполнения	УПРАВЛЕНИЕ ЗАДАНИЯМИ Добавить задание Удалить выделенные задания Удалить выполненные задания Удалить все задания Показать результат Сохранить в файл
05.06.2025 14:49	05.06.2025 14:49	Проверка целостности	admin	АРМ-DL80-C	Dallas Lock 8.0 ИК12	Ожидание выполнения	
05.06.2025 14:49	05.06.2025 14:49	Проверка целостности	admin	АРМ-DL80-K	Dallas Lock 8.0 ИК12	OK	
05.06.2025 14:46	1 из 1	Получение конфигу...	admin	АРМ-DL80-K	Dallas Lock 8.0 ИК12	OK	
05.06.2025 14:48	05.06.2025 14:48	Получение конфигу...	admin	АРМ-DL80-K	Dallas Lock 8.0 ИК12	OK	

Рис. 153. Вкладка «Задания»

Список заданий на уровне ДБ представляет собой таблицу с полями:

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



— задание выполнено;



— задание ожидает выполнения;



— при выполнении задания произошла ошибка.

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

5.11.1 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. 154).

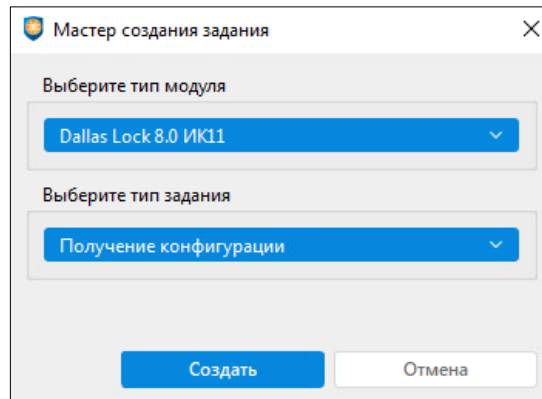


Рис. 154. Мастер создания задания

4. Выбрать тип модуля и тип задания.

5. Нажать кнопку **Создать**.

6. При необходимости указать дополнительную информацию, необходимую для создания задания. Очередь созданных заданий доступна при выборе объекта в дереве и переходе на вкладку *Задания*. Созданное задание ассоциируется с конкретным модулем в домене, поэтому при создании задания на уровне ДБ в списке появятся записи о заданиях по количеству в домене модулей того типа, который указан при создании задания. Типы заданий для каждого отдельного модуля перечислены в таблице ниже.



Если задания были созданы одновременно для определенного типа модулей, то они автоматически будут объединены в группу.

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

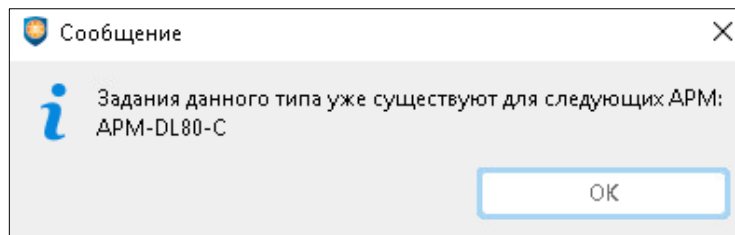


Рис. 155. Предупреждение о создании дубликата задания

Таблица 26. Типы заданий

Наименование модуля	Типы заданий
СЗИ Dallas Lock 8.0-K/C	• изменение параметров лицензии (изменяет номер лицензии и код технической поддержки); • получение конфигурации; • применение конфигурации; • проверка целостности; • удаление DL8.0; • сканирование системы на индикаторы компрометации (IoC)
СЗИ НСД Dallas Lock Linux	• изменение параметров лицензии (изменяет номер лицензии и код технической поддержки);

	• получение конфигурации; • применение конфигурации; • удаление СЗИ НСД Dallas Lock Linux; • сканирование системы на индикаторы компрометации (IoC)
Dallas Lock СЗИ ВИ	• изменение параметров лицензии (изменяет номер лицензии и код технической поддержки); • получение конфигурации; • получение отчета о конфигурации (<i>формат *.rtf</i>); • применение конфигурации; • проверка обновлений
СДЗ Dallas Lock	• очистка журнала; • получение конфигурации; • получение отчета об аппаратном обеспечении; • получение отчета по конфигурации; • применение конфигурации; • сброс ДВК; • тестирование функций СДЗ
СДЗ УБ Dallas Lock	• очистка журнала; • получение конфигурации; • получение отчета об аппаратном обеспечении; • получение отчета по конфигурации; • тестирование функций СДЗ; • применение конфигурации
WAF Dallas Lock	• восстановить резервную копию; • обновление базы разрешающих правил; • сбор журналов; • сброс к заводским настройкам; • создать резервную копию; • применение файла лицензии
Агент ЕЦУ (Windows/Linux)	• отчет об аппаратном обеспечении; • удаление Агента ЕЦУ; • отчет о программном обеспечении
Агент ЕЦУ (Android)	• информация об устройстве; • отчет о программном обеспечении
Kaspersky Endpoint Security	• обновление антивирусных баз; • сканирование клиентских АРМ

5.11.2 Результат выполнения задания

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

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

5.11.3 Удаление заданий

Для удаления задания из списка необходимо выбрать задание и нажать на панели инструментов команду **Удалить выделенные задания**, после чего подтвердить удаление.

Также на панели инструменты доступны команды для удаления нескольких заданий:

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

5.12 Журнал ДБ

Вкладка *Журналы* на уровне Домена безопасности позволяет просматривать следующие категории журналов ДБ (рис. 156):

- «Журнал ЕЦУ» — отображаются регистрируемые события, связанные непосредственно с работой текущего ДБ **ЕЦУ Dallas Lock**;
- «Журнал сессий» — отображается информация о создании и завершении сессии на АРМ;
- «Журнал Syslog» — отображаются регистрируемые события, связанные с изменением конфигурации сетевых устройств, зарегистрированных в ДБ.

СводкаПользователиПолитикиКомпонентыЗаданияЖурналы

Журнал ЕЦУЖурнал сессийЖурнал Syslog

№	Дата и время	Пользователь	Событие	Объект	Результат	Комментарий
22	2025-06-05 18:19:30 (GMT+03:00)	admin	Подключение консоли управления	Консоль "UCC-1K4"	OK	
21	2025-06-05 18:05:43 (GMT+03:00)		Прекращение обслуживания термин...	АРМ "АРМ-DL80-K", Модуль...	OK	Действие инициировано модулем
20	2025-06-05 18:04:19 (GMT+03:00)		Прекращение обслуживания термин...	АРМ "АРМ-DL80-K", Модуль...	OK	Действие инициировано модулем
19	2025-06-05 18:04:19 (GMT+03:00)		Добавление объекта в ДБ	АРМ "АРМ-DL80-K", Модуль...	OK	
18	2025-06-05 18:04:19 (GMT+03:00)		Добавление объекта в ДБ	АРМ "АРМ-DL80-K"	OK	
17	2025-06-05 17:39:37 (GMT+03:00)		Добавление объекта в ДБ	АРМ "АРМ-DL80-C", Модуль...	OK	
16	2025-06-05 17:39:37 (GMT+03:00)		Добавление объекта в ДБ	АРМ "АРМ-DL80-C"	OK	
15	2025-06-05 17:38:22 (GMT+03:00)		Добавление объекта в ДБ	АРМ "АРМ-DLL", Модуль "D...	OK	
14	2025-06-05 17:38:22 (GMT+03:00)		Добавление объекта в ДБ	АРМ "АРМ-DLL"	OK	
13	2025-06-05 16:48:37 (GMT+03:00)	admin	Подключение консоли управления	Консоль "UCC-1K4"	OK	
12	2025-06-05 16:48:23 (GMT+03:00)		Регистрация консоли управления	Консоль "UCC-1K4"	OK	
11	2025-06-05 16:48:10 (GMT+03:00)		Инициализация подсистемы аудита	ДБ "Домен безопасности"	OK	
10	2025-06-05 16:48:10 (GMT+03:00)		Запуск службы ЕЦУ	ДБ "Домен безопасности"	OK	
9	2025-06-05 16:48:10 (GMT+03:00)		Режим работы сервера	Сервер "ucsc-ik4.dl.local:17900"	OK	Сервер функционирует в соответс...
8	2025-06-05 16:48:10 (GMT+03:00)		Чтение файла с лицензией	Сервер "ucsc-ik4.dl.local:17900"	OK	Сервер успешно прочитал файл с...
6	2025-06-05 16:48:05 (GMT+03:00)		Чтение файла с лицензией	Сервер "ucsc-ik4.dl.local:17900"	OK	Сервер успешно прочитал файл с...
3	2025-06-05 16:48:05 (GMT+03:00)		Остановка службы ЕЦУ	ДБ "Домен безопасности"	OK	
2	2025-06-05 16:48:05 (GMT+03:00)		Инициализация подсистемы аудита	ДБ "Домен безопасности"	OK	
1	2025-06-05 16:48:05 (GMT+03:00)		Запуск службы ЕЦУ	ДБ "Домен безопасности"	OK	
4	2025-06-05 16:48:05 (GMT+03:00)		Режим работы сервера	Сервер "ucsc-ik4.dl.local:17900"	На сервере...	Сервер работает в режиме ограни...
7	2025-06-05 16:48:10 (GMT+03:00)		Проверка токена с лицензией	Сервер "ucsc-ik4.dl.local:17900"	В токене от...	Сервер не обнаружил ключ с лицен...
5	2025-06-05 16:48:05 (GMT+03:00)		Проверка токена с лицензией	Сервер "ucsc-ik4.dl.local:17900"	В токене от...	Сервер не обнаружил ключ с лицен...

ФИЛЬТРЫ

☒ Количество запрашиваемых записей

100Последних записей

☐ Фильтр по времени

С05.06.202418:19:52

По05.06.202518:19:52

Часовой поясGMT+3:00

☒ Фильтр по параметрам

Пользователь*

Объект*

РезультатВсе

Комментарий*

Выбор

Выбрать всеОчистить

☒ Архивация журналов

☒ Ввод ДБ в подчинение другому ДБ

☒ Включение КПСН

☒ Включение терминального сервера

☒ Вывод ДБ из подчинения

☒ Вывод модуля из ДБ

☒ Вывод сервера из кластера ЕЦУ

☒ Выключение КПСН

☒ Выключение терминального сервера

☒ Добавление IOS

☒ Добавление КПСН

ПрименитьСбросить

☐ Просматривать архив

ДЕЙСТВИЯ

Очистить журнал

Экспортировать журнал

Обновить журнал

ОПЕРАТИВНОЕ УПРАВЛЕНИЕ

Собрать журналы

Рис. 156. Вкладка «Журналы» Домена безопасности



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**.



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

Справа расположены панель инструментов *Фильтры* и панель инструментов *Действия*. Параметры фильтрации зависят от категории журнала. Сброс и применение выбранных фильтров осуществляется по команде **Сбросить** и **Применить** соответственно. Отфильтрованные записи журнала можно сохранить в выбранном типе файла (HTML, TXT, CSV) с помощью команды **Экспортировать журнал** на панели инструментов *Действия* (рис. 157). Экспортировать журнал можно учитывая текущую сортировку, для этого необходимо установить соответствующий флаг в окне **Экспорт журнала**.

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

По команде **Обновить журнал** осуществляется обновление содержимого текущего журнала.

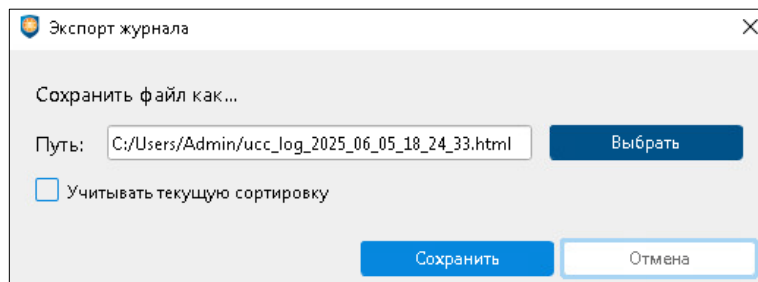


Рис. 157. Окно «Экспорт журнала»

Двойной клик по пункту журнала откроет окно с подробностями записи (рис. 158). Нажимая на кнопки **вверх** и **вниз**, можно просматривать записи журнала.

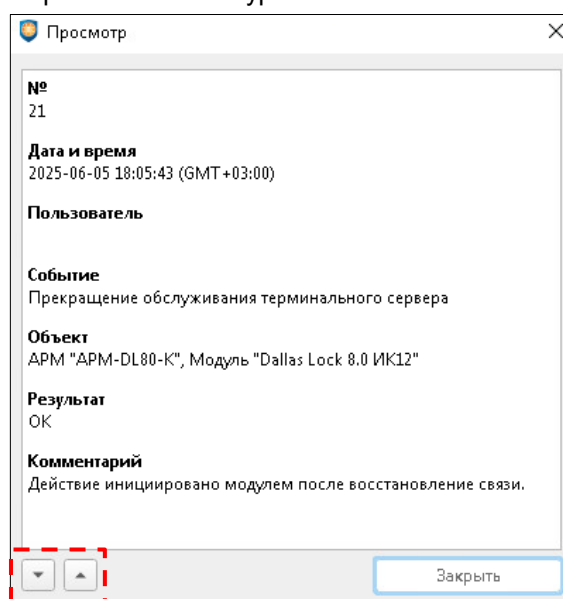


Рис. 158. Просмотр подробности записи журнала

6 ГРУППЫ ДОМЕНА БЕЗОПАСНОСТИ

6.1 Базовые группы

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

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

Удаление, переименование и перемещение базовых групп недоступно.



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*».



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



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

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

6.2 Настройка групп

Создать группу/подгруппу можно несколькими способами:

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

Введенное на этапе создания наименование группы, можно впоследствии изменить.

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

Удалить существующую группу можно с помощью кнопки **Удалить** 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. 159).

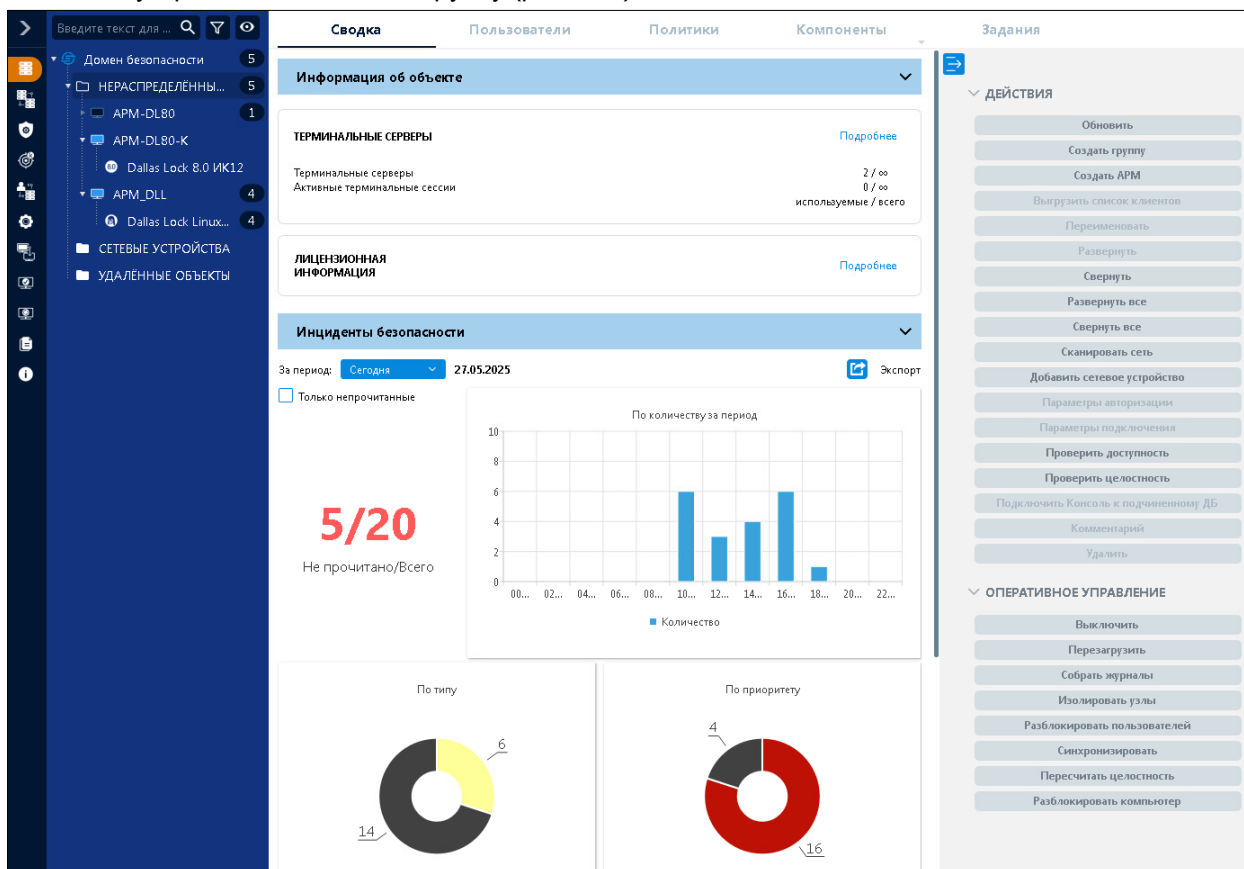


Рис. 159. Вкладка «Сводка» для группы ДБ

Управление данной вкладкой аналогично управлению вкладкой **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.
10. Удалить.

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. Изолировать узлы.

7. Включить узлы в сеть.
8. Синхронизировать.
9. Системный журнал.
10. Включить аварийный режим.
11. Отключить аварийный режим.
12. Сбросить блокировки.
13. Обновить.
14. Удаленное включение.



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

6.2.2 Пользователи и группы для группы ДБ

Вкладка *Пользователи* на уровне группы ДБ содержит списки глобальных учетных записей и групп пользователей группы ДБ.

Учетные записи группы ДБ

Категория **Пользователи** содержит список учетных записей пользователей группы ДБ (рис. 160).

Состоян...	Учетная запись	Категория	Тип учетной записи ЕЦУ	Владелец	Роль администрирования	Полное имя	Описание
☒	admin	Глобальная	Все	Домен - Домен безопасности	Администратор (Домен - Домен безопасности)		Администрат.
☒	Test	Глобальная	Все	Домен - Домен безопасности	Не назначено		
☒	anonymous	Глобальная	Система, D18.0 (ИК10, ИК11), СЗИ ВИ (ИКА)	Домен - Домен безопасности	Не назначено	Anonymous user	Используется

Рис. 160. 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.



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* 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 — **Группы**. Этот инструмент функционирует аналогично *«Локальным группам»* в ОС семейства Windows и доступен в категории **Группы** на вкладке *Пользователи* (рис. 161).



Сводка	Пользователи	Политики	Компоненты	Задания
	Пользователи	Группы		
Сост...	Название группы	Категория	Тип	Описание группы
☒	Администраторы	Глобальная	Система, D18.0 (ИК10, ИК11), СЗИ ВИ (ИК4)	Администраторы имеют полные, ничем не ограниченные права доступа к...
☒	Администраторы Нурей-V	Глобальная	Система, D18.0 (ИК10, ИК11), СЗИ ВИ (ИК4)	Члены этой группы имеют полный и неограниченный доступ ко всем функ...
☒	Гости	Глобальная	Система, D18.0 (ИК10, ИК11), СЗИ ВИ (ИК4)	Гости по умолчанию имеют те же права, что и пользователи, за исключение...
☒	Криптографические операторы	Глобальная	Система, D18.0 (ИК10, ИК11), СЗИ ВИ (ИК4)	Членам этой группы разрешено выполнение операции криптографии.
☒	Операторы архива	Глобальная	Система, D18.0 (ИК10, ИК11), СЗИ ВИ (ИК4)	Операторы архива могут переназначать ограничения доступа только в цел...
☒	Операторы настройки сети	Глобальная	Система, D18.0 (ИК10, ИК11), СЗИ ВИ (ИК4)	Члены этой группы могут иметь некоторые административные права для уп...
☒	Операторы помощи по контролю учетных записей	Глобальная	Система, D18.0 (ИК10, ИК11), СЗИ ВИ (ИК4)	Члены этой группы могут удаленно запрашивать атрибуты авторизации и ра...

Рис. 161. Список групп пользователей группы ДБ

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

У модулей существует также свой список групп пользователей, в котором также можно выбрать необходимые для доступа к работе на модуле.

За данную функцию отвечает поле *Состояние*. Поле *Состояние* на уровне группы домена безопасности принимает следующий вид:

- ☒ — отмеченное флагом поле означает, что данная группа пользователей имеет доступ на уровне группы ДБ, при этом *Состояние* задано (переопределено) на данном уровне дерева;
- ☒ — отмеченное флагом поле означает, что данная группа пользователей имеет доступ на уровне группы ДБ, при этом *Состояние* наследуется с уровня выше в дереве;
- ☐ — пустое поле означает, что группа пользователей отключена для работы на уровне группы ДБ, при этом *Состояние* задано (переопределено) на данном уровне дерева;
- ☒ — пустое поле означает, что группа пользователей отключена для работы на уровне группы ДБ, при этом *Состояние* наследуется с уровня выше в дереве.



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* доступны:

- создание глобальных групп пользователей (см. [«Создание групп пользователей»](#));
- удаление глобальных групп пользователей (см. [«Удаление групп пользователей ДБ»](#));
- просмотр и настройка параметров групп пользователей (см. [«Параметры групп пользователей»](#));
- смена типа учетных записей группы, в зависимости от того, для модулей какого типа применяется данная группа пользователей;
- установка наследования с помощью параметра *Наследовать*;
- просмотр свойств групп.

6.2.3 Политики для группы ДБ

Вкладка *Политики* на уровне группы позволяет редактировать параметры безопасности на уровне группы (подгруппы) (рис. 162).

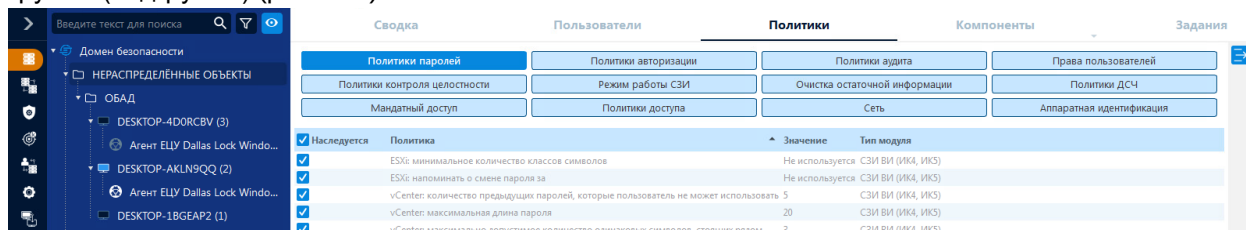


Рис. 162. Политики для групп Домена безопасности

Настройка политик для группы (подгруппы) производится аналогично настройке политик для ДБ (см. [«Политики ДБ»](#)). Для применения параметров на модулях необходима синхронизация.

Политики могут наследовать установленные настройки (от ДБ или от группы, в состав которой входит данная группа (подгруппа)) или принимать индивидуальные значения следующим образом:

1. Политики, для которых отмечено наследование, примут значения, установленные для родительского объекта в дереве объектов **ЕЦУ**: значения для ДБ или группы. В этом случае политики будут отображаться нечетким серым цветом.
2. Политики, для которых выбраны и установлены оригинальные настройки, будут отображаться четким черным цветом.

Для того, чтобы установить или снять наследование настроек, имеются следующие возможности:

1. Для того, чтобы все параметры наследовали значения, установленные для родительского объекта дерева, необходимо поставить флаг в поле *Наследуется* (рис. 163).

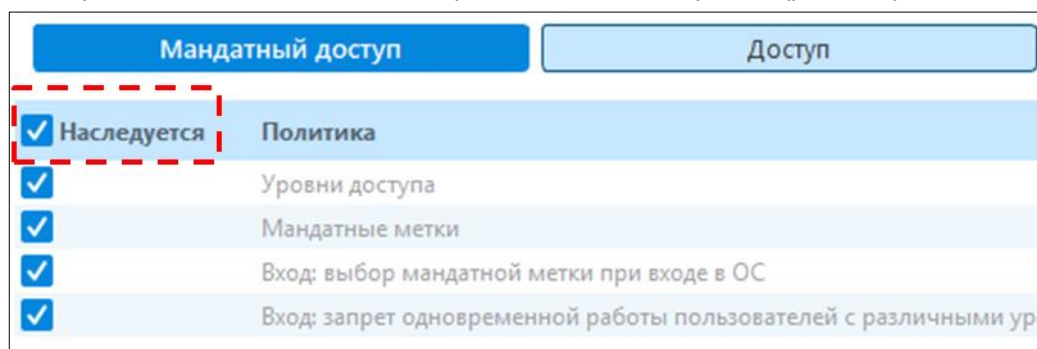


Рис. 163. Включение наследования политик объекта

2. Если снять флаг из поля *Наследуется*, то все параметры одновременно станут обозначены как индивидуально настроенные (рис. 164).

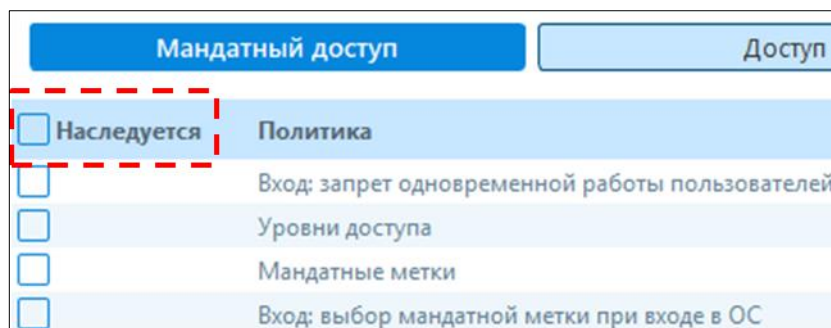


Рис. 164. Выключение наследования политик объекта

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 Межсетевой экран для группы ДБ

Вкладка *Межсетевой экран* на уровне группы позволяет управлять межсетевым экраном на уровне группы (подгруппы) Домена безопасности (рис. 165).

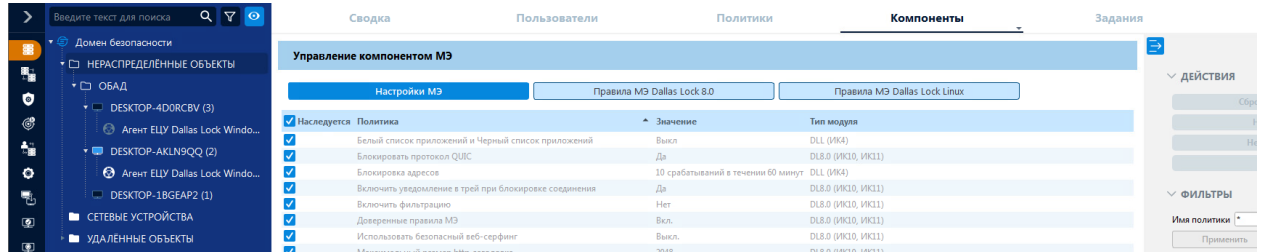


Рис. 165. Межсетевой экран для групп Домена безопасности

Управление межсетевым экраном на уровне группы ДБ производится аналогично управлению межсетевым экраном для ДБ (см. [«Межсетевой экран»](#)).

6.2.5 Система контроля накопителей для группы ДБ

Вкладка *Система контроля накопителей* на уровне группы позволяет управлять накопителями на уровне группы (подгруппы) Домена безопасности (рис. 166).

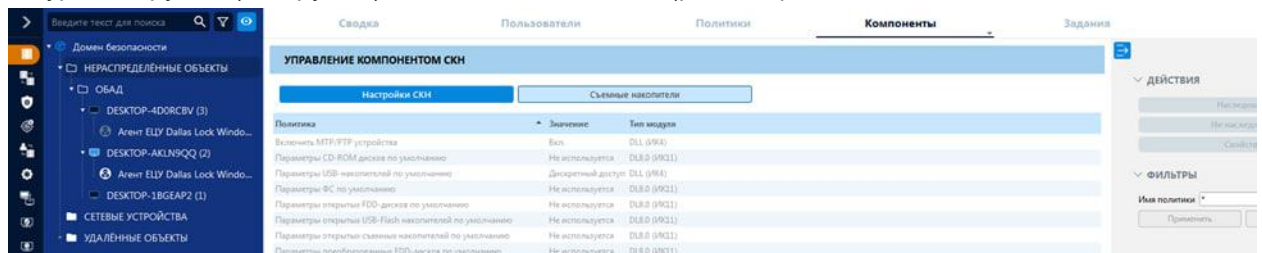


Рис. 166. Система контроля накопителей для групп Домена безопасности

Управление системой контроля накопителей на уровне группы ДБ производится аналогично управлению системой контроля накопителей для ДБ (см. [«Система контроля накопителей»](#)).

6.2.6 Контроль ресурсов для группы ДБ

Вкладка *Контроль ресурсов* на уровне группы позволяет управлять контролем ресурсов на уровне группы (подгруппы) Домена безопасности (рис. 167).

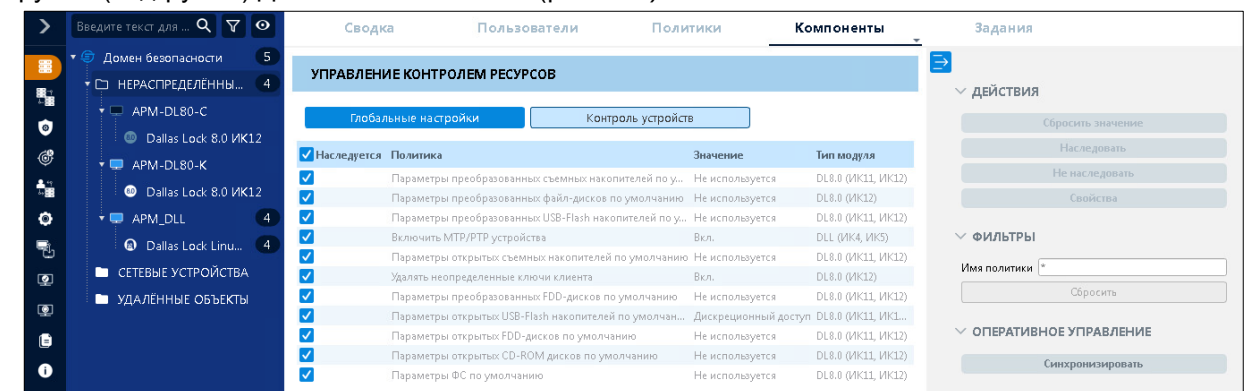


Рис. 167. Контроль ресурсов для групп Домена безопасности

Управление контролем ресурсов на уровне группы ДБ производится аналогично управлению контролем ресурсов для ДБ (см. [«Контроль ресурсов»](#)).

6.2.7 Система обнаружения вторжений для группы ДБ

Вкладка *Система обнаружения вторжений* на уровне группы позволяет управлять системой обнаружения вторжений на уровне группы (подгруппы) Домена безопасности (рис. 168).

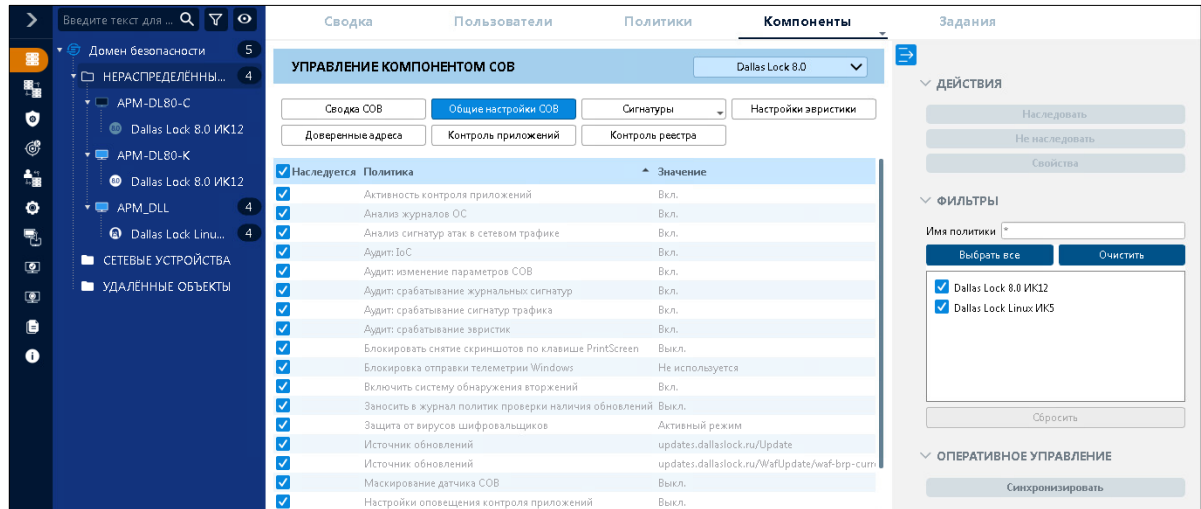


Рис. 168. Система обнаружения вторжений для групп Домена безопасности

Управление системой обнаружения вторжений на уровне группы ДБ производится аналогично управлению системой обнаружения вторжений для ДБ (см. [«Система обнаружения вторжений»](#)).

На уровне группы ДБ на вкладке *Компоненты* → *Система обнаружения вторжений* доступно:

- просмотр журнала событий (см. [«Сводка СОВ»](#));
- просмотр настроенных политик и параметров СОВ;
- управление политиками СОВ для модулей (см. [«Общие настройки СОВ»](#)) и настройками эвристик (см. [«Настройки эвристик»](#));
- установка наследования с помощью параметра *Наследовать*;
- активация/деактивация сигнатур журналов, сигнатур трафика (см. [«Сигнатуры»](#)), правил контроля приложений (см. [«Контроль приложений»](#)) и контролируемых ключей реестра (см. [«Контроль реестра»](#));
- управление параметром *Отметка в журнале* для перечня определенных доверенных адресов;
- синхронизация с модулями.

При этом на уровне группы ДБ индикаторы состояния для сигнатур и контролируемых ключей реестра могут принимать следующий вид:

-  — сигнатура / ключ реестра или вся группа сигнатур / ключей активирована, состояние не наследуется с верхнего уровня домена;
-  — сигнатура / ключ реестра или вся группа сигнатур / ключей деактивирована, состояние не наследуется с верхнего уровня домена;
-  — сигнатура / ключ реестра или вся группа сигнатур / ключей активирована, состояние наследуется с верхнего уровня домена;
-  — сигнатура / ключ реестра или вся группа сигнатур / ключей деактивирована, состояние наследуется с верхнего уровня домена;
-  — активированы не все сигнатуры / ключи, входящие в группу, и не для всех сигнатур / ключей наследуется состояние с верхнего уровня домена;
-  — активированы не все сигнатуры / ключи, входящие в группу, но для всех сигнатур / ключей состояние наследуется с верхнего уровня.



Возможные индикаторы состояния для сигнатур журналов модулей **СЗИ НСД Dallas Lock 8.0** отличаются от представленных в данном пункте (см. [«Сигнатуры журналов для модулей СЗИ НСД Dallas Lock 8.0-С/К»](#)).

Для правил контроля приложений на уровне группы ДБ выделены следующие индикаторы состояния:

-  — правило активировано, все значения для системных функций установлены в *Разрешено*, но его состояние активности не наследуется с верхнего уровня домена;
-  — правило активировано, все значения для системных функций установлены в *Запрещено*, но его состояние активности не наследуется с верхнего уровня домена;
-  — правило активировано, все значения для системных функций установлены в *Разрешено*, состояние активности наследуется с верхнего уровня домена;
-  — правило активировано, все значения для системных функций установлены в *Запрещено*, состояние активности наследуется с верхнего уровня домена;
-  — правило активировано, не все значения для системных функций выставлены в *Разрешено* или *Запрещено*, состояние активности не наследуется с верхнего уровня домена;
-  — правило активировано, не все значения для системных функций выставлены в *Разрешено* или *Запрещено*, состояние активности наследуется с верхнего уровня домена;
-  — правило деактивировано.

6.2.8 Безопасная среда COB (песочница) для группы ДБ

Вкладка *Безопасная среда COB (песочница)* на уровне группы позволяет управлять безопасной средой на уровне группы (подгруппы) Домена безопасности (рис. 169).



Рис. 169. Безопасная среда COB (песочница) для групп Домена безопасности

Управление вкладкой *Безопасная среда COB (песочница)* доступно только на уровне корня ДБ ЕЦУ (см. [«Безопасная среда COB \(песочница\)»](#)). На уровне группы (подгруппы), АРМ и модулей функциональные возможности ограничены — доступен только просмотр параметров и их значений.

6.2.9 Средство обнаружения и реагирования для группы ДБ

Вкладка *Средство обнаружения и реагирования* на уровне группы позволяет управлять средством обнаружения и реагирования на уровне группы (подгруппы) Домена безопасности (рис. 170).

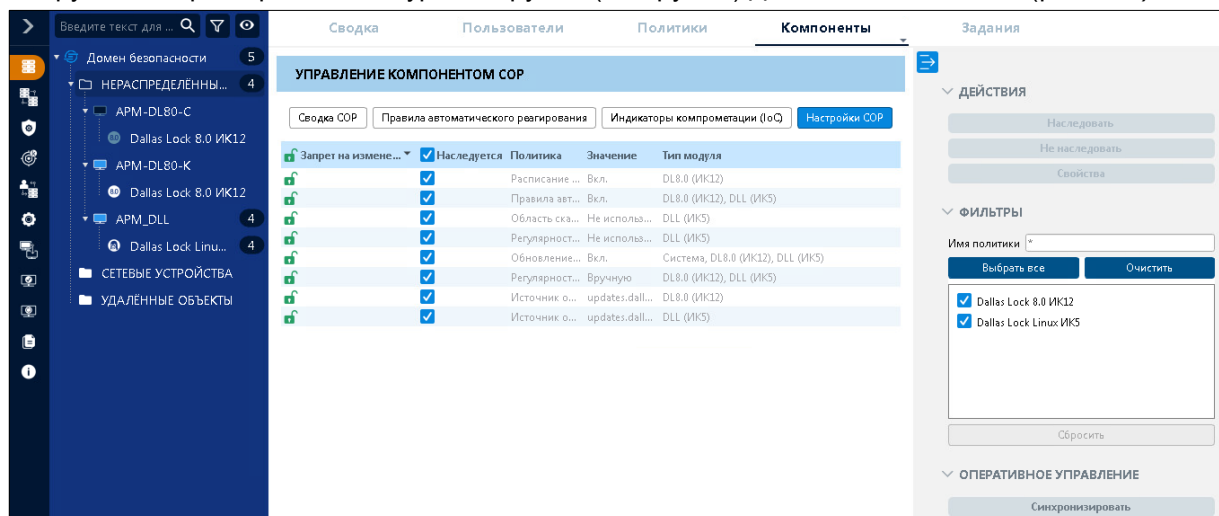


Рис. 170. Средство обнаружения и реагирования для групп Домена безопасности

На уровне группы ДБ возможен только просмотр настроек средства обнаружения и реагирования, управление осуществляется на уровне ДБ (см. [«Средство обнаружения и реагирования»](#)).

На уровне группы ДБ на вкладке *Компоненты* → *Средство обнаружения и реагирования* доступно:

- просмотр журнала событий и запуск обновления СОВ (см. [«Сводка СОР»](#));
- редактирование политик СОР (см. [«Настройки СОР»](#));
- просмотр и активация/деактивация правил автоматического реагирования (см. [«Правила автоматического реагирования»](#));
- просмотр, активация/деактивация и обновление перечня индикаторов компрометации (см. [«Индикаторы компрометации \(IoC\)»](#));
- установка наследования с помощью параметра *Наследовать*;
- синхронизация с модулями.

Для правил автоматического реагирования на уровне группы ДБ определены следующие индикаторы состояния:

- ✓ — правило активно;
- ✓ — правило активно и наследуется;
- ✗ — правило неактивно;
- ✗ — правило неактивно и наследуется.

6.2.10 Задания для группы ДБ

Вкладка **Задания** на уровне группы позволяет управлять заданиями на уровне группы (подгруппы) Домена безопасности (рис. 171).

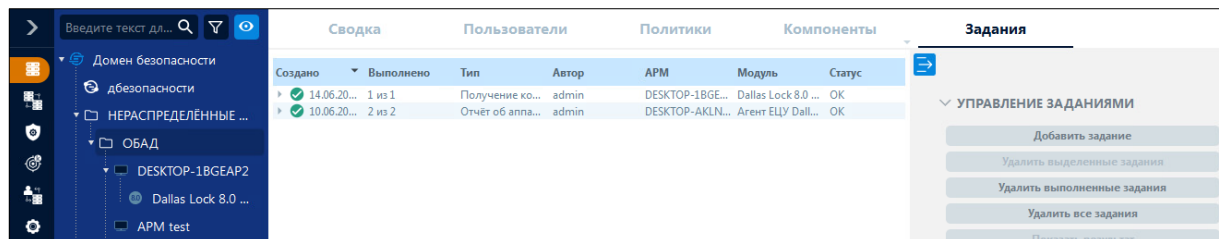


Рис. 171. Задания для групп Домена безопасности

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

7 АРМ ДОМЕНА БЕЗОПАСНОСТИ ЕЦУ

В ЕЦУ Dallas Lock АРМ используется как способ представления совокупности нескольких модулей в качестве единой машины (рис. 172).

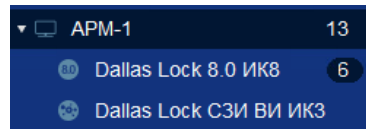


Рис. 172. АРМ в дереве ЕЦУ Dallas Lock

АРМ может включать в себя модули следующих типов:

- СЗИ Dallas Lock 8.0-K/C;
- СЗИ НСД Dallas Lock Linux;
- СДЗ Dallas Lock;
- СДЗ УБ Dallas Lock;
- СЗИ ВИ Dallas Lock;
- Агент ЕЦУ.

7.1 Настройка АРМ

Создать АРМ в Консоли ЕЦУ можно с помощью кнопки **Создать АРМ** на панели инструментов *Действия* или воспользовавшись контекстным меню в дереве ДБ. При создании АРМ потребуется ввести наименование, которое можно впоследствии изменить.

Перемещение АРМ в дереве осуществляется перетаскиванием значка кнопкой мыши в поле другого значка (*Drag-and-drop*). Перемещение АРМ осуществляется со всеми вложенными модулями.

Удалить существующее АРМ можно с помощью кнопки **Удалить** на панели инструментов *Действия* или воспользовавшись контекстным меню в дереве ДБ. Удаление АРМ осуществляется со всеми вложенными объектами.

Каждое АРМ в дереве объектов содержит одинаковые вкладки для индивидуальной настройки параметров для модулей в составе данного АРМ.

7.1.1 Сводка АРМ

Вкладка *Сводка* для выбранного АРМ в дереве объектов отображает общее состояние модулей, входящих в АРМ (рис. 173).

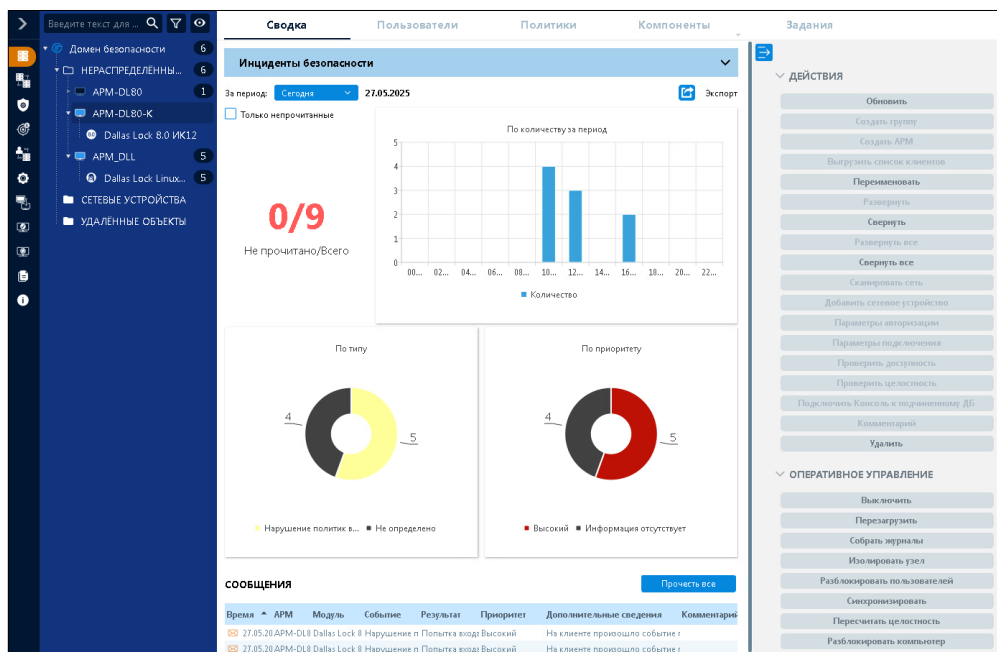


Рис. 173. Вкладка «Сводка» АРМ

На панели инструментов доступны следующие действия с APM:

1. Обновить.
2. Переименовать APM.
3. Удалить APM.

На панели инструментов доступны следующие команды оперативного управления для APM:

1. Выключить.
2. Перезагрузить.
3. Изолировать узел.
4. Включить узел в сеть.
5. Разблокировать пользователей.
6. Разблокировать компьютер.
7. Пересчитать целостность.
8. Собрать журналы.
9. Синхронизировать.
10. Удаленное управление.

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



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

7.1.2 Пользователи и группы APM

Вкладка *Пользователи* для выбранного APM содержит списки глобальных и доменных учетных записей, и групп пользователей APM (рис. 174).

Сост...	Учетная запись	Категория	Тип учетной записи ЕЦУ	Владелец	Роль администрирования	Полное имя	Описание
☒	admin	Глобальная	Все	Домен - Домен безопасности	Администратор (Домен - Домен безопасности)		Админ
☒	anonymous	Глобальная	Система, DL8.0 (ИК10, ИК11), СЗИ ВИ (ИК4)	Домен - Домен безопасности	Не назначено	Anonymous user	Исполь

Рис. 174. Вкладка «Пользователи» APM

Настройка пользователей для APM 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 APM

Вкладка *Политики* для выбранного APM позволяет редактировать параметры безопасности на уровне APM (рис. 175).

Наследуется	Политика	Значение	Тип модуля
☒	ESXi: миним...	Не использ...	СЗИ ВИ (ИК4, ИКС)
☒	ESXi: напом...	Не использ...	СЗИ ВИ (ИК4, ИКС)
☒	oVirt: Колл...	5	СЗИ ВИ (ИКС)

Рис. 175. Вкладка «Политики» APM

Настройка политик для APM производится аналогично настройке политик для группы ДБ (см. [«Политики для группы ДБ»](#)). Для применения параметров на модулях необходима синхронизация.

7.1.4 Межсетевой экран APM

Вкладка *Межсетевой экран* для выбранного APM позволяет управлять межсетевым экраном на уровне APM (рис. 176).

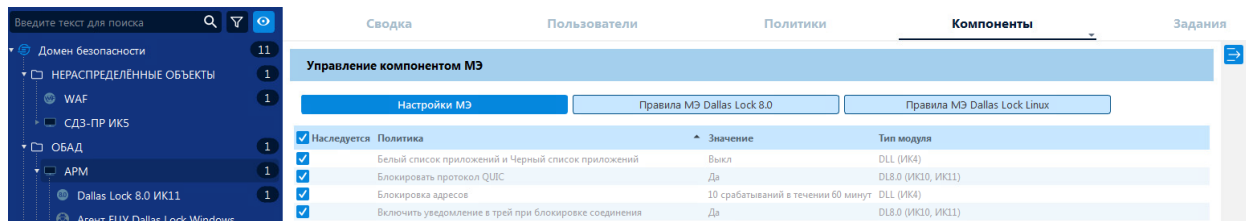


Рис. 176. Вкладка «Межсетевой экран» APM

Управление межсетевым экраном на уровне APM производится аналогично управлению межсетевым экраном для ДБ (см. [«Межсетевой экран»](#)).

7.1.5 Система контроля накопителей APM

Вкладка *Система контроля накопителей* для выбранного APM позволяет управлять системой контроля накопителей на уровне APM (рис. 177).

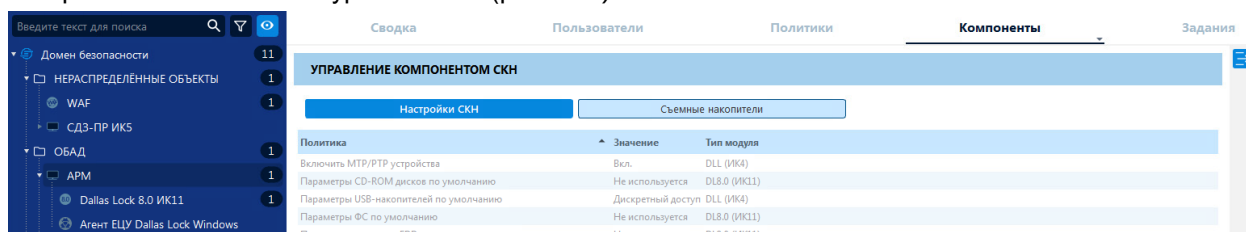


Рис. 177. Вкладка «Управление компонентом СКН» APM

Управление компонентом СКН на уровне APM производится аналогично управлению компонентом СКН для ДБ (см. [«Система контроля накопителей»](#)).

7.1.6 Контроль ресурсов APM

Вкладка *Контроль ресурсов* для выбранного APM позволяет управлять контролем ресурсов на уровне APM (рис. 178).

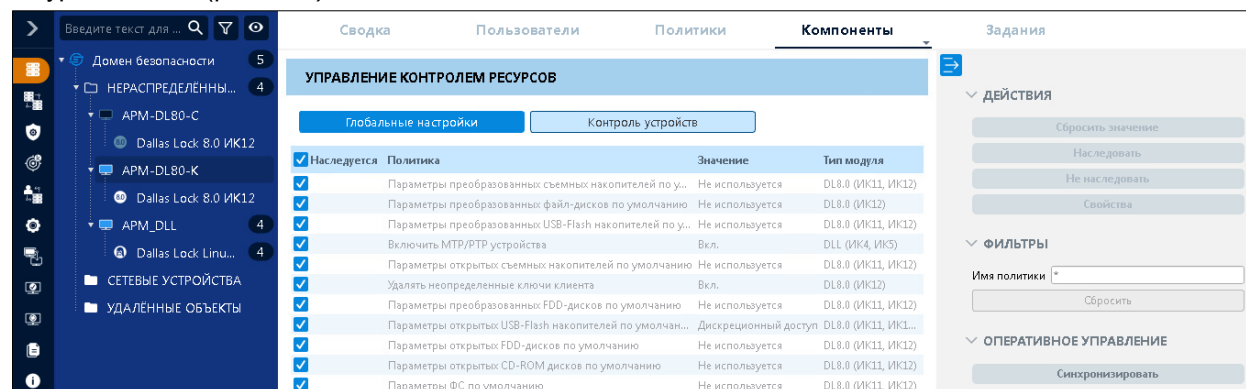


Рис. 178. Вкладка «Контроль ресурсов» APM

Управление контролем ресурсов на уровне APM производится аналогично управлению контролем ресурсов для ДБ (см. [«Контроль ресурсов»](#)).

7.1.7 Система обнаружения вторжений APM

Вкладка *Система обнаружения вторжений* для выбранного APM позволяет управлять компонентом COB на уровне APM (рис. 179).

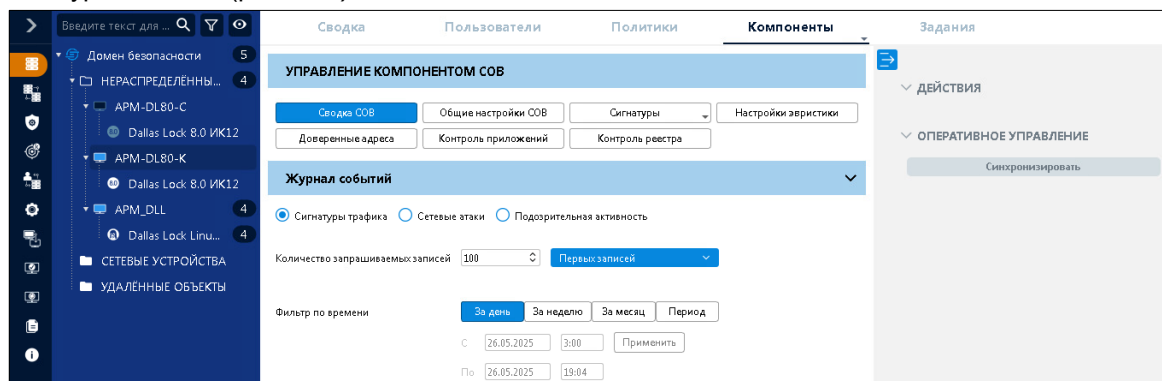


Рис. 179. Вкладка «Система обнаружения вторжений» APM

Управление системой обнаружения вторжений на уровне APM производится аналогично управлению компонентом COB для группы ДБ (см. [«Система обнаружения вторжений для группы ДБ»](#)).

7.1.8 Безопасная среда COB (песочница) APM

Вкладка *Безопасная среда COB (песочница)* для выбранного APM позволяет управлять безопасной средой на уровне APM (рис. 180).

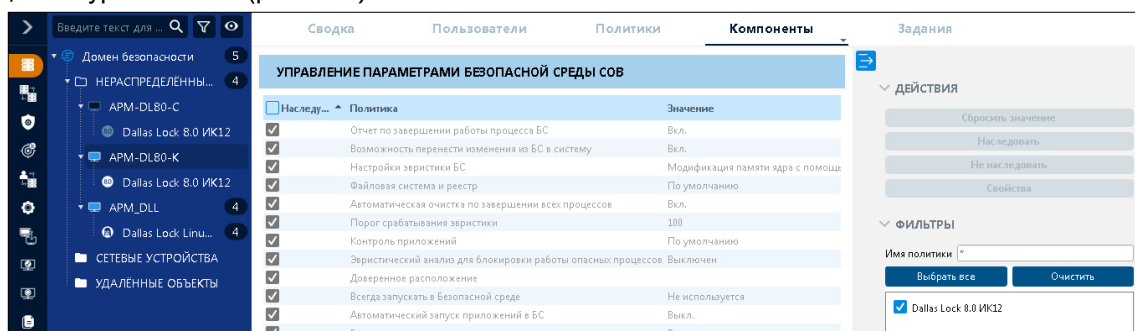


Рис. 180. Вкладка «Безопасная среда COB (песочница)» APM

Управление безопасной средой COB на уровне APM производится аналогично управлению безопасной средой для группы ДБ: возможен только просмотр параметров (см. [«Безопасная среда COB \(песочница\) для группы ДБ»](#)).

7.1.9 Средство обнаружения и реагирования APM

Вкладка *Средство обнаружения и реагирования* для выбранного APM позволяет управлять средством обнаружения и реагирования на уровне APM (рис. 181).

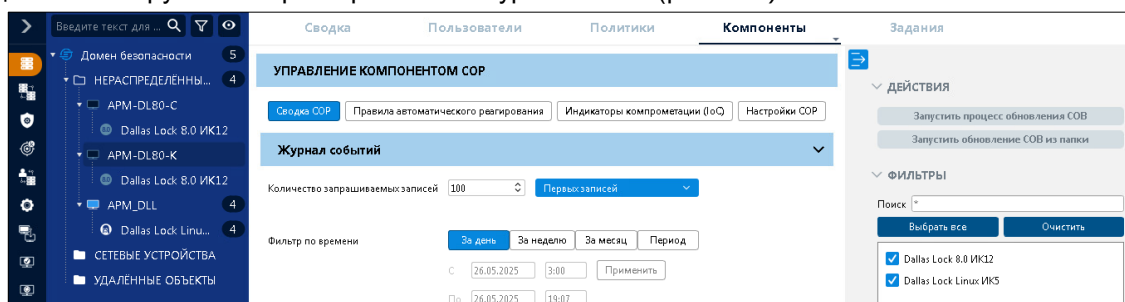


Рис. 181. Вкладка «Средство обнаружения и реагирования» APM

Управление средством обнаружения и реагирования на уровне АРМ производится аналогично управлению средством обнаружения и реагирования на уровне группы ДБ (см. [«Средство обнаружения и реагирования для группы ДБ»](#)).

7.1.10 Задания АРМ

Вкладка **Задания** для выбранного АРМ позволяет управлять заданиями на уровне АРМ (рис. 182).

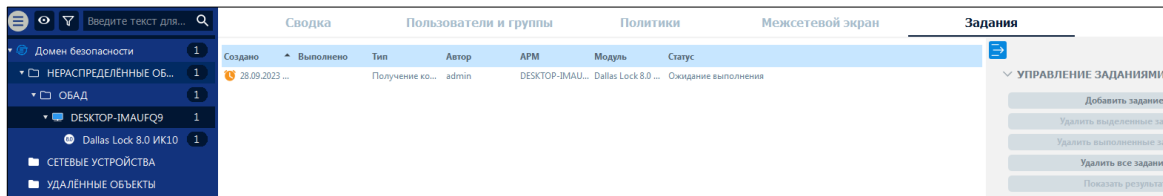


Рис. 182. Вкладка «Задания» АРМ

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 сети (данная функция доступна для модулей **СЗИ Dallas Lock 8.0**, **СЗИ НСД Dallas Lock Linux**, **Агент ЕЦУ**), необходимо:

1. На уровне Домена безопасности или группы (подгруппы) на вкладке *Сводка* на панели инструментов *Действия* нажать кнопку **Сканировать сеть** или воспользоваться контекстным меню в дереве ДБ.
2. Появится окно **Сканирование сети**, в котором необходимо выбрать вкладку *Модули*, ввести один IP-адрес или диапазон IP-адресов для сканирования и нажать кнопку **Сканировать** (рис. 183). Также возможен импорт адресов из файла, для чего необходимо нажать кнопку **Импорт из файла**, после чего выбрать файл формата txt, csv или html.

Рис. 183. Окно «Сканирование сети»



Импорт адресов можно произвести не из любого html-файла, а только из отчета, созданного **ЕЦУ**.

3. После нажатия кнопки **Сканировать** откроется окно сканирования сети и регистрации модулей (рис. 184). Процесс сканирования сети можно остановить нажатием на кнопку **Прервать**, полученные до прерывания процесса результаты при этом сохраняются.

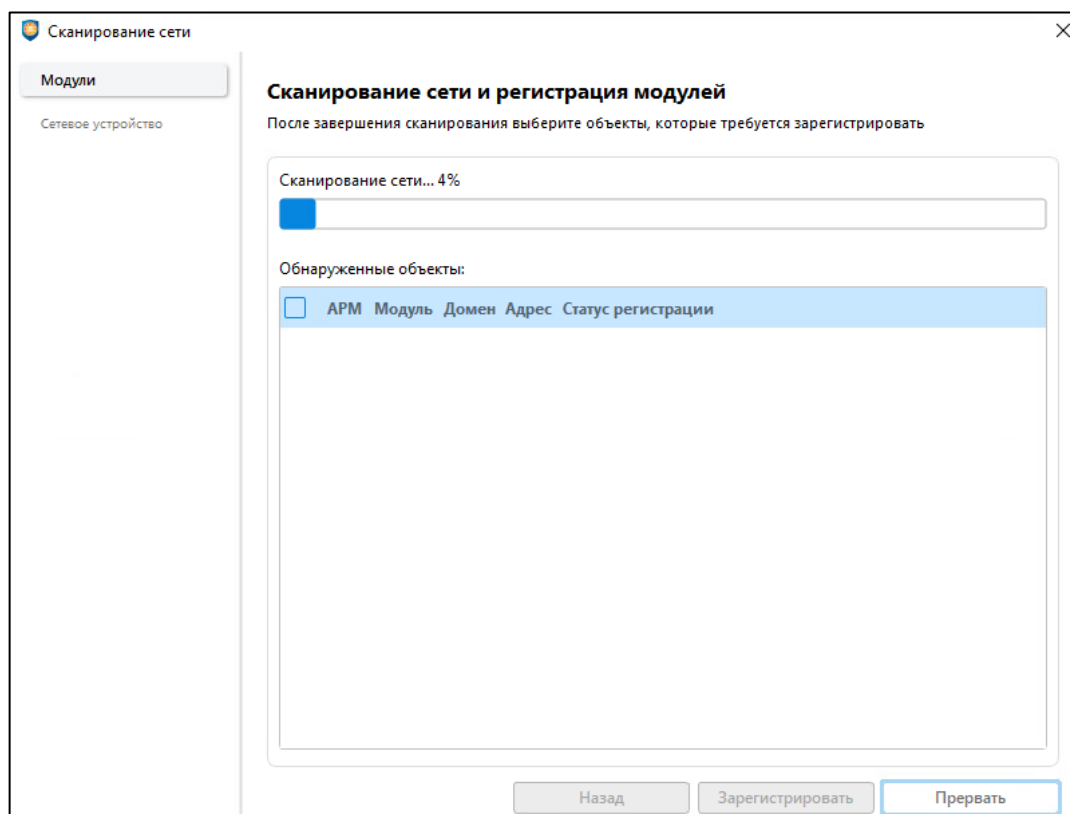


Рис. 184. Процесс сканирования сети

4. По завершении процесса сканирования из списка обнаруженных объектов можно выбрать те модули, которые необходимо зарегистрировать в ДБ, либо установить флаг возле столбца *APM* для выбора всех обнаруженных модулей (рис. 185).

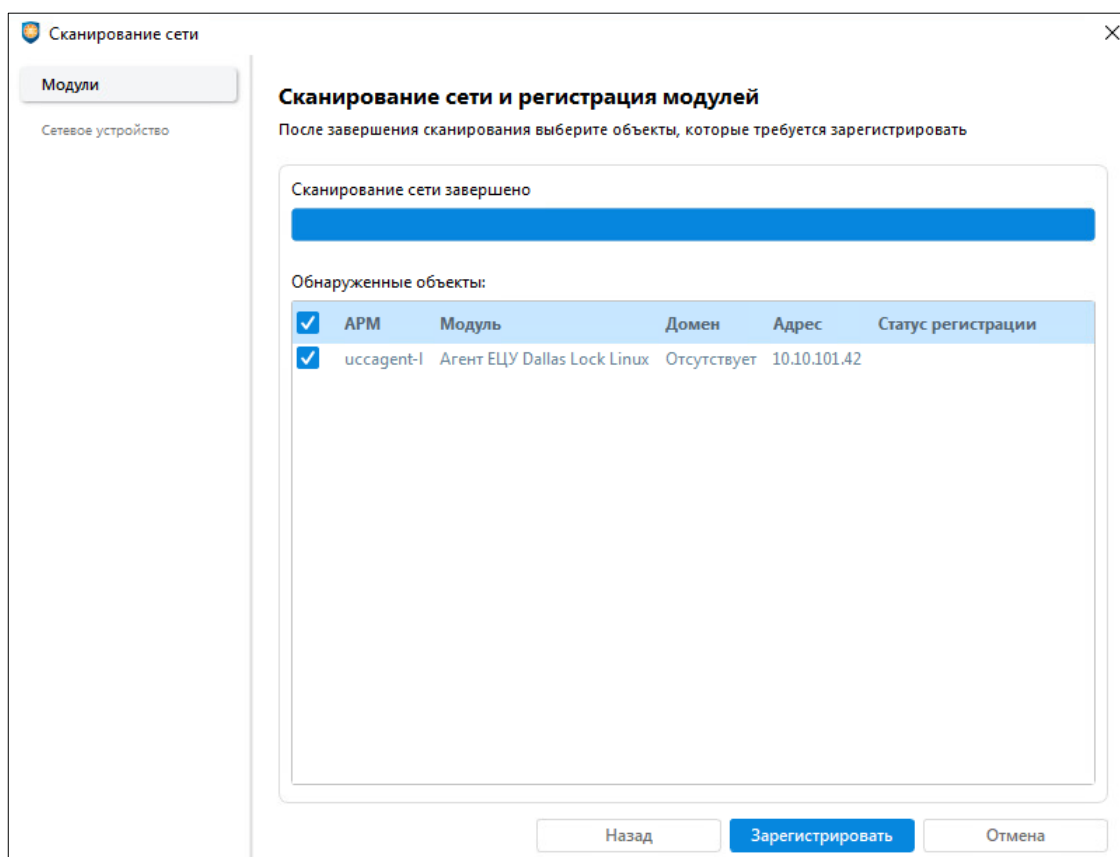


Рис. 185. Выбор объектов для регистрации в ДБ

После выбора регистрируемых модулей нажать кнопку **Зарегистрировать**. Процесс регистрации модулей также можно остановить нажатием на кнопку **Прервать**, полученные до прерывания процесса результаты при этом сохраняются.

5. Появится окно **Регистрация модулей**, в котором нужно ввести авторизационные данные администратора модуля и ключ доступа к ДБ (рис. 186).

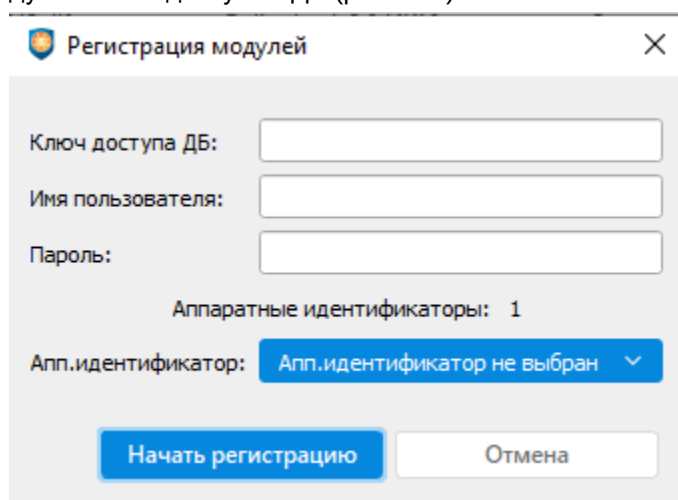


Рис. 186 Ввод данных для регистрации

Нажать кнопку **Начать регистрацию** после ввода всех данных.

6. Если введенные данные верны, то в статусе регистрации отобразится результат «ОК», и зарегистрированные модули появятся в дереве Домена безопасности в базовой группе «Нераспределенные объекты».



Зарегистрировать модули в ДБ **ЕЦУ** получится, только при условии, что на АРМ, где установлены данные модули, настроено разрешающее правило фильтрации на TCP-порты 17901 и 17903 на входящее соединение.

Перемещение модуля в дереве осуществляется перетаскиванием значка кнопкой мыши в поле другого значка (*Drag-and-drop*).

Имеется возможность добавить комментарий к модулю, для этого нужно нажать кнопку **Комментарий** на панели *Действия* или воспользоваться контекстным меню в дереве ДБ (рис. 187). Добавленный комментарий отобразится в разделе *Информация об объекте* вкладки *Сводка*.



Максимальная длина комментария к модулю составляет 256 символов.

Для вывода модуля из Домена безопасности **ЕЦУ** необходимо:

1. Выбрать пункт **Удалить модуль** из контекстного меню данного модуля в дереве ДБ (рис. 187), или воспользоваться командой **Удалить** на панели инструментов *Действия* вкладки *Сводка* на уровне модуля в дереве ДБ (рис. 188).

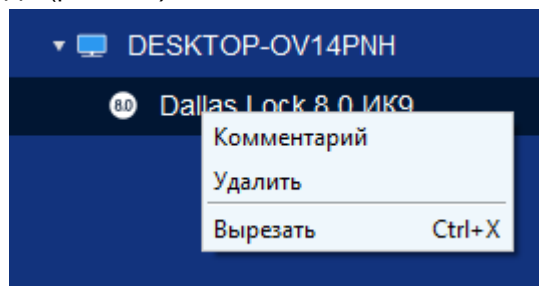


Рис. 187. Удаление модуля посредством контекстного меню

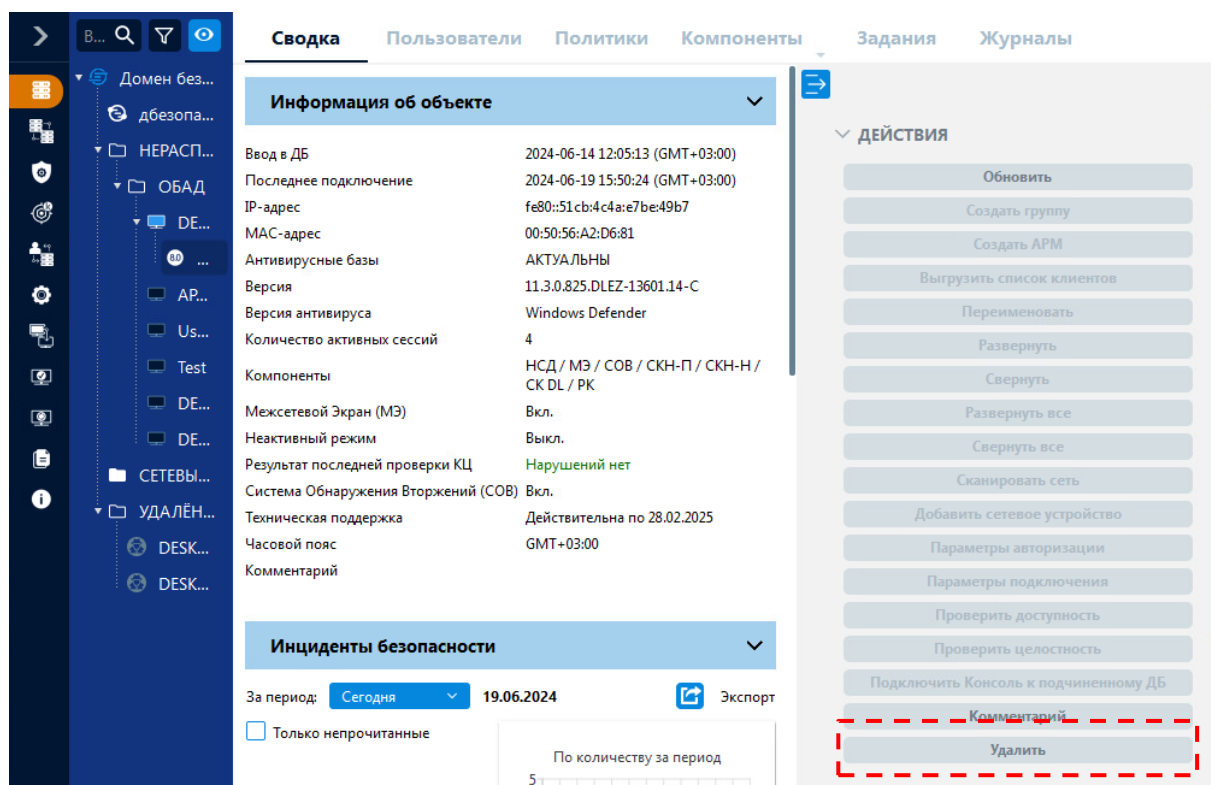


Рис. 188. Удаление посредством панели «Действия»

- 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.



В ЕЦУ реализована возможность работы с модулями, расположенными за NAT, в рамках одной сессии. Как только сессия завершится, связь с модулем разорвется. В следующий раз ЕЦУ сможет связаться с модулем, когда модуль создаст новую сессию.

8.1.1 Сводка модуля

Вкладка *Сводка* на уровне модуля отображает общее состояние модуля (рис. 189).

Рис. 189. 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.



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

8.1.2 Пользователи и группы модуля

Вкладка *Пользователи* 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. 190).



Рис. 190. Вкладка «Пользователи» 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»).



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*.

Для изменения категории пользователя или группы средствами **ЕЦУ** нужно выделить необходимого пользователя или группу, после на панели инструментов нажать кнопку **Сделать глобальной**. При этом имя модульного пользователя или модульной группы при смене категории не должно совпадать с существующими именами глобальных пользователей или 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. 191).

☒	Состояние	Учетная запись	Категория	Тип учетной записи ЕЦУ
☒		admin	Глобальная	Все
☒		admin	Модульная	DL8.0 ИК10
☒		anonymous	Глобальная	Система, DL8.0 ИК8, DL8.0

Рис. 191. Совпадение имен модульного и глобального пользователя



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. 192).

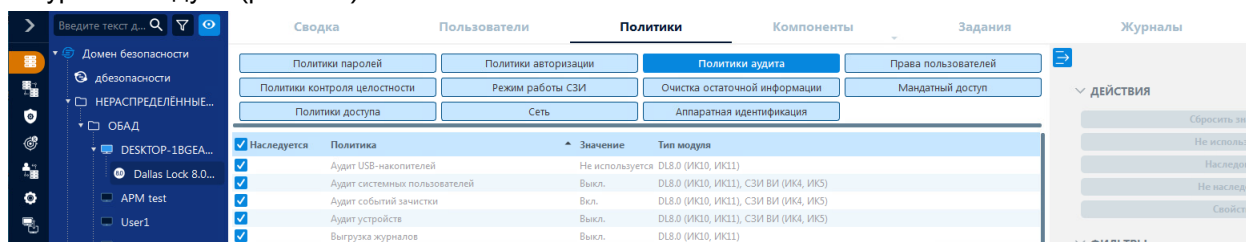


Рис. 192. Вкладка «Политики» модуля

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 Межсетевой экран модуля

Вкладка **Компоненты** → **Межсетевой экран** на уровне модуля позволяет управлять МЭ для модуля (рис. 193).

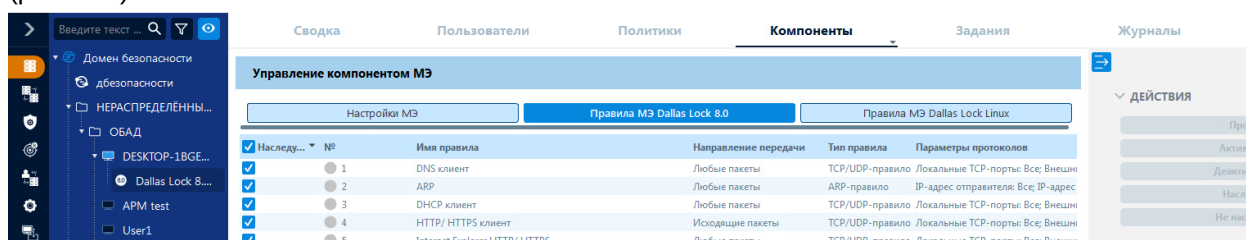


Рис. 193. Вкладка «Межсетевой экран» модуля

На уровне модуля доступны настройки МЭ, актуальные для данного типа модуля **ЕЦУ**.

Управление МЭ на уровне модуля производится аналогично управлению межсетевым экраном для ДБ (см. [«Межсетевой экран»](#)).

8.1.5 Система контроля накопителей модуля

Вкладка **Компоненты** → **Система контроля накопителей** на уровне модуля позволяет управлять накопителями для модуля (рис. 194).

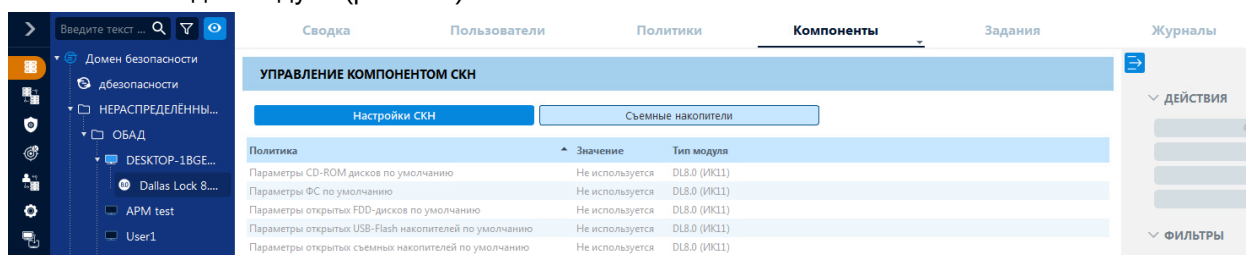


Рис. 194. Вкладка «Система контроля накопителей» модуля

Управление системой контроля накопителей на уровне модуля производится аналогично управлению системой контроля накопителей для ДБ (см. [«Система контроля накопителей»](#)).

8.1.6 Контроль ресурсов модуля

Вкладка **Компоненты** → **Контроль ресурсов** на уровне модуля позволяет управлять контролем ресурсов для модуля (рис. 195).

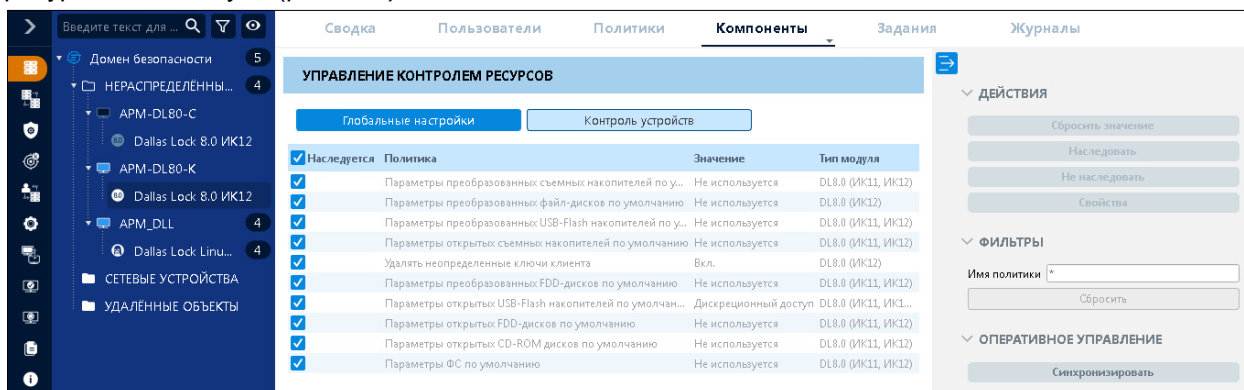


Рис. 195. Вкладка «Контроль ресурсов» модуля

Управление контролем ресурсов на уровне модуля производится аналогично управлению контролем ресурсов для ДБ (см. [«Контроль ресурсов»](#)).

8.1.7 Система обнаружения вторжений модуля

Вкладка **Компоненты** → **Система обнаружения вторжений** на уровне модуля позволяет управлять компонентом СОВ на уровне модуля (рис. 196).

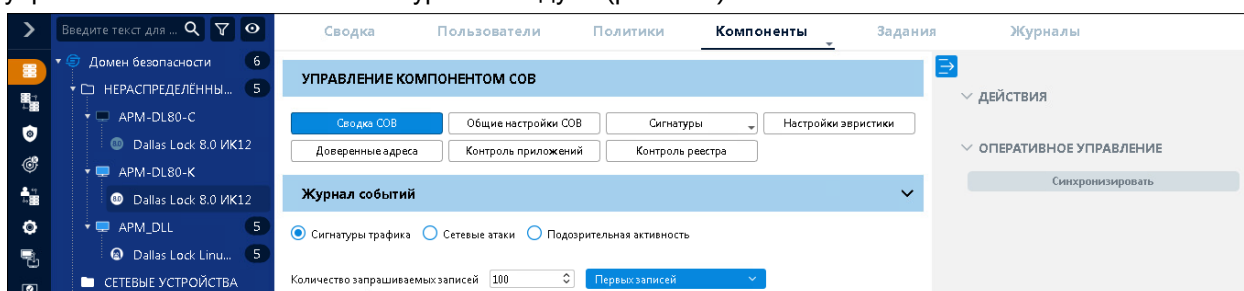


Рис. 196. Вкладка «Система обнаружения вторжений» модуля

Управление системой обнаружения вторжений на уровне модуля производится аналогично управлению компонентом СОВ для группы ДБ (см. [«Система обнаружения вторжений для группы ДБ»](#)).

8.1.8 Безопасная среда СОВ (песочница) модуля

Вкладка **Компоненты** → **Безопасная среда СОВ (песочница)** на уровне модуля позволяет управлять безопасной средой на уровне модуля (рис. 197).



Рис. 197. Вкладка «Безопасная среда СОВ (песочница)» модуля

Управление безопасной средой СОВ на уровне модуля производится аналогично управлению безопасной средой для группы ДБ: возможен только просмотр параметров (см. [«Безопасная среда СОВ \(песочница\) для группы ДБ»](#)).

8.1.9 Средство обнаружения и реагирования модуля

Вкладка **Компоненты** → **Средство обнаружения и реагирования** на уровне модуля позволяет управлять средством обнаружения и реагирования на уровне модуля (рис. 198).

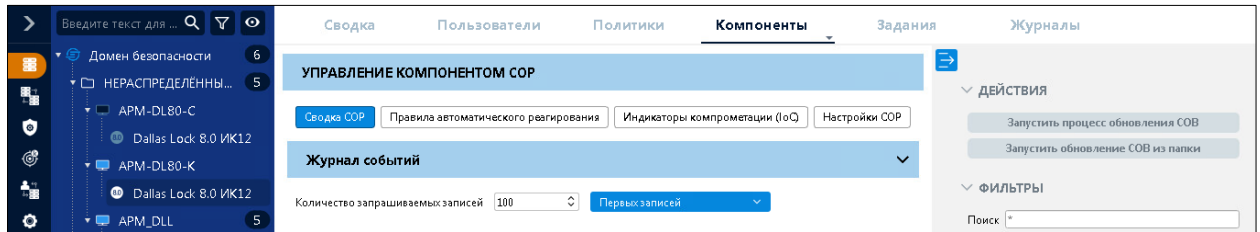


Рис. 198. Вкладка «Средство обнаружения и реагирования» модуля

Управление средством обнаружения и реагирования на уровне модуля производится аналогично управлению средством обнаружения и реагирования на уровне группы ДБ (см. [«Средство обнаружения и реагирования для группы ДБ»](#)).

8.1.10 Задания модуля

Вкладка **Задания** на уровне модуля позволяет управлять заданиями для модуля (рис. 199).

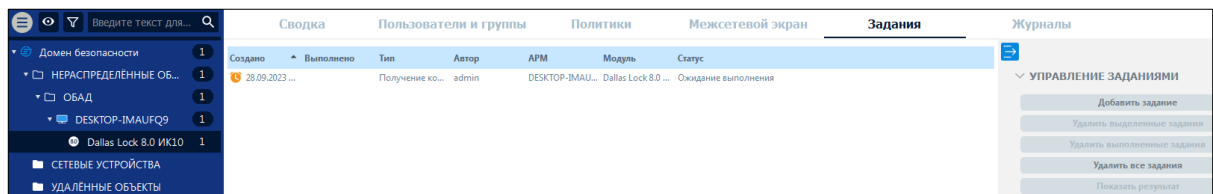


Рис. 199. Вкладка «Задания» модуля

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»](#)).

8.1.11 Журналы модуля

Вкладка **Журналы** для выбранного модуля позволяет просматривать журналы безопасности модуля (рис. 200).



Рис. 200. Вкладка «Журналы» модуля

Категории журналов на вкладке соответствуют названиям журналов на модулях.

Справа расположены панель инструментов **Фильтры** и панель инструментов **Действия**.

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

Отфильтрованные записи журнала можно сохранить в выбранную папку в нужном типе файла (TXT, CSV) с помощью команды **Экспортировать журнал** на панели инструментов **Действия**.

Для очистки журнала модуля используется команда **Очистить журнал**.

По команде **Обновить журнал** осуществляется обновление содержимого открытого журнала.

9 МОДУЛЬ СЗИ DALLAS LOCK 8.0-С/К

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»](#)).



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.



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».



Не рекомендуется вводить в **ЕЦУ** модуль **СЗИ Dallas Lock 8.0**, являющийся контроллером домена, так как:

- ввод контроллера домена под управление **ЕЦУ** приводит к созданию лишних доменных учетных записей;
- при совпадении логинов уже имеющихся доменных учетных записей с логинами локальных учетных записей **ЕЦУ** происходит изменение параметров доменных учетных записей (изменение пароля, списка групп), при этом изменение локальных учетных записей приводит к соответствующим изменениям доменных учетных записей.

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. 201).

Рис. 201. 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. 202).

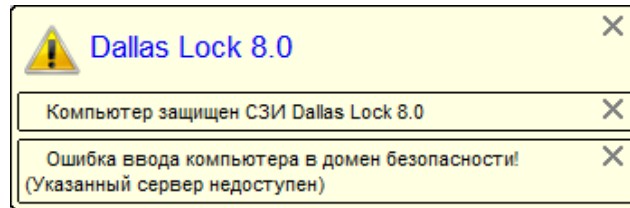


Рис. 202. Ошибка ввода компьютера в ДБ

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 **Сеть**. Выбрать параметр **Домен безопасности** и нажать на **Свойства** панели *Действия*. Откроется окно **Настройки домена безопасности** (рис. 203).

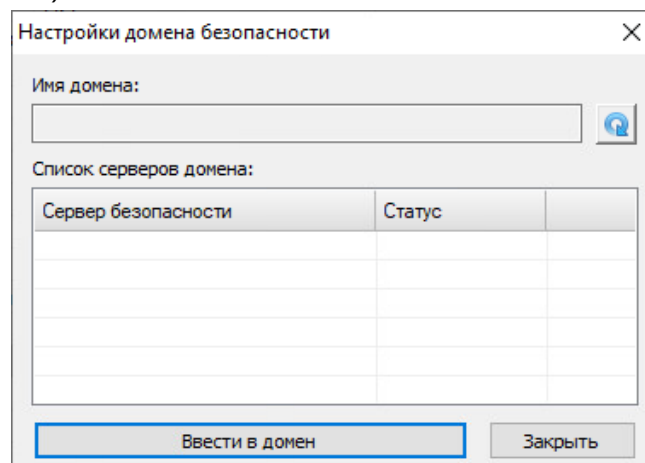


Рис. 203. Настройки ДБ

4. Нажать кнопку **Ввести в домен**. Откроется окно ввода клиента в домен безопасности (рис. 204), где необходимо:
 - выбрать пункт *Домен Единого центра управления*;
 - ввести имя сервера **ЕЦУ**;
 - указать ключ доступа к данному ДБ;
 - указать имя АРМ, в составе которого необходимо ввести модуль.

Рис. 204. 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. 205).

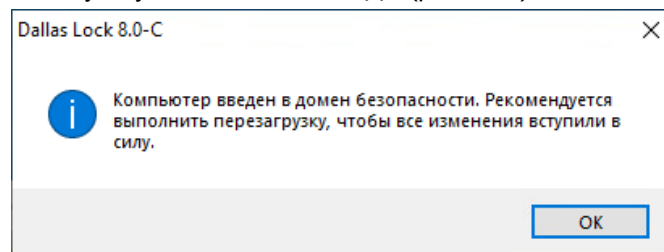


Рис. 205. Сообщение об успешном вводе модуля в ДБ

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 **Сеть**. Выбрать параметр **Домен безопасности** и нажать на **Свойства** панели *Действия*. Откроется окно **Настройки домена безопасности** (рис. 206).

Сервер безопасности	Статус
obad-win2016-34:17900	Подключен

Рис. 206. Настройки ДБ

3. Нажать **Вывести из домена**. Откроется окно для подтверждения вывода модуля из ДБ (рис. 207).

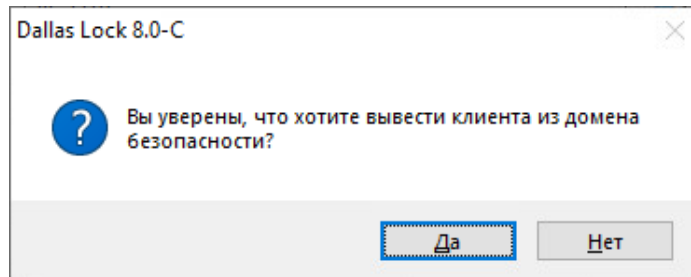


Рис. 207. Вывод модуля из ДБ

4. Нажать **Да**. Появится сообщение о том, что модуль успешно выведен из ДБ (рис. 208).

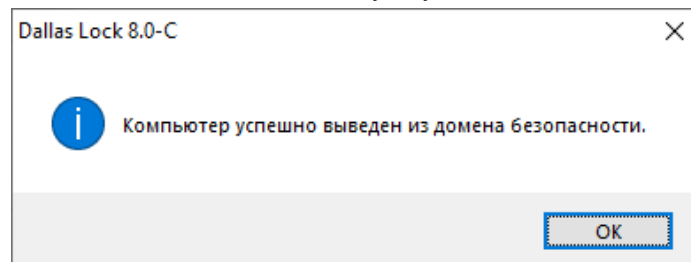


Рис. 208. Сообщение об успешном выводе модуля из ДБ

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



При отсутствии сетевого подключения к Службе **ЕЦУ**, модуль может быть выведен из Домена безопасности **ЕЦУ** принудительно. При этом, в Консоли **ЕЦУ** такой модуль продолжит отображаться, но его статус будет «Недоступен».

Поэтому, каждый модуль, выведенный из состава ДБ во время отсутствия связи со Службой **ЕЦУ**, необходимо дополнительно удалять вручную из Консоли **ЕЦУ**.

9.3 Удаленное развертывание СЗИ Dallas Lock 8.0

Существует возможность выполнить установку **Dallas Lock 8.0** централизованно на один или несколько компьютеров, расположенных в одной ЛВС.

Удаленная установка возможна в следующих вариантах:

- централизованно — для группы компьютеров, имеющих одинаковые имена и пароли администратора ОС;
- для компьютеров, имеющих индивидуальные имя и пароль администратора ОС, удаленную установку следует выполнять отдельно от других.

9.3.1 Удаленное развертывание с помощью консоли ЕЦУ



По умолчанию в операционных системах начиная с Windows 7 доступ к удаленному компьютеру под локальной учетной записью запрещен. Подробную информацию об этом ограничении можно найти на официальном сайте Справки и поддержки компании Microsoft по адресу <https://support.microsoft.com/kb/951016> (на английском языке).

Для разрешения удаленного подключения под локальной учетной записью необходимо в редакторе реестра по пути `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` создать ключ типа `dword` с именем `LocalAccountTokenFilterPolicy` со значением «1» («LocalAccountTokenFilterPolicy»=dword:00000001) и перезагрузить компьютер. В крупных сетях с AD данное значение можно распространить через политики.

По умолчанию удаленное развертывание выполняется через порт 445. Для этого на целевых ТС в Брандмауэре Windows необходимо разрешить входящие подключения для порта 445.

Для нескольких целевых ТС централизованную удаленную установку можно осуществить только при выполнении следующих условий:

- целевые ТС входят в тот же домен AD или LDAP, что и APM с **ЕЦУ Dallas Lock**;
- известны имя пользователя и пароль доменной учетной записи с правами администратора домена.

Для ввода клиента в домен безопасности **ЕЦУ** в поле определения домена указывается имя пользователя и домен, в связи с чем на клиенте **СЗИ НСД Dallas Lock 8.0** не допускается наличие пробела в имени пользователя ОС.

На клиенте **СЗИ НСД Dallas Lock 8.0** не поддерживаются полные имена домена — не допускается наличие точки в имени домена. При необходимости указании доменного логина в мастере разворачивания **DL8.0** используйте запись вида `domain\user`.

Для удаленной установки **СЗИ НСД Dallas Lock 8.0** на клиенте для учетной записи администратора должен быть задан пароль. Установку необходимо осуществлять по протоколу IPv4, на момент обновления и установки модулей необходимо отключить протокол IPv6 на APM с консолью **ЕЦУ**. Далее необходимо выполнить следующие шаги:

1. Перед централизованной установкой необходимо разместить на компьютере, на котором запущена консоль **ЕЦУ**, дистрибутив **СЗИ НСД Dallas Lock 8.0**.
2. Запустить консоль **ЕЦУ** от имени администратора.
3. Далее необходимо открыть главное меню консоли **ЕЦУ** и выбрать **Удаленная установка**. Откроется страница мастера удаленной установки (рис. 209) из списка выбрать *Dallas Lock 8.0* и нажать кнопку **Далее**.

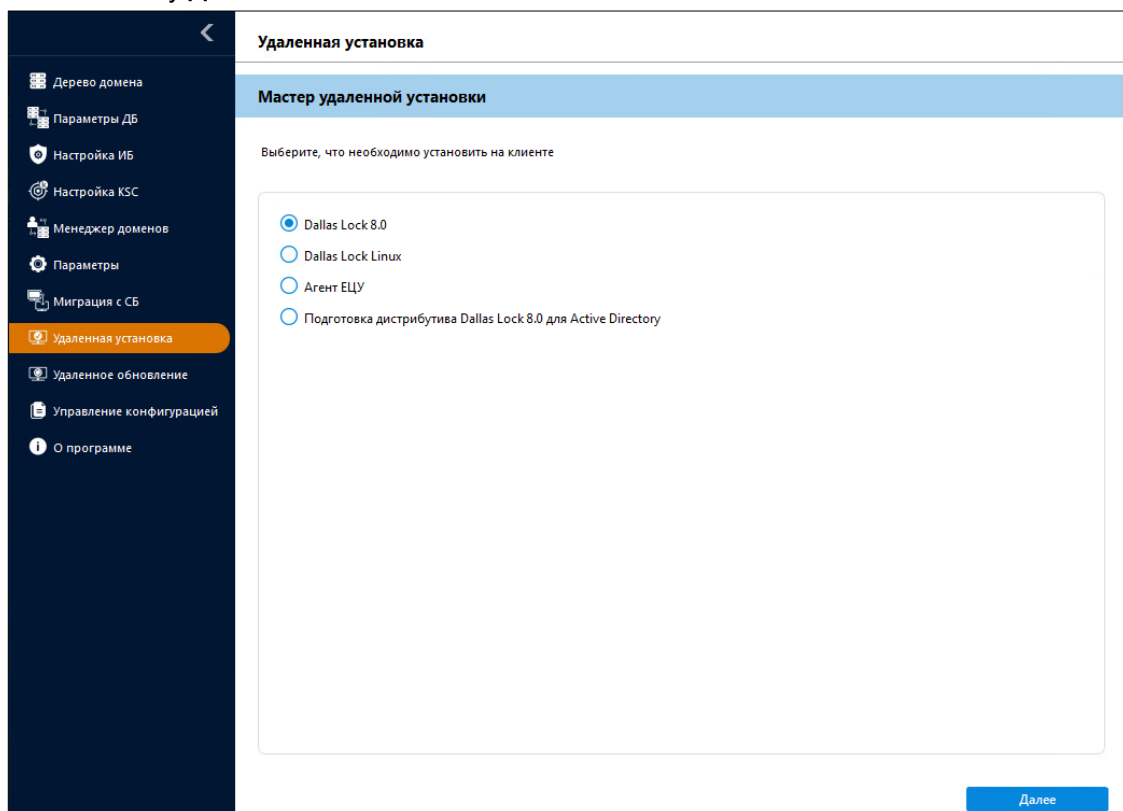


Рис. 209. Мастер удаленной установки

На открывшейся странице необходимо добавить целевые ТС для удаленного развертывания. ТС можно добавить одним из следующих способов, через:

- ручной ввод адреса — для этого нужно заполнить поля *Порт* и «Введите IP-адрес или сетевое имя компьютера», затем нажать кнопку **Добавить компьютер** (рис. 210);
- импорт из файла — нажать **Импорт из файла** и прикрепить текстовый файл со списком IP-адресов целевых ТС;
- файл списка клиентов — нажать **Импорт из файла** и выбрать файл со списком заранее выгруженных клиентов.



Для файла с IP-адресами возможен следующий формат списка: в каждой строке файла может быть указан только один IP-адрес без дополнительных символов.

Пример:

```
192.168.0.1
192.168.0.35
10.10.112.55
```

Рис. 210. Список целевых ТС для удаленного развертывания СЗИ НСД Dallas Lock 8.0

Кнопка **Удалить** необходима для удаления добавленных ранее IP-адресов.

После добавления целевых ТС в список необходимо нажать кнопку **Далее**.

4. Заполнить параметры установки, которые будут применены к модулям в процессе активации **СЗИ НСД Dallas Lock 8.0** (рис. 211):

- логин и пароль администратора ОС на целевых ТС;
- логин и пароль суперпользователя (опционально).

1 2 3 4 5

Мастер удаленной установки Dallas Lock 8.0

Ввод авторизационных данных
Учетные данные администратора ОС компьютеров клиентов

Имя
Допустимые форматы ввода имени: user или domain\user

Пароль

☐ Создать нового пользователя в качестве администратора ИБ

Имя
Формат допускает только ввод имени без домена

Пароль

Подтверждение пароля

Назад Далее Отмена

Рис. 211. Параметры установки СЗИ НСД Dallas Lock 8.0

После заполнения всех необходимых полей нужно нажать кнопку **Далее**.

5. На следующей странице (рис. 212) необходимо указать:

- путь к исходному дистрибутиву **СЗИ НСД Dallas Lock 8.0**;
- номер лицензии, который указан на обложке футляра;
- код технической поддержки, который указан в письме, отправленном на электронную почту.

При необходимости применения определенной конфигурации для дистрибутива, можно поставить флаг *Сохранять настройки от предыдущей установки* или указать путь к файлу конфигурации для **СЗИ Dallas Lock 8.0**. Если поле не отмечено флагом и не указан путь к файлу конфигурации, применяется конфигурация «По умолчанию», что имеет смысл только при обновлении.

Для ввода модулей в Домен безопасности **ЕЦУ** сразу после установки, можно поставить флаг *Ввод в домен безопасности ЕЦУ*, указать имя сервера **ЕЦУ** и ключ доступа к ДБ. Затем нажать **Далее**.

Если данные для ввода модуля в ДБ **ЕЦУ** (в том числе ключ доступа) были указаны неверно, то установка будет приостановлена. Кнопка **Далее** будет неактивна до тех пор, пока данные для ввода в ДБ **ЕЦУ** не будут введены верно. Чтобы продолжить установку без ввода модуля в ДБ **ЕЦУ** необходимо снять флаг *Ввод в домен безопасности ЕЦУ*.

1 2 3 4 5

Мастер удаленной установки Dallas Lock 8.0

Параметры установки
Выбор установочного файла и параметров установки

Исходный дистрибутив

Номер лицензии

Код техподдержки

☐ Сохранять настройки от предыдущей установки

Файл конфигурации

☐ Ввод в домен безопасности ЕЦУ

Имя сервера

Ключ доступа к ДБ

Рис. 212. Выбор установочного файла СЗИ НСД Dallas Lock 8.0

6. На следующей странице (рис. 213) можно настроить дополнительные параметры установки, такие как:

- перезагрузка удаленного компьютера после установки. Поставленный на странице флаг позволяет автоматически перезагрузить компьютер после завершения установки **СЗИ Dallas Lock 8.0** по истечении установленного времени, иначе компьютер должен быть перезагружен пользователем самостоятельно;
- сообщение для пользователей. Сообщение, указанное на данной странице, будет повторяться с заданным интервалом, для пользователей, на чьих компьютерах производится установка **СЗИ Dallas Lock 8.0**.

Затем нажать кнопку **Установить**.

1 2 3 4 5

Мастер удаленной установки Dallas Lock 8.0

Процесс установки
Выбор дополнительных параметров установки

☒ Перезагрузить удаленный компьютер после установки

Перезагрузить через (мин.)
Диапазон от 1 до 999999

Сообщение для пользователей

Повторять сообщение через (мин.)
Диапазон в минутах, 0 - не повторять

Рис. 213. Дополнительные параметры установки СЗИ НСД Dallas Lock 8.0

7. Далее можно просматривать состояние процесса установки для каждого клиента (рис. 214).

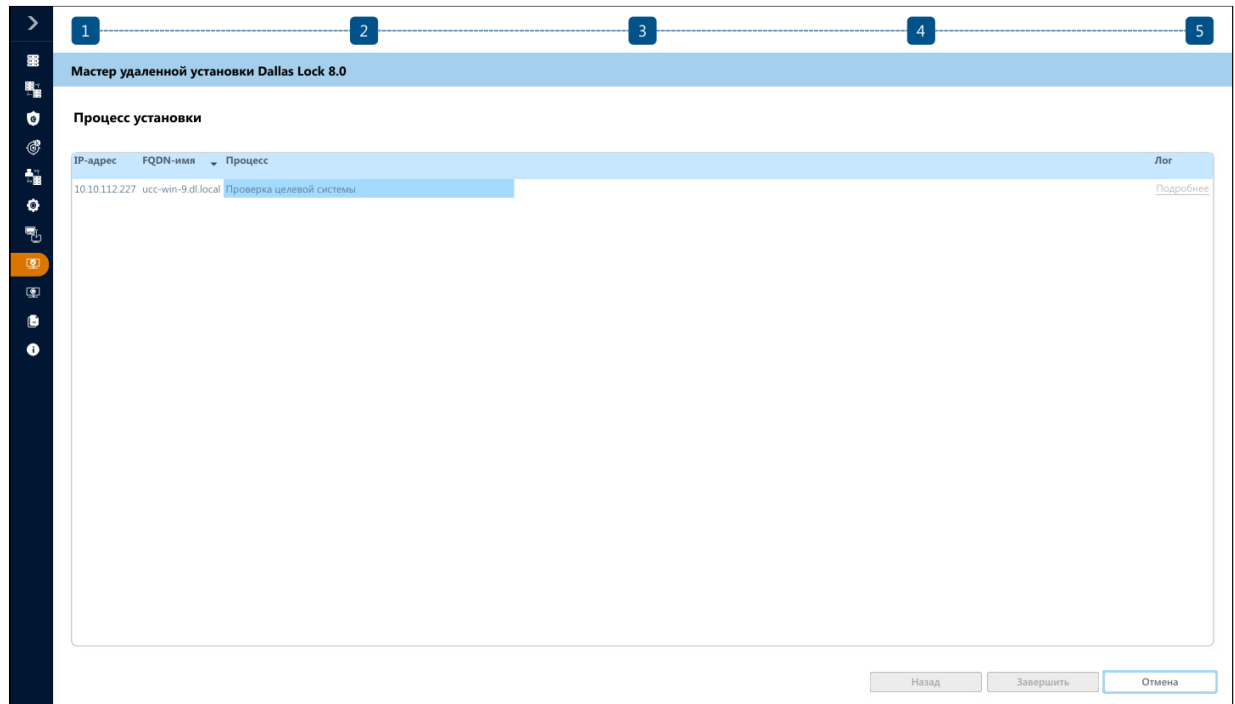


Рис. 214. Информация о ходе централизованной установки средствами ЕЦУ

8. По окончании процесса централизованной установки появятся соответствующие комментарии удачного или не удачного завершения операции.



При удаленной установке объекты с одинаковыми именами объединяются, вне зависимости от регистра. После объединения отображается имя, которое было ранее сохранено в ЕЦУ.

9.3.2 Централизованная установка средствами Active Directory

Средствами Microsoft Windows возможна централизованная установка **Dallas Lock 8.0** на рабочие станции, входящие в состав Контроллера домена. Необходимые для установки действия включают в себя:

- Формирование файла установки в консоли **ЕЦУ**.
- Создание точки распространения на Контроллере домена.
- Создание объекта групповой политики для централизованной установки средствами AD.
- Конфигурация и применение групповой политики.

9.3.2.1 Подготовка 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**.



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** и выбрать **Удаленная установка**. Откроется страница мастера удаленной установки (рис. 215)

из списка выбрать *Подготовка дистрибутива Dallas Lock 8.0 для Active Directory* и нажать кнопку **Далее**.

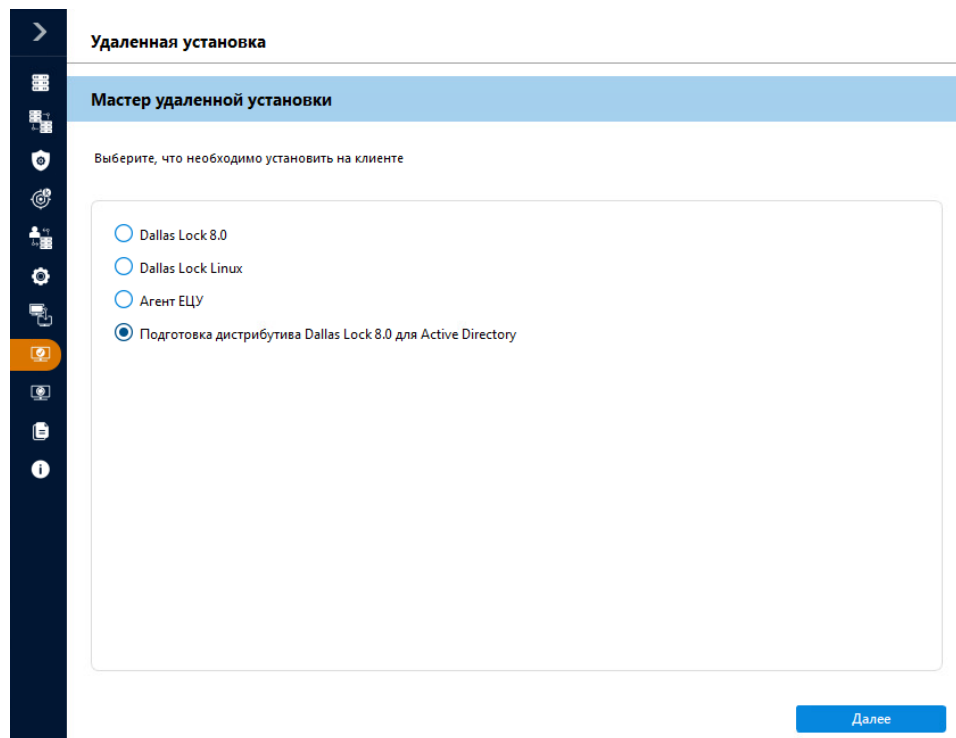


Рис. 215. Мастер удаленной установки

На странице заполнить учетные данные администратора ОС компьютеров клиентов (рис. 216). 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**.

Рис. 216. Мастер подготовки дистрибутива СЗИ Dallas Lock 8.0 для AD

После заполнения полей нажать кнопка **Далее** для перехода к следующему шагу.

На втором шаге подготовки дистрибутива необходимо указать параметры удаленной установки, которые будут применены к целевым ТС после активации **СЗИ Dallas Lock 8.0** (рис. 217):

- Путь к исходному дистрибутиву **СЗИ Dallas Lock 8.0**.
- номер лицензии, который указан на обложке футляра;
- код технической поддержки, который указан в письме, отправленном на электронную почту.

При необходимости применения определенной конфигурации для дистрибутива, можно поставить флаг *Сохранять настройки от предыдущей установки* или указать путь к файлу конфигурации для **СЗИ Dallas Lock 8.0**. Если поле не отмечено флагом и не указан путь к файлу конфигурации, применяется конфигурация «По умолчанию», что имеет смысл только при обновлении.

При необходимости ввода в домен **ЕЦУ** можно поставить флаг *Ввод в домен безопасности ЕЦУ*, указать имя сервера **ЕЦУ** и ключ доступа к ДБ.

После заполнения полей нажать кнопку **Далее** для перехода к следующей странице.

The screenshot displays the 'Мастер подготовки дистрибутива Dallas Lock 8.0 для Active Directory' wizard. The current step is 'Параметры установки' (Installation parameters), which involves selecting the installation file and parameters. The form includes the following elements:

- Исходный дистрибутив** (Source distribution): A text input field with a 'Выбрать' (Select) button.
- Номер лицензии** (License number): A text input field.
- Код техподдержки** (Support code): A text input field.
- Сохранять настройки от предыдущей установки** (Save settings from previous installation): An unchecked checkbox.
- Файл конфигурации** (Configuration file): A text input field with a 'Выбрать' (Select) button.
- Ввод в домен безопасности ЕЦУ** (Enter ECU security domain): An unchecked checkbox.
- Имя сервера** (Server name): A dropdown menu currently showing 'DESKTOP-1BGEAP2:17900'.
- Ключ доступа к ДБ** (Database access key): A text input field.
- Navigation buttons**: 'Назад' (Back), 'Далее' (Next), and 'Отмена' (Cancel) buttons at the bottom right.

Рис. 217. Ввод параметров для дистрибутива

На следующем шаге подготовки дистрибутива указываются параметры перезагрузки при установке (рис. 218). Поставленный на странице флаг *Перезагрузить удаленный компьютер после установки* позволяет автоматически перезагрузить компьютер после завершения установки **СЗИ Dallas Lock 8.0** по истечению установленного времени, иначе компьютер должен быть перезагружен пользователем самостоятельно.

Также на данной странице задается произвольное сообщение и интервал, через который оно будет повторяться, для пользователей, на чьих компьютерах производится установка **СЗИ**. Для продолжения подготовки дистрибутива нажать **Подготовить**.

1 **2** **3** **4**

Мастер подготовки дистрибутива Dallas Lock 8.0 для Active Directory

Дополнительные параметры установки
Выбор дополнительных параметров установки

☐ Перезагрузить удаленный компьютер после установки

Перезагрузить через (мин.)
Диапазон от 1 до 999999

Сообщение для пользователей

Повторять сообщение через (мин.)
Диапазон в минутах, 0 - не повторять

Рис. 218. Настройка параметров перезагрузки

Появится страница с сообщением об успешном обновлении дистрибутива для установки AD. Дистрибутив будет расположен по пути, указанному на странице (рис. 219).

1 **2** **3** **4**

Мастер подготовки дистрибутива Dallas Lock 8.0 для Active Directory

Результат подготовки

Обновление msi успешно завершено.
ВАЖНО: При настройке групповой политики на контроллере домена, дистрибутив для установки необходимо добавить в раздел "Конфигурация компьютера".

Дистрибутив расположен:
C:/Users/user/AppData/Local/Temp/DallasLock8.0C-AD.msi

Рис. 219. Завершение подготовки дистрибутива

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

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

9.3.2.2 Создание объекта групповой политики

На контроллере домена необходимо создать объект групповой политики для развертывания Dallas Lock 8.0.

1. Для этого в службах AD необходимо открыть оснастку **Active Directory — пользователи и компьютеры**. Далее найти или создать подразделение, которое будет содержать компьютеры, на которые требуется установить систему защиты (рис. 220, рис. 221).

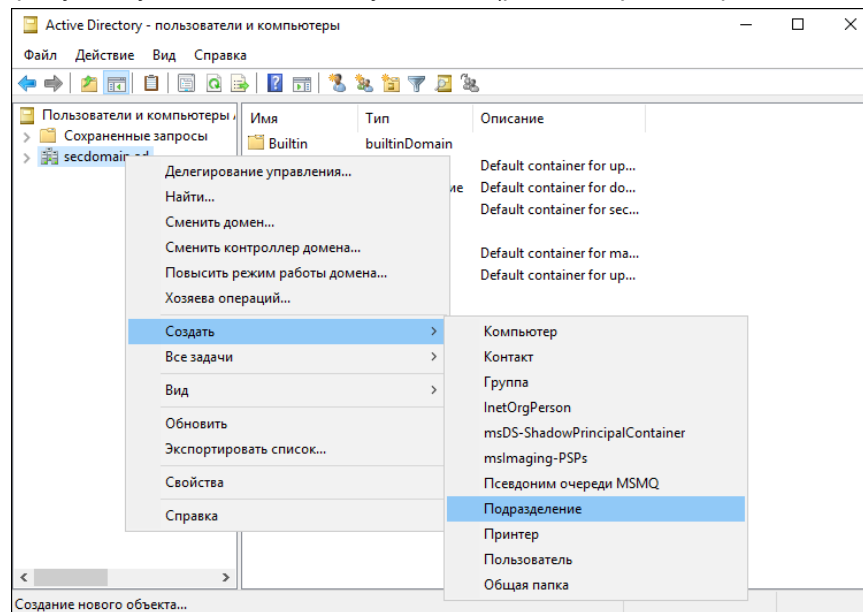


Рис. 220. Создание подразделения в AD

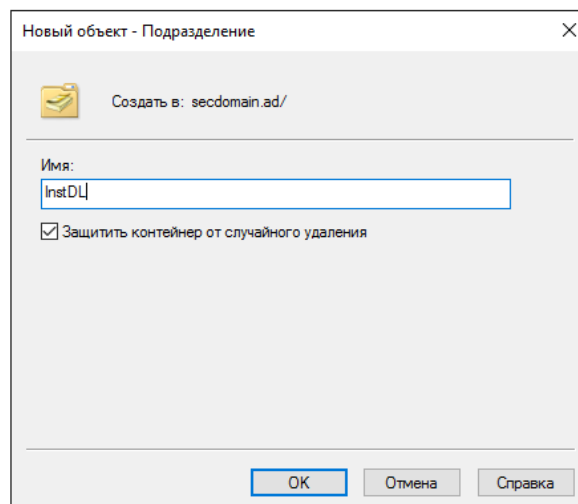


Рис. 221. Имя нового подразделения в AD

- В это подразделение перенести необходимые компьютеры с помощью функции из контекстного меню **Переместить** (рис. 222, рис. 223).

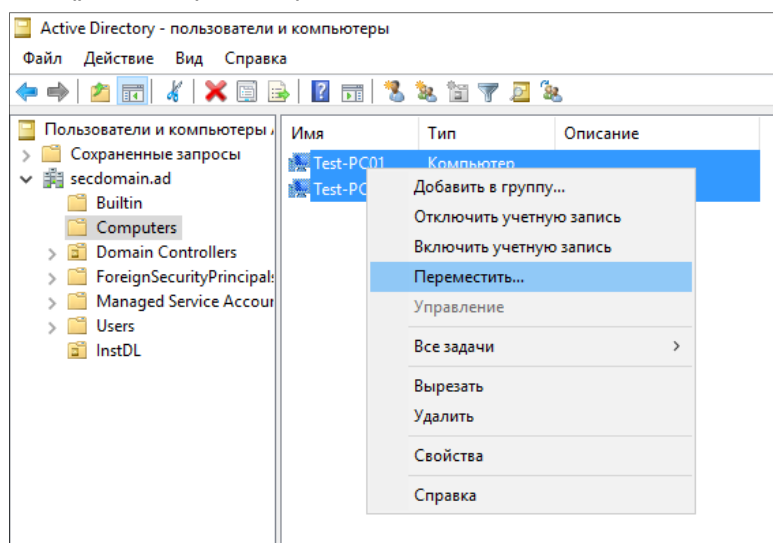


Рис. 222. Пункт контекстного меню «Переместить...»

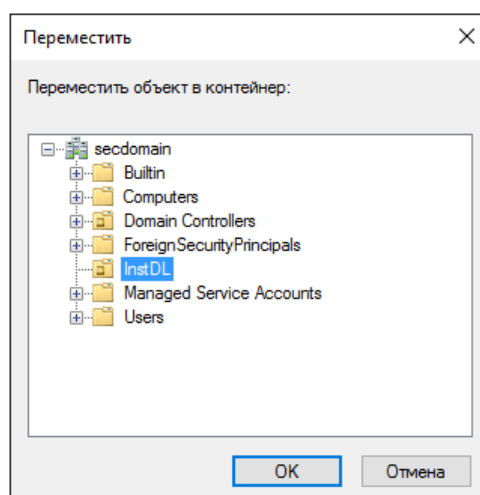


Рис. 223. Перенос рабочих станций в подразделение

В созданном подразделении появится список с необходимыми компьютерами. Таким образом, создан объект групповой политики для развертывания ПО.



Для корректной удаленной установки msi-файла **СЗИ Dallas Lock 8.0**, подразделение следует создавать именно для компьютеров, а не для пользователей.

9.3.2.3 Создание групповой политики

Теперь для выбранного подразделения необходимо создать групповую политику, с помощью которой и будет происходить удаленная установка системы защиты. Создание и редактирование групповых политик объектов AD в Windows Server осуществляется из отдельной консоли.

- 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. 224).

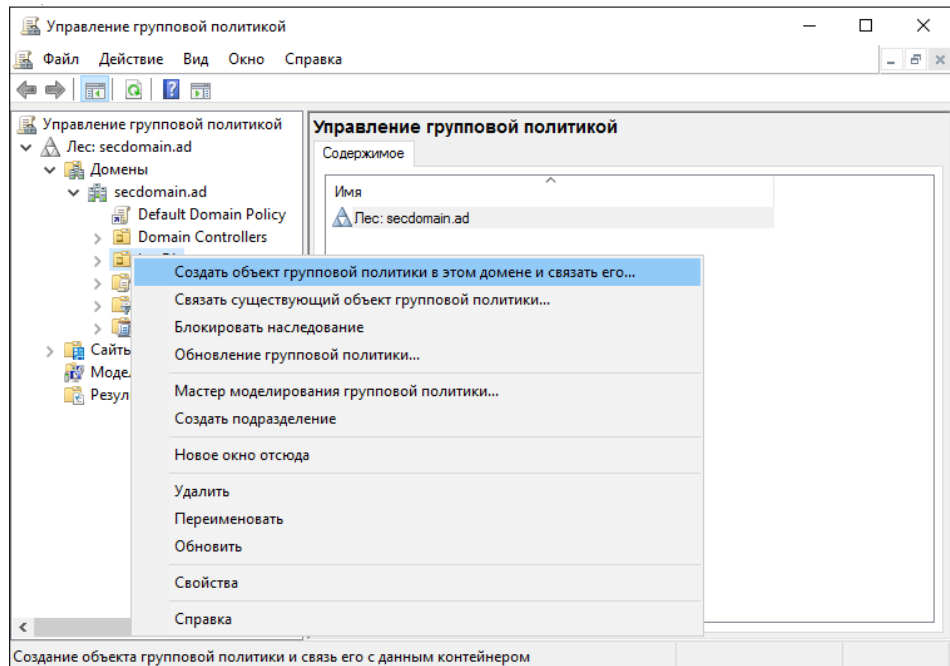


Рис. 224. Консоль управления групповой политикой на Windows Server

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. 225).

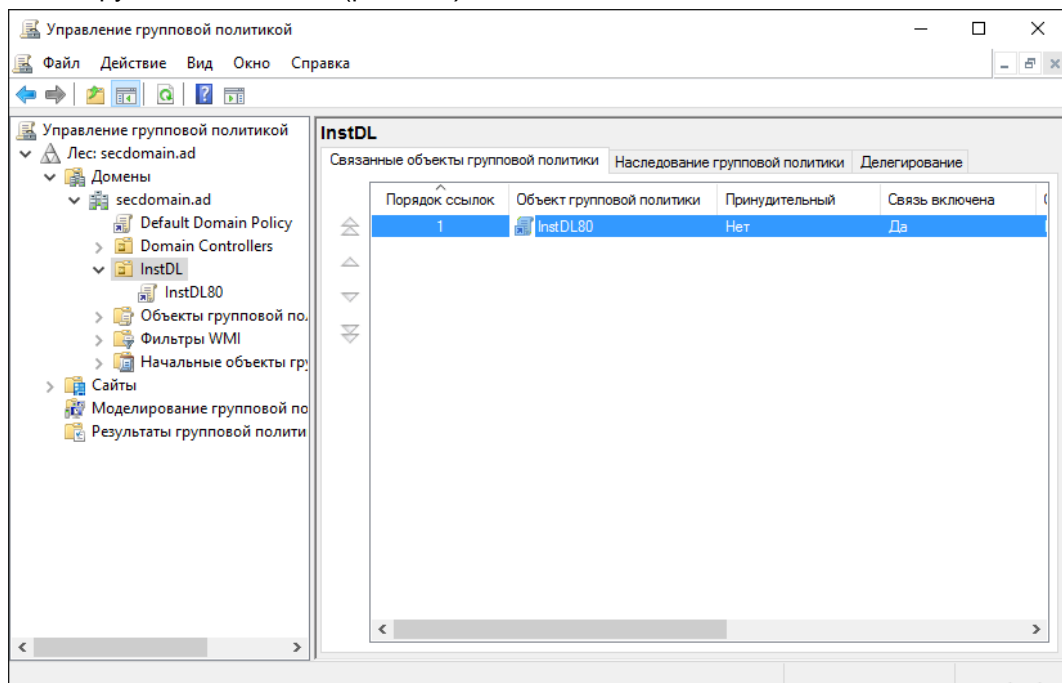


Рис. 225. Новый объект групповой политики, связанный с подразделением

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

9.3.2.4 Создание источника установки

Теперь необходимо определить так называемый источник распространения пакета или установки сформированного msi-файла на сервере Windows. Это должна быть общая сетевая папка, к которой разрешен доступ следующим группам пользователей:

- администраторы;
- прошедшие проверку;
- пользователи домена.

Рекомендуется использовать в качестве точки распространения контейнер местонахождения самой групповой политики. Определить путь к папке со скриптами групповой политики можно различными способами.

1. Вначале необходимо определить уникальное имя групповой политики.

В ОС Windows Server определить уникальное имя (уникальный код) групповой политики можно через **консоль управления групповыми политиками**, выделив необходимую политику и открыв вкладку свойств *Сведения* (рис. 226).

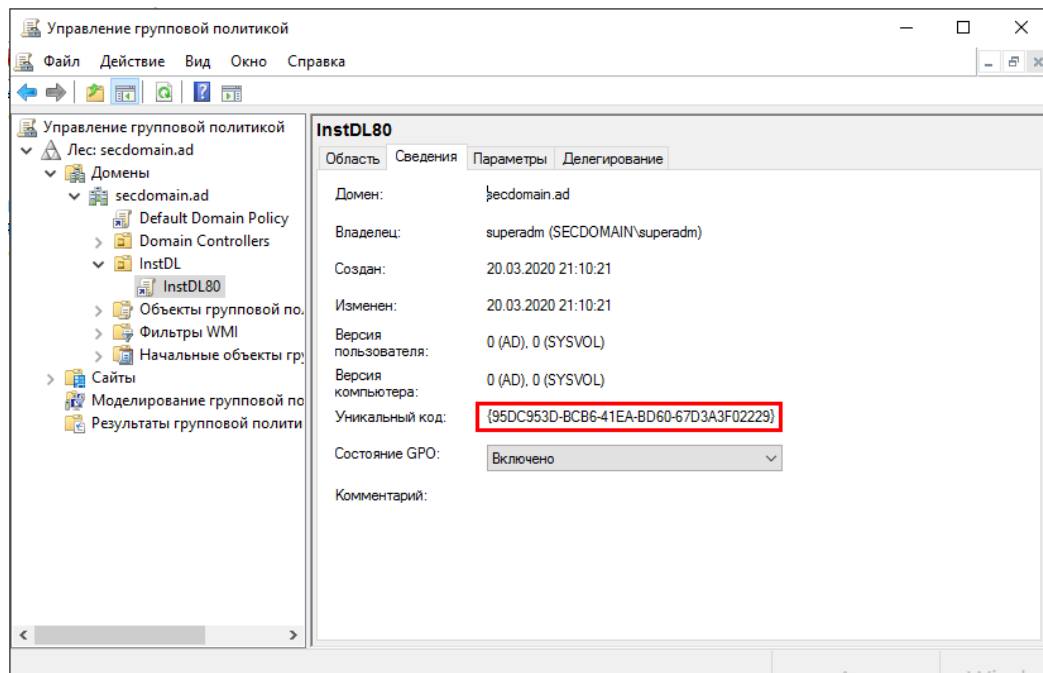


Рис. 226. Новый объект групповой политики, связанный с подразделением

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. 227).

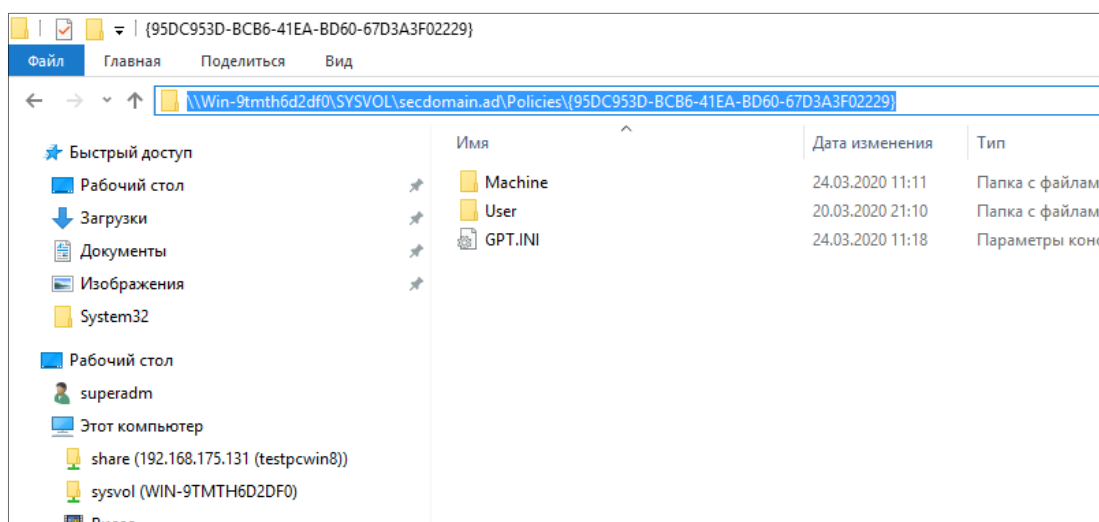


Рис. 227. Расположение папки-контейнера групповой политики

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. 228).

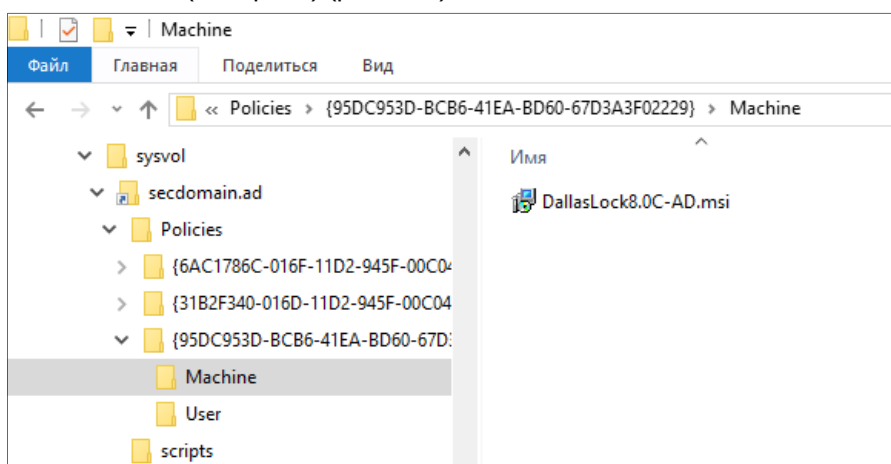


Рис. 228. Перенос msi-дистрибутива в папку групповой политики

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

9.3.2.5 Настройка групповой политики

Теперь необходимо изменить созданный объект групповой политики для развертывания ПО.

1. В Windows Server редактор объектов групповой политики открывается в консоли управления групповыми политиками. Необходимо выбрать созданную политику правым щелчком мыши и нажать в появившемся контекстном меню **Изменить** (рис. 229).

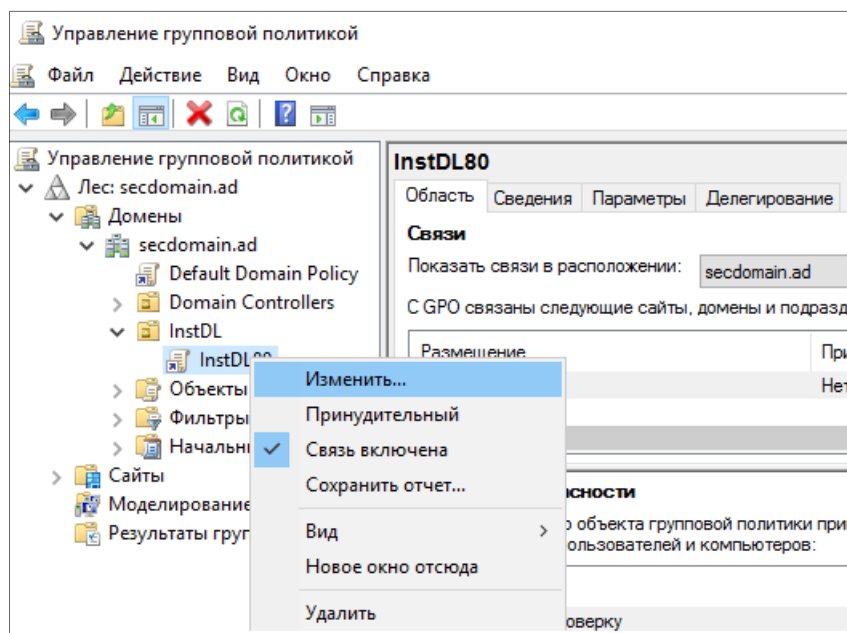


Рис. 229. Вызов контекстного меню в Консоли управления групповой политикой

Откроется необходимое окно редактора. В данном окне в дереве параметров требуется выбрать установку программ (рис. 230).

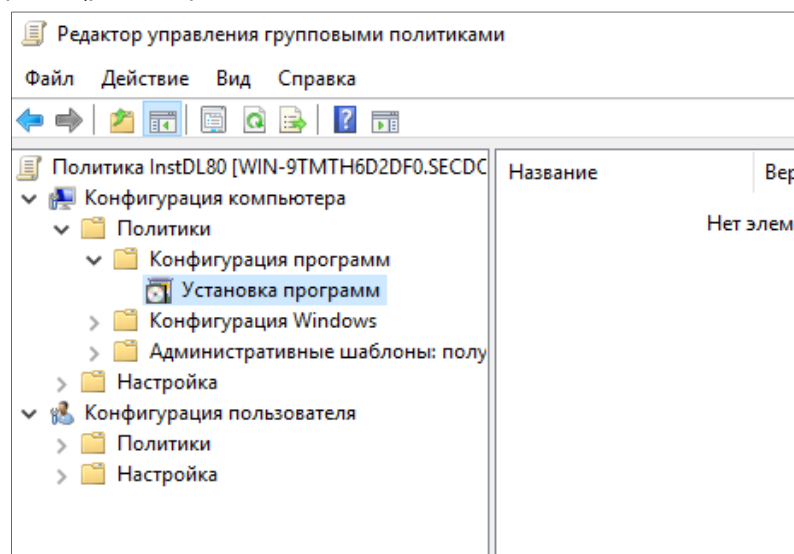


Рис. 230. Окно редактора групповой политики

- Далее в правом поле окна установки программ с помощью контекстного меню создать пакет установки: нажать последовательно **Создать, Пакет...** (рис. 231).

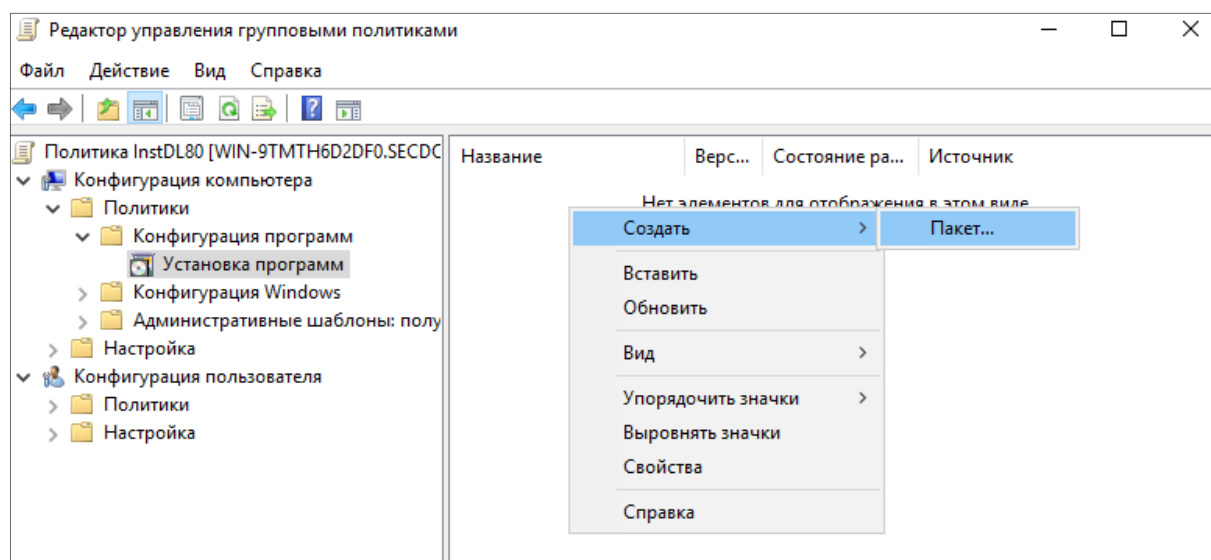


Рис. 231. Создание пакета конфигурации

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. 232).

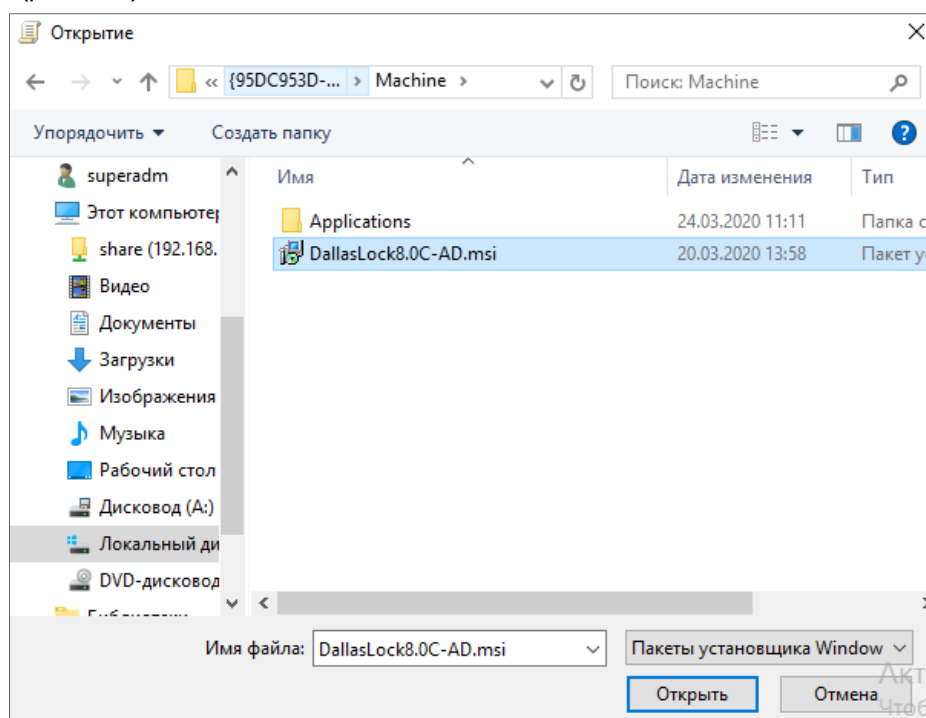


Рис. 232. Выбор расположения пакета установки

4. Выбрать msi-пакет и нажать кнопку **Открыть**.
5. В диалоговом окне выбора метода развертывания программ необходимо выбрать вариант *назначенный* и нажать **ОК** (рис. 233).

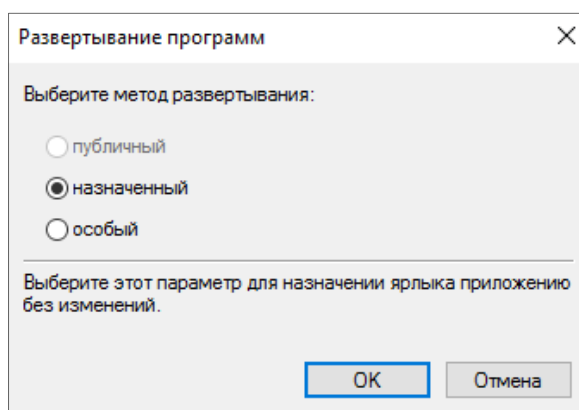


Рис. 233. Выбор метода развертывания программ

Система развернет сформированный файл установки. Выбранный общий установочный пакет появится на правой панели редактора объектов групповой политики (рис. 234).

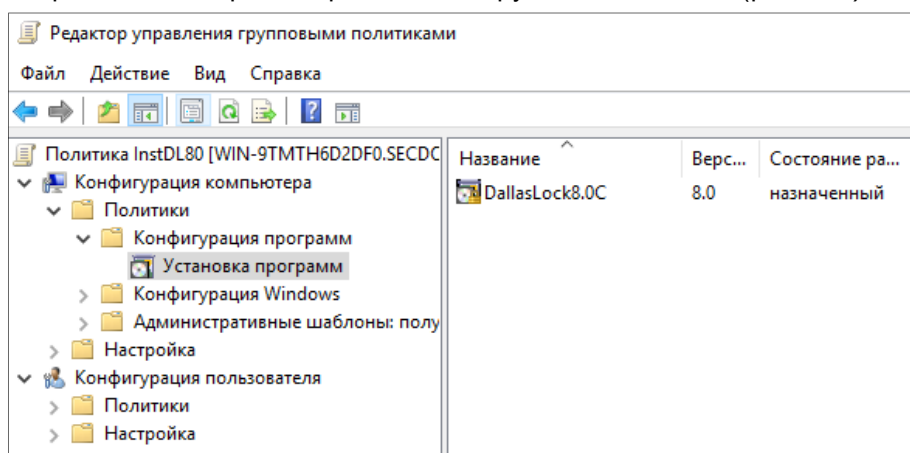


Рис. 234. Появление назначенного пакета установки в окне конфигурации

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 Удаленное обновление СЗИ НСД Dallas Lock 8.0

Централизованное обновление предназначено для обновления зарегистрированных в **ЕЦУ** клиентов **Dallas Lock 8.0** (начиная с обновления ИК9 на ИК10 и т.д.). Полномочиями на запуск централизованного обновления обладает только уполномоченный пользователь **ЕЦУ** с ролью *Администратор*.

После централизованного или локального обновления модуля на следующий ИК на стороне клиента сохраняются:

- текущее расположение модуля в дереве ДБ;
- все ранее собранные журналы;
- настроенные политики безопасности;
- параметры учетных записей.

Установку необходимо осуществлять по протоколу IPv4, на момент обновления и установки модулей необходимо отключить протокол IPv6 на APM с консолью **ЕЦУ**.

Для удаленного обновления **СЗИ НСД Dallas Lock 8.0** необходимо выполнить следующие шаги:

1. Необходимо открыть главное меню консоли **ЕЦУ** → **Удаленное обновление**. Откроется страница мастера удаленного обновления (рис. 215) из списка выбрать *Dallas Lock 8.0* и нажать кнопку **Далее**.

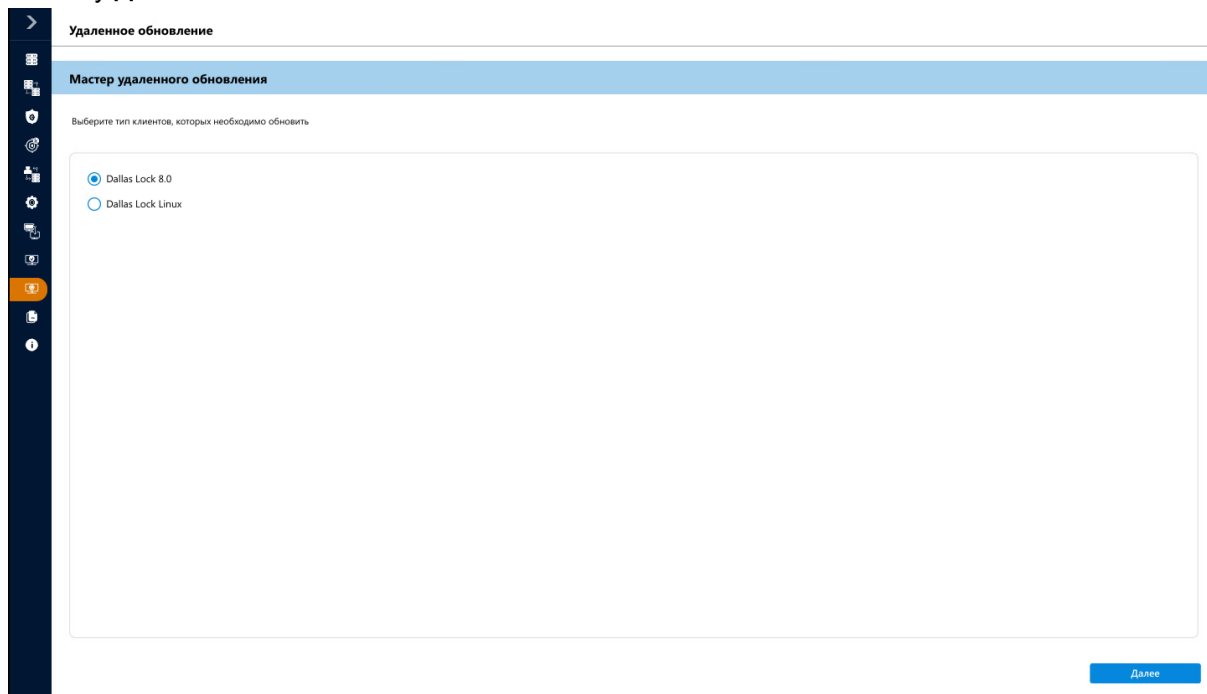


Рис. 235. Мастер удаленного обновления

2. На открывшейся странице необходимо выбрать клиентов, модули которых необходимо обновить (рис. 236). Необходимый объект можно найти по имени через поисковую строку или при помощи дерева клиентов **Dallas Lock 8.0**, поставив напротив нужного клиента флажок.

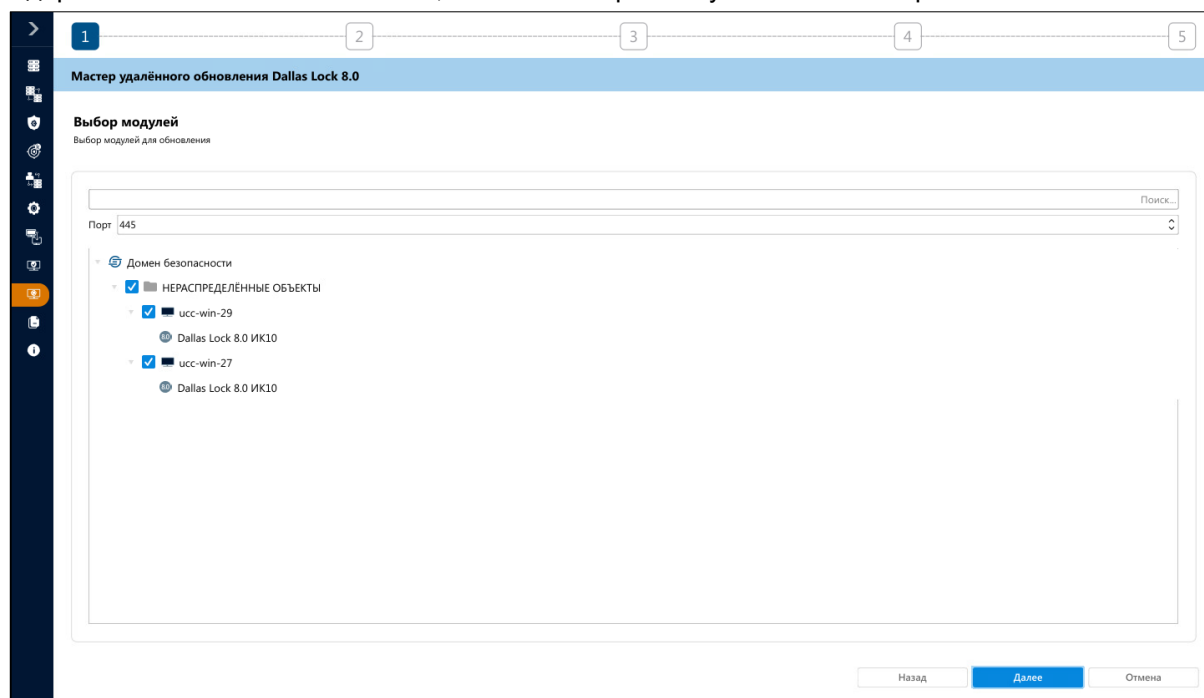


Рис. 236. Страница выбора модулей для обновления

3. Заполнить параметры, которые будут применены к модулям в процессе обновления **СЗИ НСД Dallas Lock 8.0** (рис. 237):

- поле *Имя* для ввода логина администратора безопасности модуля **Dallas Lock 8.0** (поле обязательно для заполнения);
- поле *Пароль* для ввода пароля (поле необязательно для заполнения).

Рис. 237. Ввод авторизационных данных для обновления

После заполнения всех необходимых полей нужно нажать кнопку **Далее**.

4. На следующей странице необходимо (рис. 238):

- указать путь к дистрибутиву с обновлением (обязательный параметр);
- ввести номер лицензии в соответствующее поле (поле обязательно для заполнения);
- ввести код техподдержки в соответствующее поле (поле обязательно для заполнения).

1 2 3 4 5

Мастер удалённого обновления Dallas Lock 8.0

Параметры обновления
Выбор дистрибутива и параметров обновления

Исходный дистрибутив: /home/user0/DallasLock8.0C.msi Выбрать

Номер лицензии: [Redacted]

Код техподдержки: [Redacted]

Назад Далее Отмена

Рис. 238. Страница параметров обновления

5. На следующей странице можно настроить дополнительные параметры обновления, такие как (рис. 239):

- перезагрузка удаленного компьютера после обновления. Поставленный на странице флаг позволяет автоматически перезагрузить компьютер после завершения обновления **СЗИ Dallas Lock 8.0** по истечению установленного времени, иначе компьютер должен быть перезагружен пользователем самостоятельно;
- сообщение для пользователей. Сообщение, указанное на данной странице, будет повторяться с заданным интервалом, для пользователей, на чьих компьютерах производится обновление **СЗИ Dallas Lock 8.0**.

Затем нажать кнопку **Обновить**.

1 2 3 4 5

Мастер удалённого обновления Dallas Lock 8.0

Процесс установки
Выбор дополнительных параметров установки

☐ Перезагрузить удаленный компьютер после установки

Перезагрузить через (мин.): [1] Диапазон от 1 до 999999

Сообщение для пользователей: [Redacted]

Повторять сообщение через (мин.): [0] Диапазон в минутах, 0 - не повторять

Назад Обновить Отмена

Рис. 239. Дополнительные параметры обновления

6. Далее можно просматривать состояние процесса обновления для каждого клиента (рис. 240). По окончании процесса централизованного обновления появятся соответствующие комментарии удачного или неудачного завершения операции.

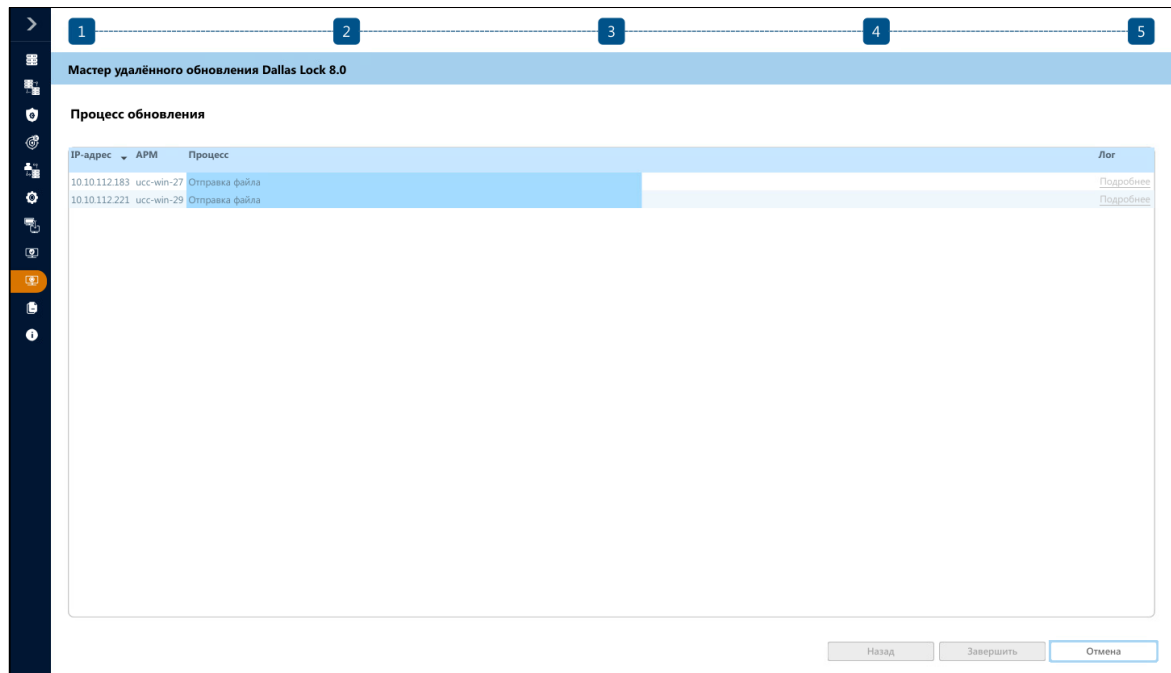


Рис. 240. Процесс обновления

9.5 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.

9.5.1 Синхронизация

Для приведения в соответствие значениям параметров, выставленным на **ЕЦУ**, на модуле **СЗИ Dallas Lock 8.0** необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между **ЕЦУ** и модулем:

- при включении модуля;
- периодически (см. [«Параметры работы модулей»](#));
- по команде пользователя:
 - из консоли **ЕЦУ**;
 - из оболочки администрирования модуля **СЗИ Dallas Lock 8.0**.

Синхронизация по команде из консоли ЕЦУ

Команда «Синхронизировать» в консоли **ЕЦУ** для модуля **СЗИ Dallas Lock 8.0** доступна на вкладке **Сводка** на уровне модуля в дереве Домена безопасности на панели инструментов **Оперативное управление** (рис. 241).

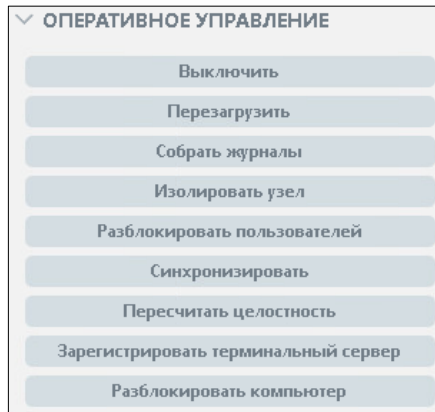


Рис. 241. Кнопка «Синхронизировать»

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**.

9.5.2 Сбор журналов

Для получения в **ЕЦУ** записей журналов, ведущихся на модуле **СЗИ Dallas Lock 8.0**, необходимо проведение сбора журналов. Сбор журналов может быть проведен при условии наличия сетевого подключения между **ЕЦУ** и модулем:

- при включении модуля;
- периодически (см. [«Параметры работы модулей»](#));
- по команде пользователя:
 - из консоли **ЕЦУ**;
 - из оболочки администрирования модуля **СЗИ Dallas Lock 8.0**.

Сбор журналов по команде из консоли ЕЦУ

Команда **Собрать журналы** в консоли **ЕЦУ** для модуля **СЗИ Dallas Lock 8.0** доступна на вкладке **Сводка** на уровне модуля в дереве Домена безопасности на панели инструментов *Оперативное управление* (рис. 242).

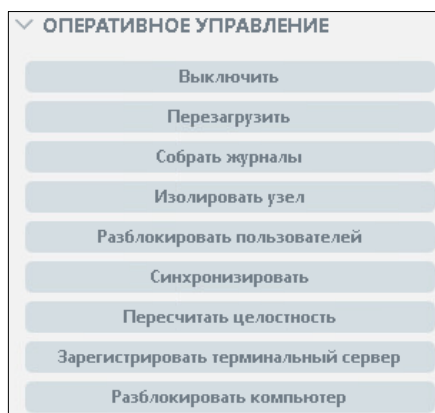


Рис. 242. Кнопка «Собрать журналы»

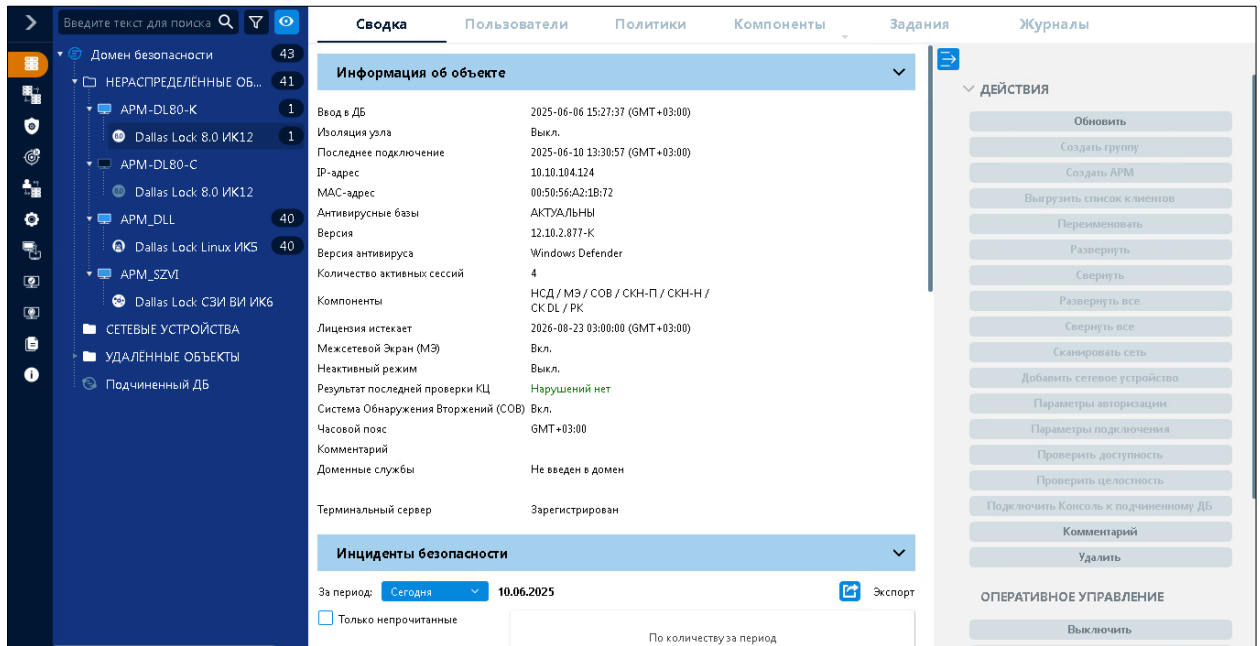
Отправка журналов по команде из оболочки администрирования DL8.0

Для отправки журналов в Домен безопасности **ЕЦУ** по команде из оболочки администрирования модуля **СЗИ Dallas Lock 8.0** на клиентском ПК необходимо выполнить следующие шаги:

1. Запустить оболочку администрирования **СЗИ Dallas Lock 8.0**.
2. Открыть основное меню нажатием кнопки .
3. Выбрать пункт дополнительного меню **Отправить журналы в Домен безопасности**.

9.5.3 Сводка модуля СЗИ Dallas Lock 8.0

Вкладка *Сводка* на уровне модуля **СЗИ Dallas Lock 8.0** отображает общее состояние модуля (рис. 243).



The screenshot displays the 'Сводка' (Summary) tab of the Dallas Lock 8.0 administration interface. The left sidebar shows a tree view of security domains, including 'Домен безопасности' (Security Domain) and 'Подчиненный ДБ' (Subordinate DB). The main content area is divided into two sections: 'Информация об объекте' (Object Information) and 'Инциденты безопасности' (Security Incidents). The 'Информация об объекте' section contains a table with system parameters and their values. The 'Инциденты безопасности' section shows a list of security incidents for the period 'Сегодня' (Today) up to '10.06.2025'. The right sidebar contains a list of actions under the heading 'ДЕЙСТВИЯ' (Actions), including 'Обновить' (Update), 'Создать группу' (Create group), 'Создать АРМ' (Create ARM), 'Выгрузить список клиентов' (Export client list), 'Переименовать' (Rename), 'Развернуть' (Expand), 'Свернуть' (Collapse), 'Развернуть все' (Expand all), 'Свернуть все' (Collapse all), 'Сканировать сеть' (Scan network), 'Добавить сетевое устройство' (Add network device), 'Параметры авторизации' (Authorization parameters), 'Параметры подключения' (Connection parameters), 'Проверить доступность' (Check availability), 'Проверить целостность' (Check integrity), 'Подключить Консоль к подчиненному ДБ' (Connect console to subordinate DB), 'Комментарий' (Comment), 'Удалить' (Delete), and 'ОПЕРАТИВНОЕ УПРАВЛЕНИЕ' (Operational management) with a 'Выключить' (Turn off) button.

Информация об объекте	
Ввод в ДБ	2025-06-06 15:27:37 (GMT+03:00)
Изоляция узла	Выкл.
Последнее подключение	2025-06-10 13:30:57 (GMT+03:00)
IP-адрес	10.10.104.124
MAC-адрес	00:50:56:A2:1B:72
Антивирусные базы	АКТУАЛЬНЫ
Версия	12.10.2.077-K
Версия антивируса	Windows Defender
Количество активных сессий	4
Компоненты	НСД / МЭ / СОВ / СКН-П / СКН-Н / СКДЛ / ПК
Лицензия истекает	2026-08-23 03:00:00 (GMT+03:00)
Межсетевой Экран (МЭ)	Вкл.
Неактивный режим	Выкл.
Результат последней проверки КЦ	Нарушений нет
Система Обнаружения Вторжений (СОВ)	Вкл.
Часовой пояс	GMT+03:00
Комментарий	
Доменные службы	Не введен в домен
Терминальный сервер	Зарегистрирован

Инциденты безопасности

За период: **Сегодня** 10.06.2025

☐ Только непрочитанные

По количеству за период

Экспорт

ДЕЙСТВИЯ

- Обновить
- Создать группу
- Создать АРМ
- Выгрузить список клиентов
- Переименовать
- Развернуть
- Свернуть
- Развернуть все
- Свернуть все
- Сканировать сеть
- Добавить сетевое устройство
- Параметры авторизации
- Параметры подключения
- Проверить доступность
- Проверить целостность
- Подключить Консоль к подчиненному ДБ
- Комментарий
- Удалить

ОПЕРАТИВНОЕ УПРАВЛЕНИЕ

Выключить

Рис. 243. 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 ввода модуля в ДБ; • информация о дате и времени последнего подключения модуля; • IP-адрес; • MAC-адрес; • статус антивирусных баз; • версия Dallas Lock 8.0; • версия антивируса; • количество активных сессий; • активные компоненты Dallas Lock 8.0; • состояние межсетевого экрана; • статус неактивного режима СЗИ; • результат последней проверки КЦ; • состояние системы обнаружения вторжений; • статус технической поддержки; • часовой пояс модуля; • комментарий к модулю; • информация о доменной службе, в которую введен модуль; • информация о статусе клиента в качестве терминального сервера.
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 <i>Комментарий</i> доступно для редактирования.

Доступны следующие действия с модулем на панели инструментов:

1. Обновить.
2. Удалить.
3. Комментарий.

Доступны следующие команды оперативного управления на панели инструментов:

1. Выключить.
2. Перезагрузить.
3. Зарегистрировать терминальный сервер.
4. Изолировать узел.
5. Включить узел в сеть.
6. Разблокировать пользователей.
7. Разблокировать компьютер.
8. Пересчитать целостность.
9. Собрать журналы.
10. Синхронизировать.



Команды *Изолировать узел* и *Включить узел в сеть* являются взаимозаменяемыми. Более подробно об изоляции узла описано в Руководстве по эксплуатации **СЗИ Dallas Lock 8.0** п. 15.2.6.



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**.

9.5.4 Пользователи и группы модуля СЗИ Dallas Lock 8.0

Вкладка *Пользователи* 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.

9.5.5 Политики модуля СЗИ Dallas Lock 8.0

На уровне модуля **СЗИ Dallas Lock 8.0** в списке на вкладке *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.

9.5.6 Межсетевой экран модуля СЗИ Dallas Lock 8.0

На уровне модуля **СЗИ Dallas Lock 8.0** в списке на вкладке **Компоненты** → **Межсетевой экран** доступны только политики МЭ, актуальные для **СЗИ Dallas Lock 8.0** (см. [«Межсетевой экран»](#)).

Настройка МЭ для модуля производится аналогично настройке МЭ для группы ДБ (см. [«Межсетевой экран для группы ДБ»](#)). Для применения параметров на модулях необходима синхронизация.

9.5.7 Система контроля накопителей модуля СЗИ Dallas Lock 8.0

На уровне модуля **СЗИ Dallas Lock 8.0** в списке на вкладке **Компоненты** → **Система контроля накопителей** доступны только параметры СКН, актуальные для **СЗИ Dallas Lock 8.0**.

Управление системой контроля накопителей на уровне группы ДБ производится аналогично управлению системой контроля накопителей для ДБ (см. [«Система контроля накопителей»](#)).

9.5.8 Контроль ресурсов модуля СЗИ Dallas Lock 8.0

На уровне модуля **СЗИ Dallas Lock 8.0** на вкладке **Компоненты** → **Контроль ресурсов** доступны только актуальные для **СЗИ Dallas Lock 8.0** настройки.

Управление контролем ресурсов на уровне модуля производится аналогично управлению контролем ресурсов для ДБ (см. [«Контроль ресурсов»](#)). Для применения параметров на модулях необходима синхронизация.

9.5.9 Система обнаружения вторжений модуля СЗИ Dallas Lock 8.0

На уровне модуля **СЗИ Dallas Lock 8.0** на вкладке **Компоненты** → **Система обнаружения вторжений** доступны только актуальные для **СЗИ Dallas Lock 8.0** настройки.

Управление системой обнаружения вторжений на уровне модуля производится аналогично управлению компонентом COB для группы ДБ (см. [«Система обнаружения вторжений для группы ДБ»](#)). Для применения параметров на модулях необходима синхронизация.

9.5.10 Безопасная среда COB (песочница) модуля СЗИ Dallas Lock 8.0

На уровне модуля **СЗИ Dallas Lock 8.0** на вкладке **Компоненты** → **Безопасная среда COB (песочница)** доступны только актуальные для **СЗИ Dallas Lock 8.0** настройки.

Управление безопасной средой COB на уровне модуля производится аналогично управлению безопасной средой для группы ДБ: возможен только просмотр параметров (см. [«Безопасная среда COB \(песочница\) для группы ДБ»](#)).

9.5.11 Средство обнаружения и реагирования модуля C3И Dallas Lock 8.0

На уровне модуля **C3И Dallas Lock 8.0** на вкладке **Компоненты** → **Средство обнаружения и реагирования** доступны только актуальные для **C3И Dallas Lock 8.0** настройки.

Управление средством обнаружения и реагирования на уровне модуля производится аналогично управлению компонентом СОР для группы ДБ (см. [«Средство обнаружения и реагирования для группы ДБ»](#)). Для применения параметров на модулях необходима синхронизация.

9.5.12 Задания модуля C3И Dallas Lock 8.0

На уровне модуля **C3И Dallas Lock 8.0** в списке на вкладке **Задания** доступны для создания только задания, актуальные для **C3И Dallas Lock 8.0** (рис. 244):

- изменение параметров лицензии;
- получение конфигурации;
- применение конфигурации;
- проверка целостности;
- удаление **DL8.0**;
- сканирование системы на индикаторы компрометации (IoC).

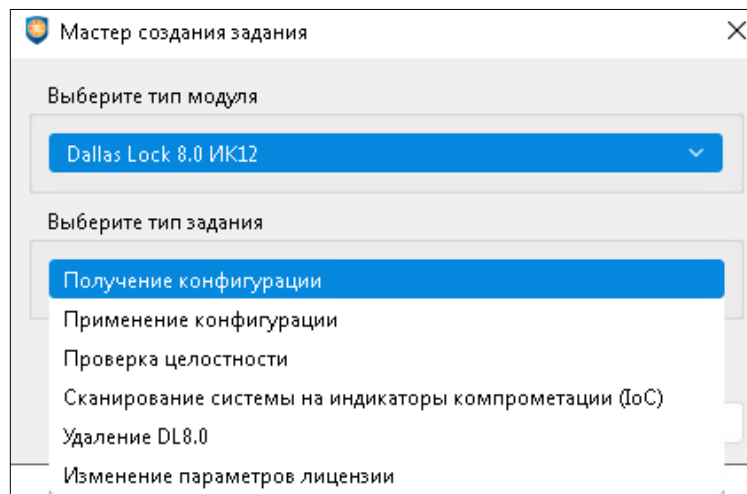


Рис. 244. Мастер создания задания для модуля C3И Dallas Lock 8.0



Если при выполнении задания на получении конфигурации **Dallas Lock 8.0** возникает ошибка, убедитесь, что АРМ с **C3И Dallas Lock 8.0** подключен к домену.

Работа с заданиями для модуля **C3И Dallas Lock 8.0** производится аналогично настройке заданий для ДБ (см. [«Задания ДБ»](#)). Для выполнения задания требуется синхронизация с модулем.

9.5.13 Журналы модуля C3И Dallas Lock 8.0

Вкладка **Журналы** для модуля **C3И Dallas Lock 8.0** позволяет просматривать журналы безопасности модуля (рис. 245).

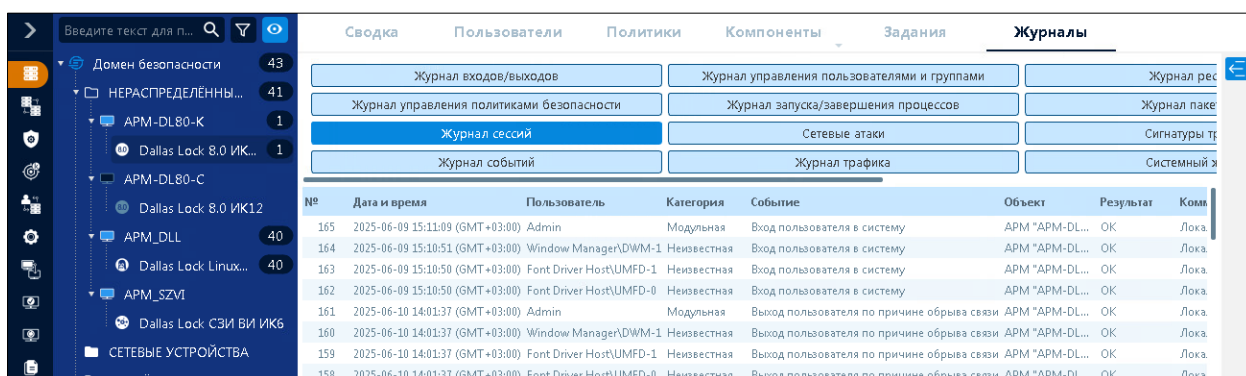


Рис. 245. Вкладка «Журналы»

Для модуля **СЗИ Dallas Lock 8.0** доступны:

- «Журнал входов/выходов»;
- «Журнал управления пользователями и группами»;
- «Журнал ресурсов»;
- «Журнал печати»;
- «Журнал управления политиками безопасности»;
- «Журнал запуска/завершения процессов»;
- «Журнал пакетов МЭ»;
- «Журнал соединений МЭ»;
- «Журнал сессий»;
- «Сетевые атаки»;
- «Сигнатуры трафика»;
- «Подозрительная активность»;
- «Журнал событий»;
- «Журнал трафика»;
- «Системный журнал»;
- «Журнал контроля приложений».

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»](#)).



При вводе модуля **СЗИ НСД Dallas Lock Linux** в ДБ должен быть соблюден ряд условий:

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



После ввода модуля **СЗИ НСД Dallas Lock Linux** под управление **ЕЦУ** значения параметров безопасности подлежат синхронизации со значениями политик **ЕЦУ** для базовой группы **«Нераспределенные объекты»**.

10.1.1 Ввод модуля в ДБ посредством графической оболочки модуля

Для ввода модуля в ДБ через графическую оболочку администратора необходимо:

1. Убедиться, что сервер **ЕЦУ** доступен по сети.
2. Запустить графическую оболочку администрирования (GUI) на модуле и авторизоваться.
3. Перейти на вкладку *Параметры безопасности* и выбрать категорию **Основные настройки**.
4. Запустить поле *Настройка домена безопасности*, где во вкладке *Единый центр управления Dallas Lock* необходимо указать (рис. 246):
 - «АРМ» — сетевое имя или прочее говорящее название для сетевого узла, которое будет отображаться в панели **ЕЦУ** в списке управляемых объектов;
 - «ДБ ЕЦУ» — сетевое имя или IP-адрес сетевого узла, на котором установлена служба **ЕЦУ**;
 - «Ключ доступа» — ключ доступа к ДБ (может быть пустым).

Рис. 246. Окно «Домен безопасности»

5. Далее необходимо нажать кнопку **Ввести в ДБ**.

Если указанные поля не заполнены, кнопка **Ввести в ДБ** будет недоступна для нажатия.

В процессе ввода модуля в Домен Безопасности кнопка **Синхронизация с ЕЦУ** будет недоступна для нажатия до успешного результата регистрации модуля в Домен Безопасности.¹⁵

Результат успешного выполнения: «Модуль успешно зарегистрирован в Домене Безопасности».

В Консоли **ЕЦУ** в группе дерева ДБ «Нераспределенные объекты» появится новый АРМ с указанным именем, в котором зарегистрирован модуль **СЗИ НСД Dallas Lock Linux**.

10.1.2 Ввод модуля в ДБ посредством консольной оболочки модуля

Для ввода модуля в ДБ через консольную оболочку администратора необходимо:

1. Убедиться, что сервер **ЕЦУ** доступен по сети.
2. Запустить консольную оболочку администрирования на модуле путем выполнения команды «*ishl*» и авторизоваться.
3. Перейти в меню централизованного управления, выполнив команду «*management-dll*». После ввода команды система перейдет в меню централизованного управления.
4. В меню централизованного управления для перехода в подменю подключения к домену безопасности, выполнить команду «*connect-domain*». После ввода команды система перейдет в раздел подключения к домену безопасности «*connect-domain*».
5. Далее консольное приложение будет ожидать ввода управляющих команд данной подсистемы, список команд приведен в Таблице 24.

Таблица 27

№	Команда	Описание
1	<i>net-name</i> <i><значение></i>	Сетевое имя или IP-адрес сетевого узла, на котором установлена Служба ЕЦУ . При указании сетевого имени или IP-адреса важно указать номер порта
2	<i>name <значение></i>	Сетевое имя или прочее говорящее название для сетевого узла, которое будет отображаться в панели ЕЦУ в списке управляемых объектов
3	<i>key <значение></i>	Ключ доступа к ДБ ЕЦУ

6. Применить внесенные изменения, выполнив команду *execute*.

7. В результате успешного выполнения появится сообщение:

«*Command 'connect-domain' executed successfully*» — модуль успешно введен в ДБ.

10.2 Вывод модуля из ДБ

Вывести модуль **СЗИ НСД Dallas Lock Linux** из Домена безопасности можно следующими способами:

- с помощью Консоли **ЕЦУ** (см. «[Настройка модуля](#)»);
- через графическую оболочку администратора **Dallas Lock Linux**;
- через консольную оболочку администратора **Dallas Lock Linux**.



При отсутствии сетевого подключения к Службе **ЕЦУ**, модуль может быть выведен из Домена безопасности **ЕЦУ** принудительно. При этом, в Консоли **ЕЦУ** такой модуль продолжит отображаться, но его статус будет «*Недоступен*».

Поэтому, каждый модуль, выведенный из состава ДБ во время отсутствия связи со Службой **ЕЦУ**, необходимо дополнительно удалять вручную из Консоли **ЕЦУ**.

¹⁵ Данное поведение кнопки **Синхронизация с ЕЦУ** при вводе модуля в ДБ посредством графической оболочки модуля соответствует сборкам **СЗИ НСД Dallas Lock Linux** новее, чем 3.25.21.

10.2.1 Вывод посредством графической оболочки модуля

Для вывода модуля через оболочку администрирования необходимо:

1. Запустить графическую оболочку администрирования (GUI) на модуле и авторизоваться.
2. Перейти на вкладку *Параметры безопасности* и выбрать категорию **Основные настройки**.
3. Запустить поле *Настройка домена безопасности*.
4. Нажать кнопку **Вывести из ДБ** (рис. 247).

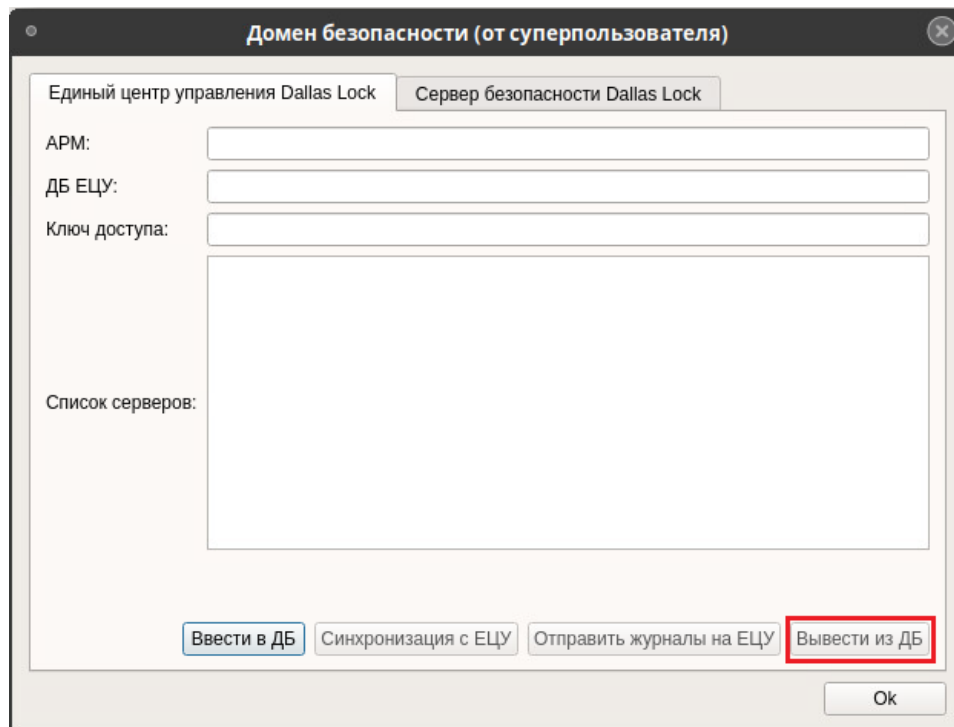


Рис. 247. Вывод модуля из ДБ

Если процесс вывода модуля из ДБ прошел успешно, то через некоторое время поля с информацией о Домене безопасности станут доступными для редактирования.

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

10.2.2 Вывод посредством консольной оболочки модуля

Для вывода модуля из ДБ через консольную оболочку администратора необходимо:

1. Запустить консольную оболочку администрирования на модуле путем выполнения команды «*ishl*» и авторизоваться.
2. Перейти в меню централизованного управления, выполнив команду «*management-dll*». После ввода команды система перейдет в раздел централизованного управления «*management-dll*».
3. В меню централизованного управления выполнить команду «*disconnect-domain*», установив для атрибута значение *force/yes*.

Пример:

disconnect-domain force <enter>

4. В результате успешного выполнения появится сообщение:
«*Unregistration success*» — модуль успешно выведен из ДБ.

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

10.3 Удаленное развертывание СЗИ НСД Dallas Lock Linux

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



Для нескольких целевых ТС централизованную удаленную установку можно осуществить только при выполнении следующих условий:

- целевые ТС входят в тот же домен AD или LDAP, что и АРМ с **ЕЦУ Dallas Lock**;
- известны имя пользователя и пароль доменной учетной записи с правами администратора домена.



В процессе удаленной установки **СЗИ НСД Dallas Lock Linux** на клиентах автоматически создается учетная запись администратора Dallas Lock Linux с именем «dlladmin» и паролем «dlladmin». После установки рекомендуется сменить пароль администратора «dlladmin».

Удаленная установка возможна в следующих вариантах:

- для группы компьютеров, имеющих одинаковые имена и пароли администратора ОС;
- для компьютеров, имеющих индивидуальные имя и пароль администратора ОС, удаленную установку следует выполнять отдельно от других.

Необходимо выполнение следующих требований для удаленных операций:

1. Наличие доступа к сети Интернет у целевых ТС.
2. Установку необходимо осуществлять по протоколу IPv4, на момент обновления и установки модулей необходимо отключить протокол IPv6 на АРМ с консолью **ЕЦУ**.
3. При удаленном развертывании **СЗИ НСД Dallas Lock Linux** предварительно на целевых ТС необходимо установить и настроить SSH-сервер. Рекомендуется использовать OpenSSH сервер. Установка клиента и сервера OpenSSH выполняется следующим образом.

Для Ubuntu в терминале необходимо выполнить команды:

- «`sudo apt-get install openssh-server openssh-client`».

Для Debian, Astra Linux, ALT Linux в терминале необходимо выполнить команды:

- «`su (sudo для Astra Linux) apt-get install openssh-server openssh-client`».

Для RHEL, РЕД ОС, РОСА, CentOS 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 RHEL, РЕД ОС, РОСА, CentOS «`su -c "systemctl start sshd.service"`»;
- для Astra Linux «`sudo systemctl start ssh`»;
- для ALT Linux «`su -c "systemctl start ssh"`».

4. По умолчанию пользователь root не имеет права на вход по SSH. Для того, чтобы разрешить ему вход, необходимо проверить конфигурационный файл sshd.

- открываем на редактирование файл: «`/etc/ssh/sshd_config`»;
- ищем строку: «`#PermitRootLogin no`»;

Если строка имеет вид «`#PermitRootLogin prohibit-password`», то можно переходить к следующему шагу.

Если строка имеет вид «`#PermitRootLogin no`», то пользователь root не имеет права на вход по SSH. Для того, чтобы разрешить ему вход, необходимо отредактировать конфигурационный файл sshd.

- 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`»).

После удаленной установки **СЗИ НСД Dallas Lock Linux** необходимо отключить SSH-сервер на целевых ТС.

Для удаленной установки **СЗИ НСД Dallas Lock Linux**, необходимо выполнить следующие шаги:

1. На целевых ТС проверить список поддерживаемых протоколов по ssh — выполнить команду «`ssh -Q cipher`».

Если в списке поддерживаемых протоколов нет следующих алгоритмов: `3des-cbc`, `aes192-cbc`, `aes128-cbc`, `arcfour128`, `arcfour`, то в конфигурационный файл необходимо прописать «`Ciphers +3des-cbc,aes192-cbc,aes128-cbc,arcfour128,arcfour`»¹⁶. Сохранить файл после внесенных изменений.

¹⁶ В ряде ОС символ «+» может не восприниматься, и строка будет считаться некорректной.



ЕЦУ Dallas Lock для связи с модулем **СЗИ НСД Dallas Lock Linux** использует алгоритмы шифрования «*3des-cbc, aes192-cbc, aes128-cbc, arcfour128, arcfour*», на стороне модуля Linux список поддерживаемых алгоритмов может несущественно отличаться, и при этом удаленная установка **СЗИ НСД Dallas Lock Linux** все равно будет возможна.

После выполнения всех настроек в конфигурационном файле сервис `sshd` необходимо перезапустить.

2. Перед централизованной установкой необходимо разместить на компьютере, на котором запущена консоль **ЕЦУ**, дистрибутив **Dallas Lock Linux**.
3. Необходимо открыть главное меню Консоли **ЕЦУ**  и выбрать **Удаленная установка**. Откроется страница мастера удаленной установки из списка выбрать *Dallas Lock Linux* и нажать кнопку **Далее**.

На открывшейся странице необходимо добавить целевые ТС для удаленного развертывания. ТС можно добавить одним из следующих способов, через:

- ручной ввод адреса — для этого нужно заполнить поля *Порт* и *Введите IP-адрес или сетевое имя компьютера*, затем нажать кнопку **Добавить компьютер** (рис. 248);
- файл списка клиентов — нажать **Импорт из файла** и выбрать файл со списком заранее выгруженных клиентов;
- импорт из файла — нажать **Импорт из файла** и прикрепить текстовый файл со списком IP-адресов целевых ТС.



Для файла с IP-адресами возможен только следующий формат списка: в каждой строке файла может быть указан только один IP-адрес без дополнительных символов.
Пример:

```
192.168.0.1
192.168.0.35
10.10.112.55
```

1 2 3 4

Мастер удаленной установки Dallas Lock Linux

Список компьютеров
Установка списка компьютеров для подключения

Введите IP адрес или сетевое имя компьютера

10.10.101.110 **Добавить компьютер**

Порт 22

IP-адрес	FQDN-имя
10.10.101.110	
192.168.131.29	redos-7-murom.isc.confident.spb.ru

Импорт из файла **Удалить**

Назад **Далее** **Отмена**

Рис. 248. Список целевых ТС для удаленного развертывания СЗИ НСД Dallas Lock Linux

После добавления целевых ТС в список необходимо нажать кнопку **Далее**.

4. Заполнить параметры установки, которые будут применены к модулям в процессе активации **СЗИ НСД Dallas Lock Linux** (рис. 249):

- логин и пароль администратора ОС на целевых ТС;
- логин и пароль суперпользователя (опционально).

Рис. 249. Параметры установки СЗИ НСД Dallas Lock Linux

После заполнения всех необходимых полей нужно нажать кнопку **Далее**.

5. На следующей странице (рис. 250) необходимо указать:

- путь к исходному дистрибутиву **СЗИ НСД Dallas Lock Linux**;
- номер лицензии, который указан на обложке футляра;
- дополнительные ключи установки;
- параметры для ввода модулей в Домен безопасности **ЕЦУ Dallas Lock** после установки (опционально).

В качестве дополнительных ключей установки можно указать следующие атрибуты:

Атрибут	Описание
<code>--confirm</code>	Спросить перед запуском встроенного скрипта
<code>--quiet</code>	Не печатать ничего кроме сообщений об ошибках
<code>--accept</code>	Принять номер лицензии
<code>--noexec</code>	Не запускать встроенный скрипт
<code>--noexec-cleanup</code>	Не запускать встроенный скрипт очистки
<code>--keep</code>	Не удалять данные о целевой директории после выполнения встроенного скрипта
<code>--noprogess</code>	Не показывать прогресс в процессе декомпрессии
<code>--nox11</code>	Данный атрибут не используется в процессе установки СЗИ НСД
<code>--nochown</code>	Не давать доступ к распакованным файлам текущему пользователю
<code>--chown</code>	Рекурсивно назначить доступ к распакованным файлам текущему пользователю
<code>--nodiskspace</code>	Не проверять доступное место на диске
<code>--target dir</code>	Извлечь непосредственно в целевую директорию (по абсолютной или относительной ссылке). Этот каталог может быть подвергнут рекурсивной обработке (см. <code>nochown</code>)

<code>--tar arg1 [arg2 ...]</code>	Доступ к содержимому архива через команду <i>tar</i> . Во встроенный скрипт будут переданы следующие аргументы
<code>--ssl-pass-src src</code>	Использовать указанный <i>src</i> в качестве источника пароля для расшифровки данных с помощью OpenSSL, см. «Аргументы парольной фразы» в руководстве OpenSSL. По умолчанию пользователю предлагается ввести пароля для расшифровки на текущем терминале
<code>--cleanup-args args</code>	Аргументы встроенного скрипта очистки. Для передачи нескольких аргументов требуется заключать их в кавычки
<code>--arm-name=name</code>	Указать под каким именем будет зарегистрирован APM в Домене безопасности ЕЦУ
<code>--ucc-addr=address</code>	Указать IP-адрес или сетевое имя компьютера Домена безопасности ЕЦУ
<code>--ucc-key=key</code>	Указать ключ Домена безопасности ЕЦУ
<code>--grub-pass=password</code>	Установить пароль GRUB для суперпользователя по умолчанию — <i>dlladmin</i>
<code>--just-check</code>	Не устанавливать, а только проверить поддержку хост-системы

Дополнительные ключи установки указываются в поле через пробел.

Пример:

`--nochown --nodiskspace`

Для ввода модулей в Домен безопасности **ЕЦУ** сразу после установки, можно поставить флаг *Ввод в домен безопасности ЕЦУ*, указать имя сервера **ЕЦУ** и ключ доступа к ДБ. Затем нажать **Установить**.

Если данные для ввода модуля в ДБ **ЕЦУ** (в том числе ключ доступа) были указаны неверно, то установка будет приостановлена. Кнопка **Установить** будет неактивна до тех пор, пока данные для ввода в ДБ **ЕЦУ** не будут введены верно. Чтобы продолжить установку без ввода модуля в ДБ **ЕЦУ** необходимо снять флаг *Ввод в домен безопасности ЕЦУ*.

Затем нажать кнопку **Установить**.

Рис. 250. Информация о ходе централизованной установки средствами ЕЦУ

6. Далее можно просматривать состояние процесса установки для каждого клиента (рис. 251).

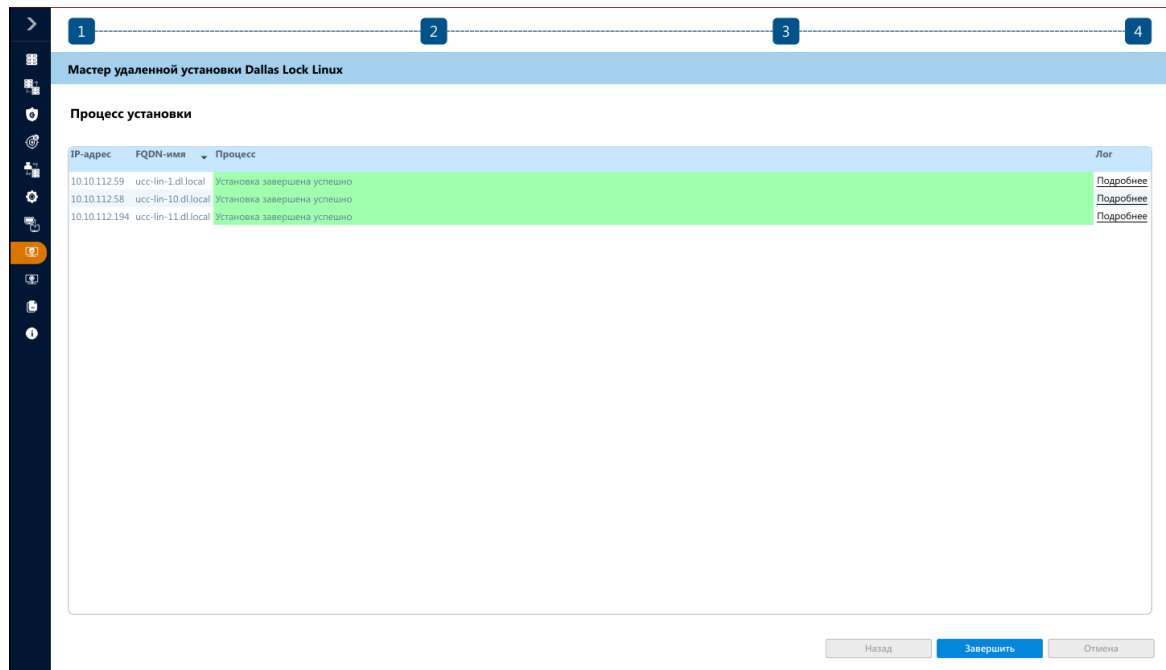


Рис. 251. Информация о ходе централизованной установки средствами ЕЦУ

7. По окончании процесса централизованной установки появятся соответствующие комментарии удачного или не удачного завершения операции.



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.



При удаленном развертывании устанавливается только **СЗИ НСД Dallas Lock Linux**. Графическая оболочка администрирования устанавливается отдельно и только локально.

При попытке развернуть графическую оболочку администрирования удаленно будет возникать ошибка запуска установочного файла (рис. 252), поскольку **СЗИ НСД** уже установлено, а графическая оболочка является избыточной и опциональной.

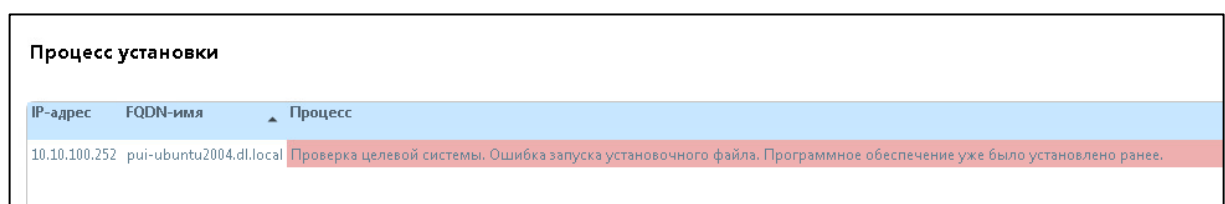


Рис. 252. Ошибка запуска установочного файла

В дереве объектов ДБ **ЕЦУ** появятся значки новых АРМ и модулей.



При удаленной установке объекты с одинаковыми именами объединяются, вне зависимости от регистра. После объединения отображается имя, которое было ранее сохранено в **ЕЦУ**.



Если установленный модуль **Dallas Lock Linux** не появился в дереве объектов ДБ **ЕЦУ**, то необходимо осуществить его ввод в ДБ **ЕЦУ** вручную.

10.4 Удаленное обновление СЗИ НСД Dallas Lock Linux

Централизованное обновление предназначено для обновления зарегистрированных в ЕЦУ клиентов **Dallas Lock Linux** (начиная с обновления ИК2 на ИК3 (версия без МЭ и с МЭ), с ИК3 (версия без МЭ) на ИК3 (версия с МЭ) и т.д.). Полномочиями на запуск централизованного обновления обладает только уполномоченный пользователь **ЕЦУ** с ролью *Администратор*.

После централизованного или локального обновления модуля на следующий ИК на стороне клиента сохраняются:

- текущее расположение модуля в дереве ДБ;
- все ранее собранные журналы;
- настроенные политики безопасности;
- параметры учетных записей.

Установку необходимо осуществлять по протоколу IPv4, на момент обновления и установки модулей необходимо отключить протокол IPv6 на АРМ с консолью ЕЦУ.

Для удаленного обновления **СЗИ НСД Dallas Lock Linux** необходимо выполнить следующие шаги:

1. Необходимо открыть главное меню консоли **ЕЦУ** → **Удаленное обновление**. Откроется страница мастера удаленного обновления из списка выбрать **Dallas Lock Linux** и нажать кнопку **Далее**.
2. На открывшейся странице необходимо выбрать модуль для обновления и клиентов, модули которых необходимо обновить (рис. 253). Необходимый объект можно найти по имени через поисковую строку или при помощи дерева клиентов **Dallas Lock Linux**, активировав напротив нужного клиента чекбокс.

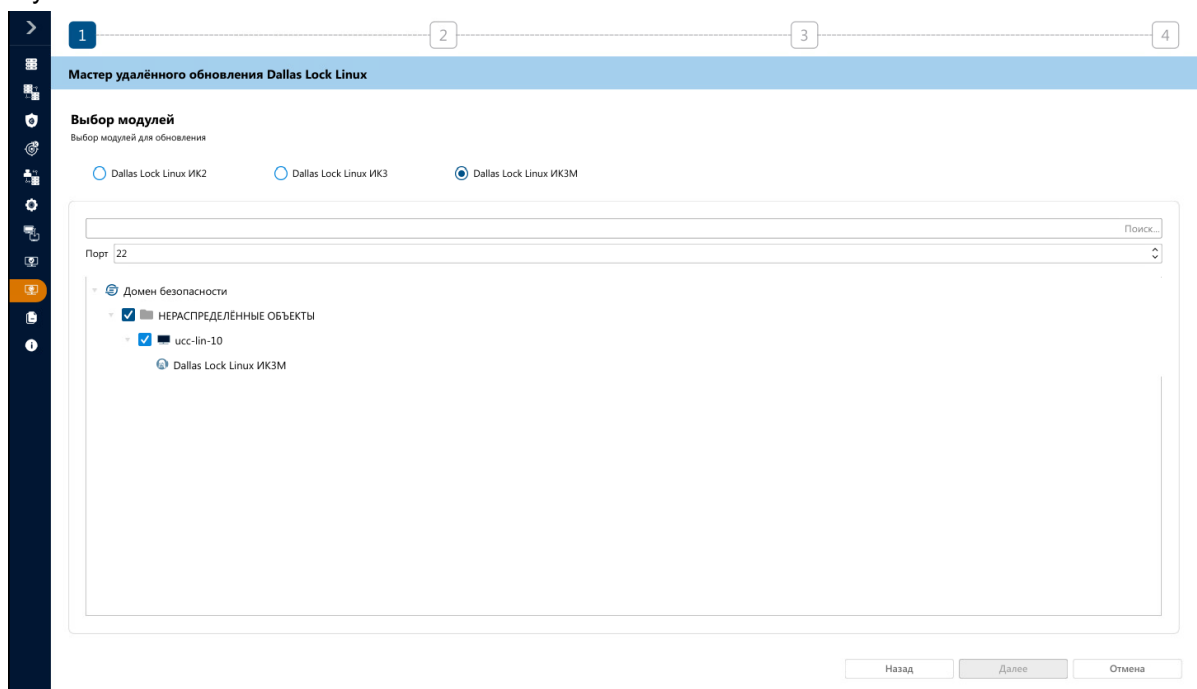


Рис. 253. Страница выбора компьютеров с Linux

3. Заполнить параметры, которые будут применены к модулям в процессе обновления **СЗИ НСД Dallas Lock Linux** (рис. 254):
 - поле *Имя* для ввода логина администратора ОС (поле обязательно для заполнения);
 - поле *Пароль* для ввода пароля администратора ОС (поле необязательно для заполнения).

Если активировать чекбокс *Пользователь является суперпользователем*, то поля для ввода данных суперпользователя станут неактивными. В противном случае необходимо ввести логин и пароль суперпользователя.

1 2 3 4

Мастер удалённого обновления Dallas Lock Linux

Ввод авторизационных данных
Учетные данные администратора ОС компьютеров клиентов

Имя user0
Пароль

☐ Пользователь является суперпользователем

Имя root
Пароль

Назад Далее Отмена

Рис. 254. Ввод авторизационных данных

После заполнения всех необходимых полей нужно нажать кнопку **Далее**.

4. На следующей странице необходимо (рис. 255):

- указать путь к дистрибутиву с обновлением (обязательный параметр);
- ввести номер лицензии в соответствующее поле (поле обязательно для заполнения);
- ввести логин администратора **СЗИ** в соответствующее поле (поле обязательно для заполнения);
- ввести пароль администратора **СЗИ** в соответствующее поле (поле необязательно для заполнения);
- выбрать в каком формате экспортировать журналы (необязательный параметр):
 - «в формате PDF»;
 - «в формате ODS»;
 - «в формате XML»;
- ввести дополнительные ключи установки в соответствующее поле (поле необязательно для заполнения).

1 2 3 4

Мастер удалённого обновления Dallas Lock Linux

Параметры обновления
Выбор дистрибутива и параметров обновления

Исходный дистрибутив: /home/user0/dllx-4.6.69.run Выбрать

Номер лицензии: [Redacted]

Имя Администратора СЗИ НСД: dilladmin

Пароль Администратора СЗИ НСД: [Masked] 👁

☒ Экспорт журналов

☒ в формате PDF ☐ в формате ODS ☐ в формате XML

Дополнительные ключи установки: [Empty field]

Назад Обновить Отмена

Рис. 255. Параметры обновления

- Далее можно просматривать состояние процесса обновления для каждого клиента (рис. 256). По окончании процесса централизованного обновления появятся соответствующие комментарии удачного или неудачного завершения операции.

1 2 3 4

Мастер удалённого обновления Dallas Lock Linux

Процесс обновления

IP-адрес	APM	Процесс	Лог
10.10.112.58	ucc-lin-10	Авторизация суперпользователем	Подробнее

Назад Завершить Отмена

Рис. 256. Процесс обновления

10.5 Настройка модуля СЗИ НСД Dallas Lock Linux

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

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



— модуль подключен;



— связь с модулем отсутствует.

Настройки на уровне модуля отображаются на нескольких основных вкладках.

10.5.1 Синхронизация

Для приведения в соответствие значениям параметров, выставленным на **ЕЦУ Dallas Lock**, на модуле **СЗИ НСД Dallas Lock Linux** необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между **ЕЦУ Dallas Lock** и модулем:

- при включении модуля;
- периодически (см. [«Параметры работы модулей»](#));
- по команде пользователя:
 - из Консоли **ЕЦУ**;
 - из графической оболочки модуля **СЗИ НСД Dallas Lock Linux**.

Синхронизация по команде из консоли ЕЦУ

Команда **Синхронизировать** в Консоли **ЕЦУ** для модуля **СЗИ НСД Dallas Lock Linux** доступна на вкладке *Сводка* на уровне модуля в дереве Домена безопасности на панели инструментов *Оперативное управление* (рис. 257).



Рис. 257. Кнопка «Синхронизировать»

Синхронизация по команде из графической оболочки СЗИ НСД Dallas Lock Linux

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

1. Запустить графическую оболочку **СЗИ НСД Dallas Lock Linux** и авторизоваться.
2. На вкладке *Параметры безопасности* выбрать категорию **Домен безопасности**, открыть для редактирования параметр **Настройка домена безопасности**.
3. В окне **Домен безопасности** нажать кнопку **Синхронизация с ЕЦУ** (рис. 258).

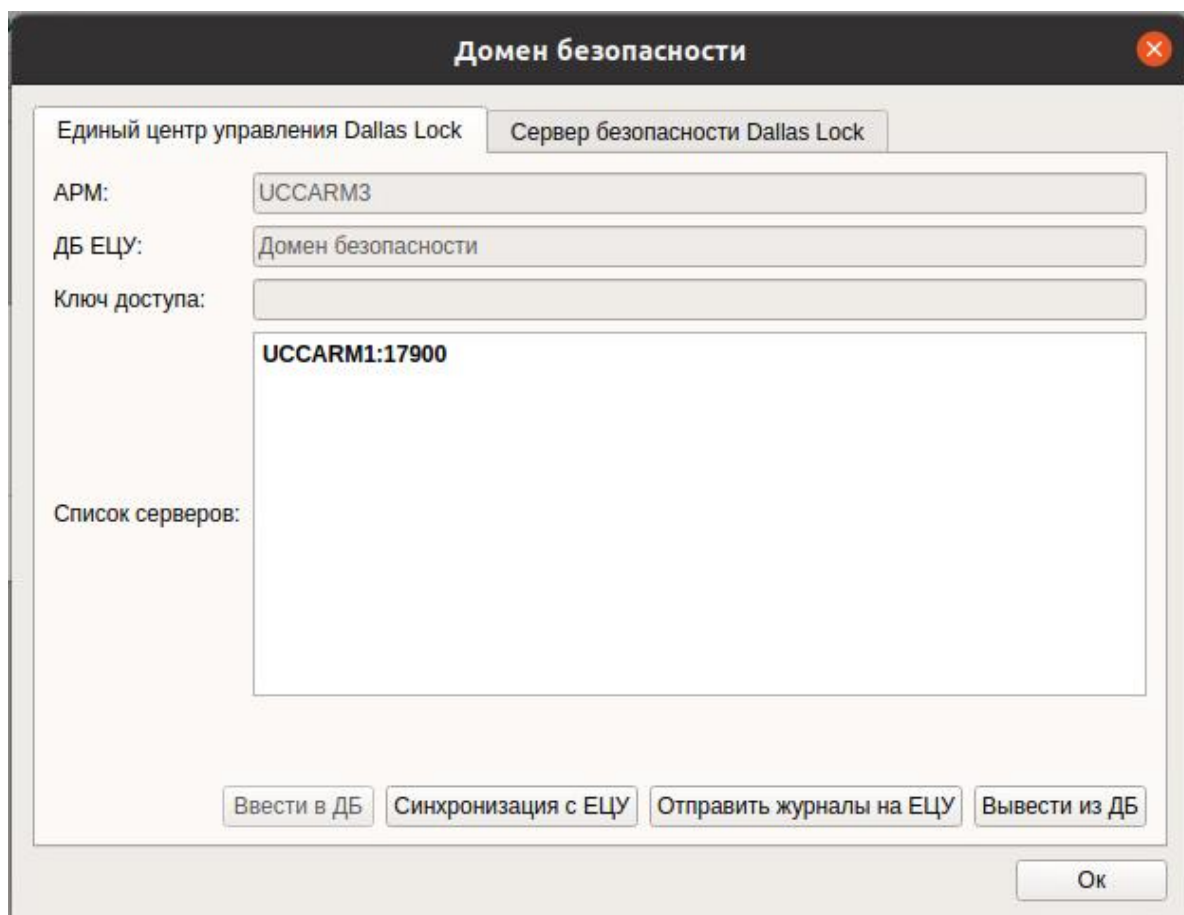


Рис. 258. Кнопка «Синхронизация с ЕЦУ»

10.5.2 Сбор журналов

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

- при включении модуля;
- периодически (см. [«Параметры работы модулей»](#));
- по команде пользователя:
 - из Консоли **ЕЦУ**;
 - из графической оболочки модуля **СЗИ НСД Dallas Lock Linux**.

Сбор журналов по команде из консоли ЕЦУ

Команда **Собрать журналы** в Консоли **ЕЦУ** для модуля **СЗИ НСД Dallas Lock Linux** доступна на вкладке «Сводка на уровне модуля в дереве Домена безопасности на панели инструментов *Оперативное управление*» (рис. 259).



Рис. 259. Кнопка «Собрать журналы»

Отправка журналов по команде из графической оболочки администратора

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

1. Запустить графическую оболочку **СЗИ НСД Dallas Lock Linux** и авторизоваться.
2. На вкладке *Параметры безопасности* выбрать категорию **Домен безопасности**, открыть для редактирования параметр **Настройка домена безопасности**.
3. В окне **Домен безопасности** нажать кнопку **Отправить журналы на ЕЦУ** (рис. 260).

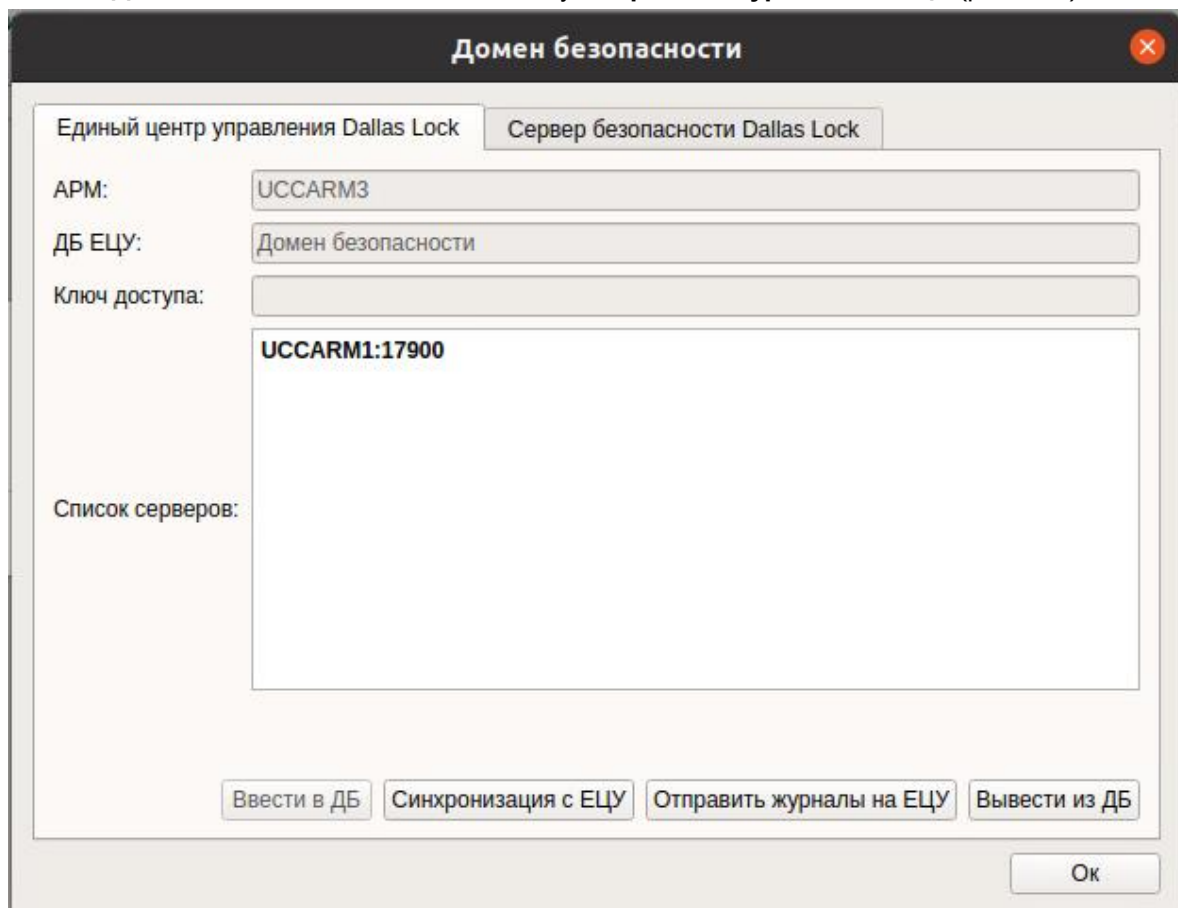


Рис. 260. Кнопка «Отправить журналы на ЕЦУ»

10.5.3 Сводка модуля СЗИ НСД Dallas Lock Linux

Вкладка *Сводка* на уровне модуля **СЗИ НСД Dallas Lock Linux** отображает общее состояние модуля (рис. 261).

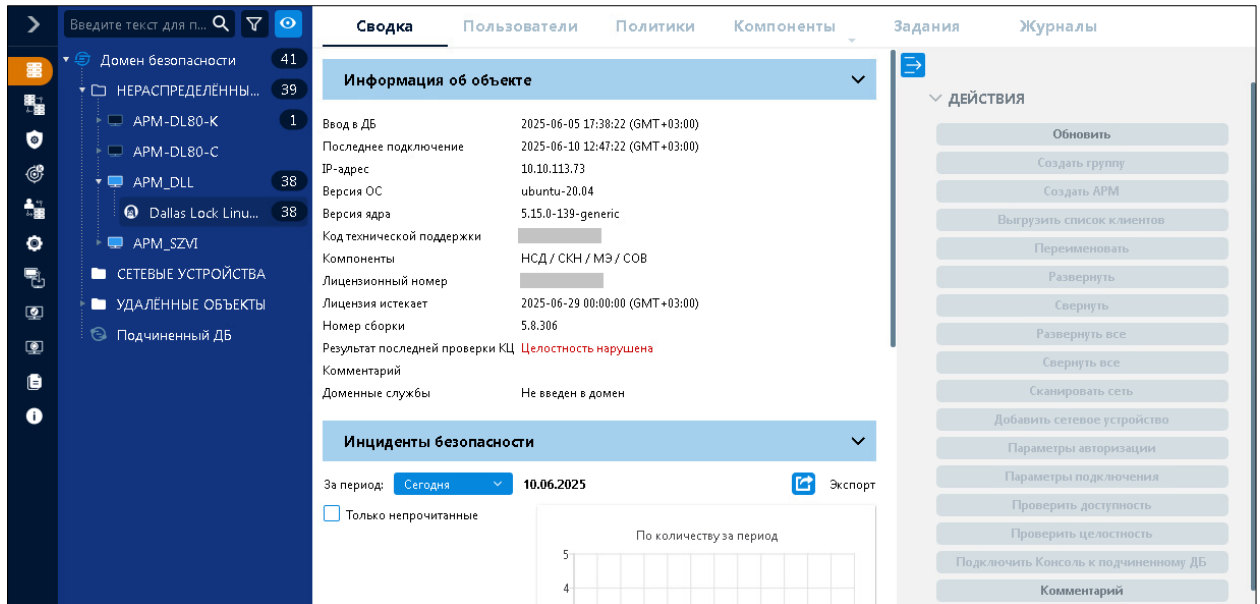


Рис. 261. Вкладка «Сводка»

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 ввода модуля в ДБ; • информация о дате и времени последнего подключения модуля; • IP-адрес; • версия операционной системы; • версия ядра; • код технической поддержки; • компоненты; • номер лицензии; • информация о сроке действия лицензии; • номер сборки; • результат последней проверки КЦ; • комментарий; • информация о доменной службе, в которую введен модуль.
Инциденты безопасности
Отображается список инцидентов безопасности модуля с графической панелью. Доступна фильтрация отображаемых событий по периоду и настройка отображения диаграмм (см. «Настройка инцидентов безопасности»). Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное. Поле «Комментарий» доступно для редактирования.

Доступны следующие действия с модулем на панели инструментов:

1. Обновить.
2. Удалить модуль.
3. Комментарий.

Доступны следующие команды оперативного управления на панели инструментов:

1. Синхронизировать.
2. Выключить.
3. Перезагрузить.
4. Разблокировать пользователей.
5. Пересчитать целостность.
6. Собрать журналы.

10.5.4 Пользователи и группы модуля СЗИ НСД Dallas Lock Linux

Вкладка *Пользователи* на уровне модуля **СЗИ НСД Dallas Lock Linux** содержит список глобальных и доменных пользователей и групп, наследуемых с уровней выше по иерархии и созданных на уровне данного модуля, а также модульных пользователей.

Управление пользователями и группами на уровне модуля **СЗИ НСД Dallas Lock Linux** производится аналогично описанному управлению пользователями и группами в разделе [«Пользователи и группы модуля»](#). Для применения изменений на модулях необходима синхронизация.

10.5.5 Политики модуля СЗИ НСД Dallas Lock Linux

На уровне модуля **СЗИ НСД Dallas Lock Linux** в списке на вкладке *Политики* доступны только политики, актуальные для **СЗИ НСД Dallas Lock Linux** (см. [«Политики ДБ»](#)).

Настройка политик для модуля производится аналогично настройке политик для группы ДБ (см. [«Политики для группы ДБ»](#)). Для применения параметров на модулях необходима синхронизация.

10.5.6 Межсетевой экран модуля СЗИ НСД Dallas Lock Linux

На уровне модуля **СЗИ Dallas Lock Linux** в списке на вкладке *Компоненты* → *Межсетевой экран* доступны только политики МЭ, актуальные для **СЗИ Dallas Lock Linux** (см. [«Межсетевой экран»](#)).

Настройка МЭ для модуля производится аналогично настройке МЭ для группы ДБ (см. [«Межсетевой экран для группы ДБ»](#)). Для применения параметров на модулях необходима синхронизация.

10.5.7 Система контроля накопителей модуля СЗИ НСД Dallas Lock Linux

На уровне модуля **СЗИ Dallas Lock Linux** в списке на вкладке *Компоненты* → *Система контроля накопителей* доступны только параметры СКН, актуальные для **СЗИ Dallas Lock Linux**.

Управление системой контроля накопителей на уровне группы ДБ производится аналогично управлению системой контроля накопителей для ДБ (см. [«Система контроля накопителей»](#)).

10.5.8 Контроль ресурсов модуля СЗИ НСД Dallas Lock Linux

На уровне модуля **СЗИ Dallas Lock Linux** на вкладке *Компоненты* → *Контроль ресурсов* доступны только актуальные для **СЗИ Dallas Lock Linux** настройки.

Управление контролем ресурсов на уровне модуля производится аналогично управлению контролем ресурсов для ДБ (см. [«Контроль ресурсов»](#)). Для применения параметров на модулях необходима синхронизация.

10.5.9 Система обнаружения вторжений модуля СЗИ НСД Dallas Lock Linux

На уровне модуля **СЗИ Dallas Lock Linux** на вкладке *Компоненты* → *Система обнаружения вторжений* доступны только актуальные для **СЗИ Dallas Lock Linux** настройки.

Управление системой обнаружения вторжений на уровне модуля производится аналогично управлению компонентом СОВ для группы ДБ (см. [«Система обнаружения вторжений для группы ДБ»](#)). Для применения параметров на модулях необходима синхронизация.

10.5.10 Средство обнаружения и реагирования модуля СЗИ НСД Dallas Lock Linux

На уровне модуля **СЗИ Dallas Lock Linux** на вкладке **Компоненты** → **Средство обнаружения и реагирования** доступны только актуальные для **СЗИ Dallas Lock Linux** настройки.

Управление средством обнаружения и реагирования на уровне модуля производится аналогично управлению компонентом СОР для группы ДБ (см. [«Средство обнаружения и реагирования для группы ДБ»](#)). Для применения параметров на модулях необходима синхронизация.

10.5.11 Задания модуля СЗИ НСД Dallas Lock Linux

На уровне модуля **СЗИ НСД Dallas Lock Linux** в списке на вкладке **Задания** доступны для создания только задания, актуальные для **СЗИ НСД Dallas Lock Linux** (рис. 262):

- изменение параметров лицензии (изменяет номер лицензии и код технической поддержки);
- получение конфигурации;
- применение конфигурации;
- удаление модуля;
- сканирование системы на индикаторы компрометации (IoC).

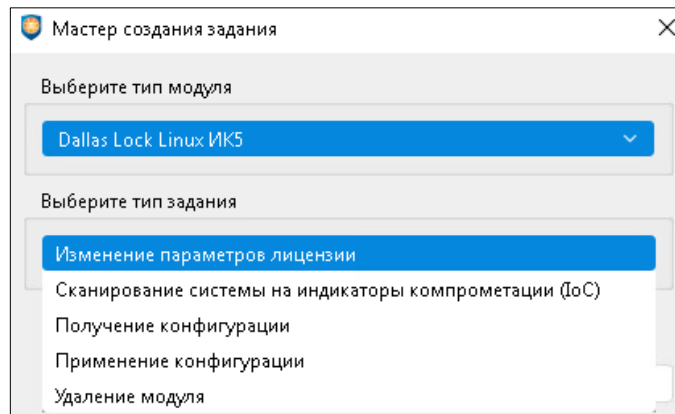


Рис. 262. Мастер создания задания для модуля СЗИ НСД Dallas Lock Linux

Работа с заданиями для модуля **СЗИ НСД Dallas Lock Linux** производится аналогично настройке заданий для ДБ (см. [«Задания ДБ»](#)).

10.5.12 Журналы модуля СЗИ НСД Dallas Lock Linux

Вкладка **Журналы** для модуля **СЗИ НСД Dallas Lock Linux** позволяет просматривать журналы безопасности модуля (рис. 263).

Введите текст для поиска

Домен безопасности

2

bds-srv22-ksc14.d.local

1

НЕРАЗРЕШЕННЫЕ ОБЪЕКТЫ

Новая группа

DESKTOP-1BGEAP2

bds-redos734-10

Dallas Lock Unix IK4

bds-srv22-ksc14.d.local

СЕТЕВЫЕ УСТРОЙСТВА

УДАЛЕННЫЕ ОБЪЕКТЫ

bds-win10-12.d.local (Kaspersky End...

bds-win10-12.d.local (Kaspersky End...

utm126 (Школа безопасности W...

1

Сводка	Пользователи	Политики	Компоненты	Задания	Журналы
Журнал входов	Журнал доступа к ресурсам	Журнал управления пользователями	Журнал печати		
Журнал управления политиками безопасности	Системный журнал	Журнал доступа к устройствам	Журнал событий безопасности МЭ		
Журнал управления МЭ					

ID	Событие	Время	Пользователь ОС	Результат	Объект	Принтер	Информация
66726	Вход пользователя	2024-07-08 13:04:53 (GMT+03:00)	dladmin	OK	dladmin	null	["info":"User authentication"]
66395	Выход пользователя	2024-07-08 13:03:11 (GMT+03:00)	gdm	OK	null	null	["msg":"gdm-launch-environment","uid":"",""]
66388	Вход пользователя	2024-07-08 13:01:36 (GMT+03:00)	gdm	OK	gdm	null	["msg":"gdm-launch-environment","info":"User authentication"]
1	Старт системы	2024-07-08 13:01:39 (GMT+03:00)	root	OK	system	null	null
66430	Вход пользователя	2024-07-08 13:03:24 (GMT+03:00)	user0	OK	root	null	["msg":"su-1","info":"User authentication","uid":"user0"]
66394	Вход пользователя	2024-07-08 13:03:11 (GMT+03:00)	user0	OK	user0	null	["msg":"gdm-password","info":"User authentication"]

Рис. 263. Вкладка «Журналы»

Для модуля **СЗИ НСД Dallas Lock Linux** доступны:

- «Журнал входов»;
- «Журнал доступа к ресурсам»;
- «Журнал управления пользователями»;

- «Журнал печати»;
- «Журнал управления политиками безопасности»;
- «Системный журнал»;
- «Журнал доступа к устройствам»;
- «Журнал событий безопасности МЭ»;
- «Журнал управления МЭ»;
- «События безопасности СОВ»;
- «Журнал событий»;
- «Управление СОВ».

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**.



При вводе модуля **СЗИ ВИ Dallas Lock** в ДБ должен быть соблюден ряд условий:

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



После ввода модуля **СЗИ ВИ Dallas Lock** под управление **ЕЦУ Dallas Lock** значения параметров безопасности подлежат синхронизации со значениями политик **ЕЦУ Dallas Lock** для базовой группы «*Нераспределенные объекты*».

Для ввода модуля в ДБ через Консоль Центра управления **СЗИ ВИ Dallas Lock** необходимо:

1. Убедиться, что сервер **ЕЦУ** доступен по сети.
2. Запустить консоль модуля.
3. Открыть главное меню  → **Параметры ЕЦУ**.
4. Поставить флаг *под управлением ЕЦУ* (рис. 264), чтобы поле настроек стало активно, затем указать следующие данные:
 - DNS-имя или IP-адрес сервера **ЕЦУ**;
 - имя АРМ, в составе которого необходимо ввести модуль;
 - ключ доступа к ДБ.

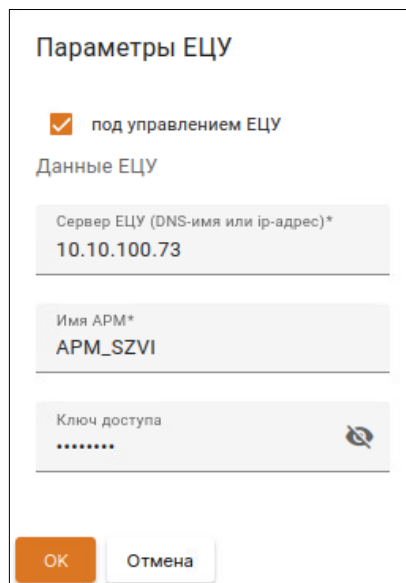


Рис. 264. Ввод в ЕЦУ

5. Нажать кнопку **ОК**, и будет инициировано создание АРМ и регистрация модуля в его составе.

Если во время процесса ввода модуля **СЗИ ВИ Dallas Lock** в ДБ возникает ошибка, содержащая текст «*Ошибка регистрации в ЕЦУ! (Некорректные параметры вызова функции.)*», то необходимо выполнить следующие действия:



- в настройках **ЕЦУ Dallas Lock** (см. «[Общие параметры работы](#)») в параметре **Способ подключения к серверу** установить значение «*Оба способа*» и выбрать приоритет подключения по IP-адресам;
- подождать 30 секунд для применения новых значений;
- повторить попытку ввода модуля **СЗИ ВИ Dallas Lock** в ДБ.

После, при необходимости, можно установить значение по умолчанию для параметра **Способ подключения к серверу** (оба способа с приоритетом подключения по полным доменным именам), на управление уже зарегистрированными в ДБ модулями **СЗИ ВИ Dallas Lock** это не повлияет.

11.2 Вывод модуля из ДБ

Вывести модуль **СЗИ ВИ Dallas Lock** из Домена безопасности можно следующими способами:

- с помощью Консоли **ЕЦУ** (см. «[Настройка модуля](#)»);
- через Консоль Центра управления **СЗИ ВИ Dallas Lock**.

Для вывода модуля через Консоль Центра управления **СЗИ ВИ Dallas Lock** необходимо:

1. Запустить консоль модуля, подключиться к Центру управления **СЗИ ВИ**.
2. Открыть главное меню  → **Параметры ЕЦУ**.
3. Убрать флаг *под управлением ЕЦУ* (рис. 264), чтобы поле настроек стало активно.
4. Нажать кнопку **ОК**.

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



При отсутствии сетевого подключения к Службе **ЕЦУ**, модуль может быть выведен из Домена безопасности **ЕЦУ** принудительно. При этом, в Консоли **ЕЦУ** такой модуль продолжит отображаться, но его статус будет «*Недоступен*».

Поэтому, каждый модуль, выведенный из состава ДБ во время отсутствия связи со Службой **ЕЦУ**, необходимо дополнительно удалять вручную из Консоли **ЕЦУ**.

11.3 Настройка СЗИ ВИ Dallas Lock

В дереве Домена безопасности **ЕЦУ** присутствуют зарегистрированные в ДБ модули **СЗИ ВИ Dallas Lock**, которые отображаются в составе АРМ.

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



- модуль подключен;
- связь с модулем отсутствует.

Настройки на уровне модуля отображаются на нескольких основных вкладках.

11.3.1 Синхронизация

Для приведения в соответствие значениям параметров, выставленным на **ЕЦУ Dallas Lock**, на модуле **СЗИ ВИ Dallas Lock** необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между **ЕЦУ Dallas Lock** и модулем:

- при включении модуля;
- периодически (см. «[Параметры работы модулей](#)»);
- по команде пользователя:
 - из Консоли **ЕЦУ**;
 - из Консоли Центра управления **СЗИ ВИ Dallas Lock**.

Синхронизация по команде из Консоли ЕЦУ

Команда **Синхронизировать** в Консоли **ЕЦУ** для **СЗИ ВИ Dallas Lock** доступна на вкладке **Сводка** на уровне модуля **Dallas Lock СЗИ ВИ** в дереве ДБ на панели инструментов **Оперативное управление** (рис. 265).



Рис. 265. Панель инструментов «Оперативное управление»

Синхронизация по команде из Консоли Центра управления СЗИ ВИ Dallas Lock

Для проведения синхронизации с Доменом безопасности **ЕЦУ Dallas Lock** по команде из Консоли Центра управления **СЗИ ВИ Dallas Lock** на клиентском ПК необходимо выполнить следующие шаги:

1. Запустить консоль модуля, подключиться к Центру управления **СЗИ ВИ**.
2. В категории **Состояние** на вкладке **Основное** нажать кнопку **Действия**.
3. В выпадающем списке нажать кнопку **Синхронизировать с ЕЦУ** (рис. 266).

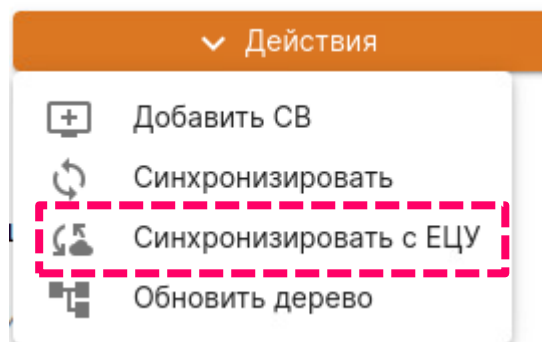


Рис. 266. Кнопка «Синхронизировать с ЕЦУ»

11.3.2 Сбор журналов

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

- при включении модуля;
- периодически (см. [«Параметры работы модулей»](#));
- по команде пользователя из Консоли **ЕЦУ**.

Сбор журналов по команде из Консоли ЕЦУ

Команда **Собрать журналы** в Консоли **ЕЦУ** для модулей **Dallas Lock СЗИ ВИ** доступна на вкладке **Сводка** на уровне модуля в дереве ДБ на панели инструментов **Оперативное управление** (рис. 265).

11.3.3 Сводка модуля Dallas Lock СЗИ ВИ

Вкладка *Сводка* на уровне модуля **Dallas Lock СЗИ ВИ** отображает общее состояние модуля (рис. 267).

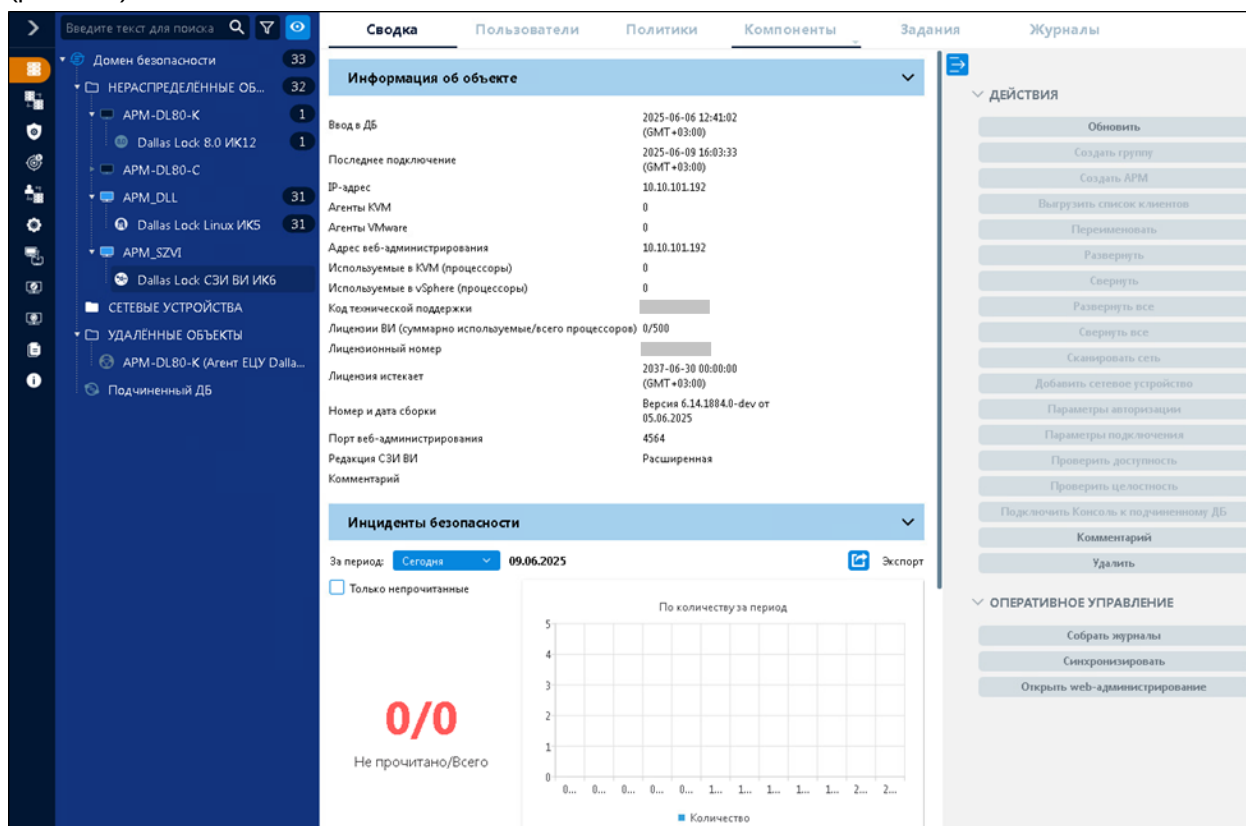


Рис. 267. Вкладка «Сводка»

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;
- IP-адрес;
- номер и дата сборки;
- номер лицензии;
- информация о сроке действия лицензии;
- код технической поддержки;
- параметры лицензии:
 - общее количество лицензий ВИ;
 - количество используемых процессоров в vSphere;
 - количество используемых процессоров в KVM;
- количество агентов VMware;
- количество агентов KVM;
- адрес и порт веб-администрирования;
- редакция **СЗИ ВИ**;
- комментарий к модулю.

Инциденты безопасности

Отображается список инцидентов безопасности модуля с графической панелью. Доступна фильтрация отображаемых событий по периоду и настройка отображения диаграмм (см. [«Настройка инцидентов безопасности»](#)).

Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное. Поле *Комментарий* доступно для редактирования.

Доступны следующие действия с модулем на панели инструментов:

1. Обновить.
2. Удалить модуль.
3. Комментарий.

Доступны следующие команды оперативного управления на панели инструментов:

1. Собрать журналы.
2. Синхронизировать.
3. Открыть web-администрирование.

11.3.4 Web-администрирование

Для перехода в веб-интерфейс **Dallas Lock СЗИ ВИ**, необходимо выбрать команду **Открыть web-администрирование** на панели инструментов *Оперативное управление* (рис. 268).

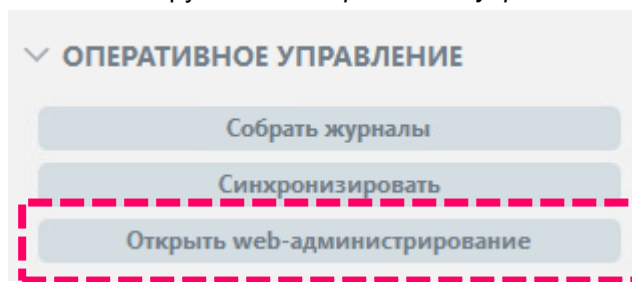


Рис. 268. Кнопка «Открыть web-администрирование»

При нажатии на кнопку **Открыть web-администрирование**, в браузере откроется окно входа в веб-консоль, где необходимо ввести логин и пароль. Затем нажать кнопку **Вход**.

11.3.5 Пользователи и группы модуля Dallas Lock СЗИ ВИ

Вкладка *Пользователи* 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.

11.3.6 Политики модуля Dallas Lock СЗИ ВИ

На уровне модуля **Dallas Lock СЗИ ВИ** в списке на вкладке *Политики* (рис. 269) доступны только политики, актуальные для **Dallas Lock СЗИ ВИ** (см. [«Политики ДБ»](#)).

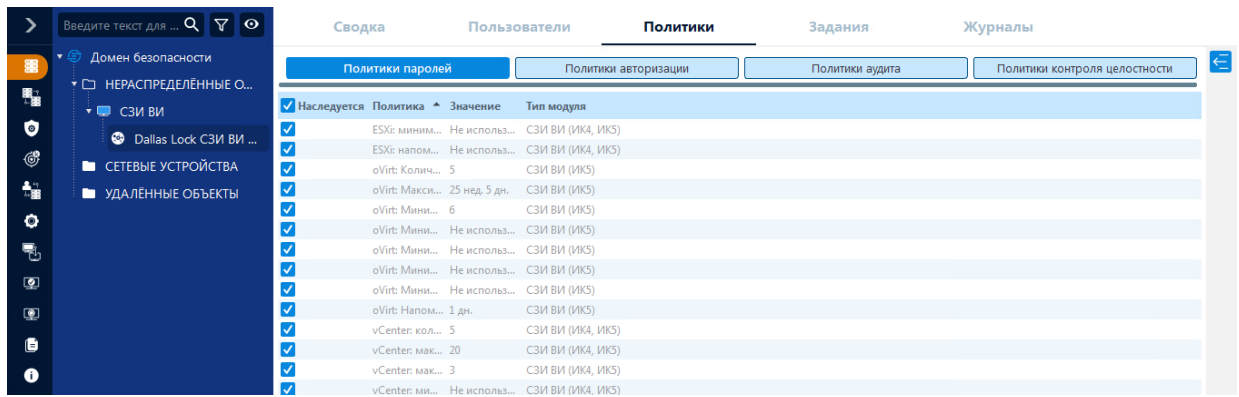


Рис. 269. Политики модуля Dallas Lock C3I BI

Настройка политик для модуля производится аналогично настройке политик для группы ДБ (см. [«Политики для группы ДБ»](#)). Для применения параметров на модулях необходима синхронизация.

11.3.7 Межсетевой экран модуля C3I BI Dallas Lock

На уровне модуля **C3I BI Dallas Lock** в списке на вкладке **Компоненты** → **Межсетевой экран** доступны только политики МЭ, актуальные для **C3I BI Dallas Lock** (см. [«Межсетевой экран»](#)).

Настройка МЭ для модуля производится аналогично настройке МЭ для группы ДБ (см. [«Межсетевой экран для группы ДБ»](#)). Для применения параметров на модулях необходима синхронизация.

11.3.8 Задания модуля Dallas Lock C3I BI

На уровне модуля **Dallas Lock C3I BI** в списке на вкладке **Задания** доступны для создания только задания, актуальные для **Dallas Lock C3I BI**¹⁷ (рис. 270):

- получение конфигурации;
- применение конфигурации;
- проверка обновлений;
- получение отчета о параметрах безопасности **C3I BI**.

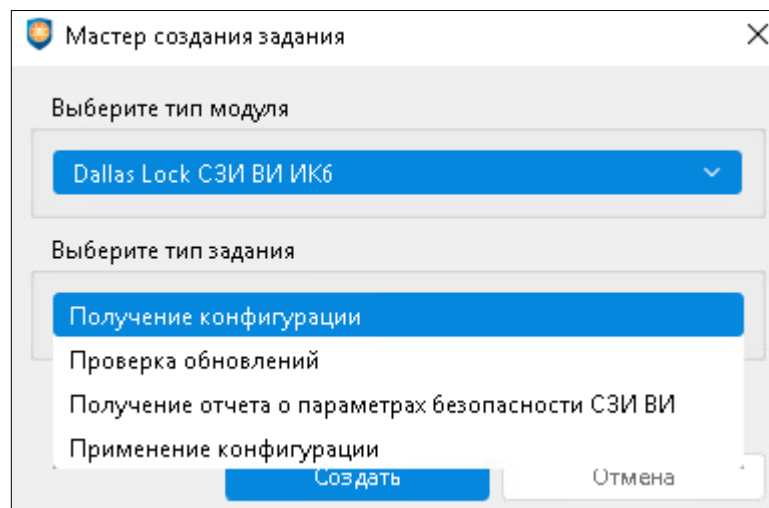


Рис. 270. Мастер создания задания для модуля Dallas Lock C3I BI

¹⁷ Список заданий может меняться в зависимости от версии клиента.

Работа с заданиями для модуля **Dallas Lock СЗИ ВИ** производится аналогично настройке заданий для ДБ (см. [«Задания ДБ»](#)).

11.3.9 Журналы модуля Dallas Lock СЗИ ВИ

Вкладка **Журналы** для модуля **Dallas Lock СЗИ ВИ** позволяет просматривать журналы безопасности модуля (рис. 271).

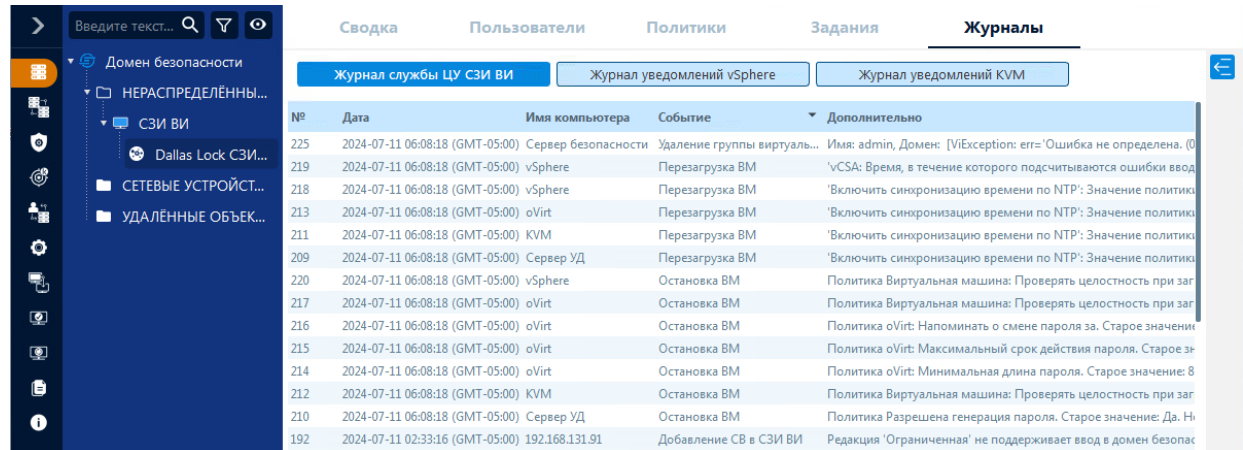


Рис. 271. Вкладка «Журналы»

Для модуля **Dallas Lock СЗИ ВИ** доступны¹⁸:

- «Журнал службы ЦУ СЗИ ВИ»;
- «Журнал уведомлений KVM»;
- «Журнал уведомлений oVirt».

Работа с журналами модулей описана в разделе [«Журналы модуля»](#).

Для получения записей журналов с модуля требуется выполнение сбора журналов.

¹⁸ Список журналов может меняться в зависимости от версии клиента.

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**.



При вводе модуля **СДЗ Dallas Lock** в ДБ должен быть соблюден ряд условий:

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



После ввода модуля **СДЗ Dallas Lock** под управление **ЕЦУ Dallas Lock** значения политик безопасности подлежат синхронизации со значениями политик **ЕЦУ Dallas Lock** для базовой группы «*Нераспределенные объекты*».

Для ввода модуля в ДБ через оболочку администратора необходимо:

1. Убедиться, что сервер **ЕЦУ** доступен по сети.
2. Запустить ТС с установленной платой **СДЗ Dallas Lock**, ввести авторизационные данные и выбрать сценарий сессии *Администрирование*.
3. Дождаться запуска оболочки администратора модуля **СДЗ Dallas Lock**.
4. Перейти на вкладку *Параметры* → категория **Параметры сети** (рис. 272).

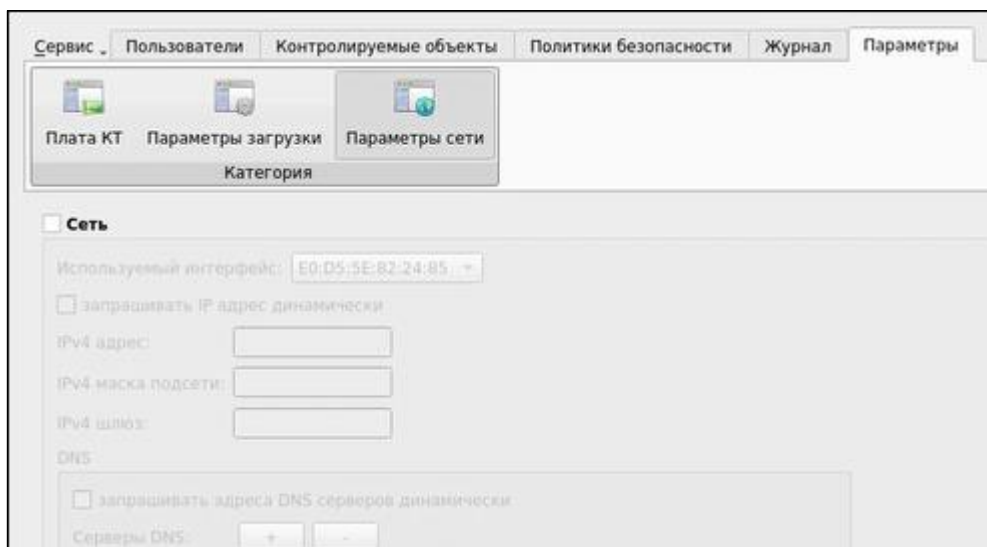


Рис. 272. Вкладка «Параметры сети» модуля СДЗ Dallas Lock

5. Поставить флаг в поле *Сеть*, после чего станут доступны для редактирования другие поля страницы.
6. Заполнить вручную необходимые сетевые параметры или же поставить флаг в поле «запрашивать IP-адрес динамически» для автоматического назначения сетевых параметров DHCP-сервером (рис. 273). Нажать кнопку **Применить**.

Сервис Пользователи Контролируемые объекты Политики безопасности Журнал Параметры

Плата КТ Параметры загрузки Параметры сети

Категория

☒ Сеть

Используемый интерфейс: E0:D5:5E:82:24:85

☒ запрашивать IP адрес динамически

IPv4 адрес: 192.168.12.168

IPv4 маска подсети: 255.255.255.0

IPv4 шлюз: 192.168.12.196

DNS

☒ запрашивать адреса DNS серверов динамически

Серверы DNS: + -

192.168.13.162
192.168.0.172
192.168.0.50
192.168.0.51

Применить

Рис. 273. Заполненные сетевые параметры

7. Заполнить параметры ввода в ДБ на панели **Централизованное управление** (рис. 274):

- выбрать *Единый Центр Управления*;
- указать имя АРМ, в составе которого необходимо ввести модуль;
- указать сетевой адрес сервера **ЕЦУ**;
- ввести ключ доступа к ДБ.

Централизованное управление

☐ Сервер Безопасности ☒ Единый Центр Управления

Имя клиента/АРМ: АРМ_СДЗ

Имя сервера: 192.168.122.125

Ключ доступа: ●●●●

Ввести в ДБ

Рис. 274. 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. 275).

Успешно

Клиент успешно введен в ДБ. При нажатии кнопки ОК будет осуществлена перезагрузка

OK

Рис. 275. 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. 276).

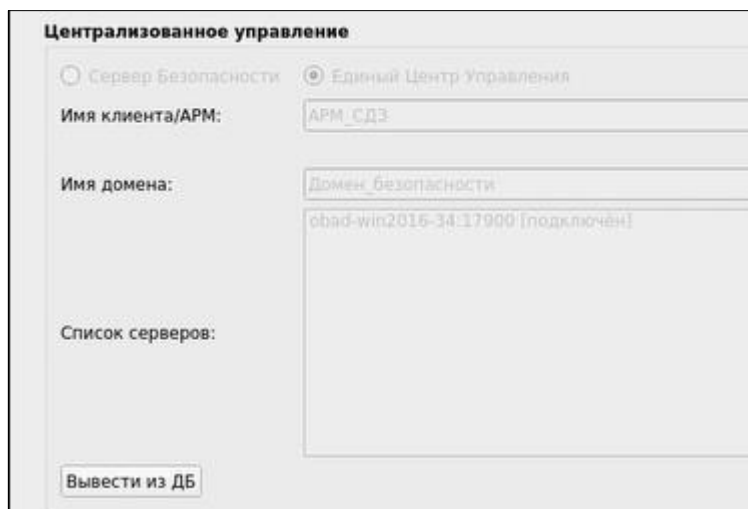


Рис. 276. Вывод модуля СДЗ посредством оболочки администратора

5. Если процесс вывода модуля из ДБ прошел успешно, то через некоторое время появится соответствующее сообщение (рис. 277).

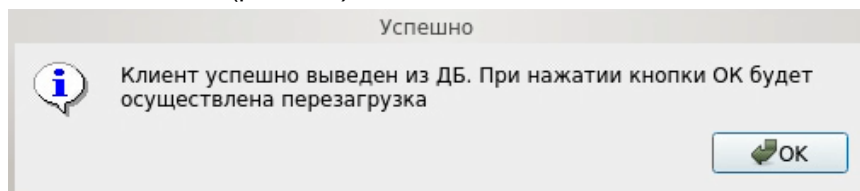


Рис. 277. Сообщение об успешном выводе модуля из ДБ

В Консоли **ЕЦУ** удаленный модуль переместится в базовую группу «Удаленные объекты» при условии наличия связи с **ЕЦУ Dallas Lock**.



При отсутствии сетевого подключения к Службе **ЕЦУ**, модуль может быть выведен из Домена безопасности **ЕЦУ** принудительно. При этом, в Консоли **ЕЦУ** такой модуль продолжит отображаться, но его статус будет «Недоступен».

Поэтому, каждый модуль, выведенный из состава ДБ во время отсутствия связи со Службой **ЕЦУ**, необходимо дополнительно удалять вручную из Консоли **ЕЦУ**.

12.3 Настройка модуля СДЗ Dallas Lock

В дереве Домена безопасности **ЕЦУ Dallas Lock** присутствуют зарегистрированные в ДБ модули **СДЗ Dallas Lock** в составе АРМ.

Значки объектов, обозначающих модули **СДЗ**, зависят от состояния модуля и могут принимать следующий вид:

-  — модуль подключен, выполнен вход в оболочку администратора на АРМ;
-  — модуль находится на связи с **ЕЦУ Dallas Lock** посредством установленного на АРМ Агента ШОС;
-  — связь с модулем отсутствует;
-  — модуль находится в режиме работы ШОС и в ШОС не установлен Агент;
-  — нет соединения между Агентом ШОС и **ЕЦУ Dallas Lock**.

Настройки на уровне модуля отображаются на нескольких основных вкладках.



В **ЕЦУ** все параметры, политики и задания **СДЗ Dallas Lock** доступны для просмотра, редактирования и назначения вне зависимости от варианта исполнения **СДЗ Dallas Lock**, однако их актуальность и возможность применения на конкретном модуле зависят от варианта исполнения **СДЗ Dallas Lock**. Более подробно об ограничениях применения настроек описано в соответствующих пунктах данного подраздела.

12.3.1 Синхронизация

Для приведения в соответствие значениям параметров, выставленным на **ЕЦУ Dallas Lock**, на модуле **СДЗ Dallas Lock** необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между **ЕЦУ Dallas Lock** и модулем при включении модуля.

12.3.2 Сбор журналов

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

12.3.3 Сводка модуля СДЗ Dallas Lock

Вкладка **Сводка** на уровне модуля **СДЗ Dallas Lock** отображает общее состояние модуля (рис. 278).

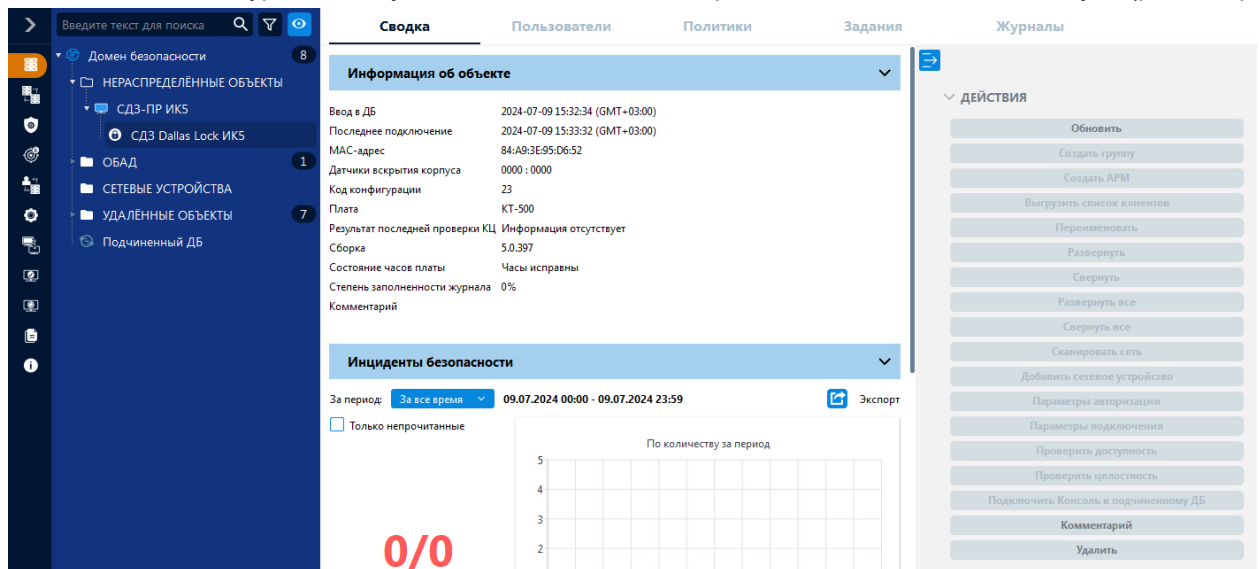


Рис. 278. Вкладка «Сводка»

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; • код конфигурации¹⁹; • состояние часов платы; • номер сборки; • состояние датчиков вскрытия корпуса¹⁹; • 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 <i>Комментарий</i> 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. Удаленное включение.
5. Пересчитать целостность.
6. Отправить данные для авторизации.
7. Удаленное управление.

12.3.4 Пользователи модуля СДЗ Dallas Lock

Вкладка *Пользователи* 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.



Изменение для учетной записи **СДЗ Dallas Lock** атрибута, являющегося для данного варианта исполнения **СДЗ Dallas Lock** неактуальным, никак не отразится на модуле **СДЗ Dallas Lock**.

Подробнее о применимости атрибутов для учетных записей различных вариантов исполнения **СДЗ Dallas Lock** см. [«Параметры пользователей»](#).

¹⁹ Информация о коде конфигурации и о датчике вскрытия корпуса неактуальна для вариантов исполнения **СДЗ Dallas Lock** ПФНА.26.20.40.140.001-04 и ПФНА.26.20.40.140.001-05 (платы **СДЗ Dallas Lock** формата USB «KT-600-PLS» и USB «KT-600-Type A»).

12.3.5 Политики модуля СДЗ Dallas Lock

На уровне модуля **СДЗ Dallas Lock** в списке на вкладке *Политики* доступны только политики, актуальные для **СДЗ Dallas Lock** (см. [«Политики ДБ»](#)), вне зависимости от варианта исполнения **СДЗ Dallas Lock**.



Если политики являются неактуальными для варианта исполнения **СДЗ Dallas Lock**, для которого выполняется настройка, изменение параметров данных политик никак не отразится на модуле **СДЗ Dallas Lock**.

Информация об ограничениях в применимости политик для конкретных вариантов исполнения **СДЗ Dallas Lock** приведена в соответствующих пунктах подраздела [«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 вкладке *Задания* доступны для создания только задания, актуальные для **СДЗ Dallas Lock** (рис. 279):

- сбросить ДВК²⁰;
- очистка журнала;
- получение конфигурации;
- получение отчета об аппаратном обеспечении;
- тестирование функций **СДЗ**;
- получение отчета по конфигурации;
- применение конфигурации.

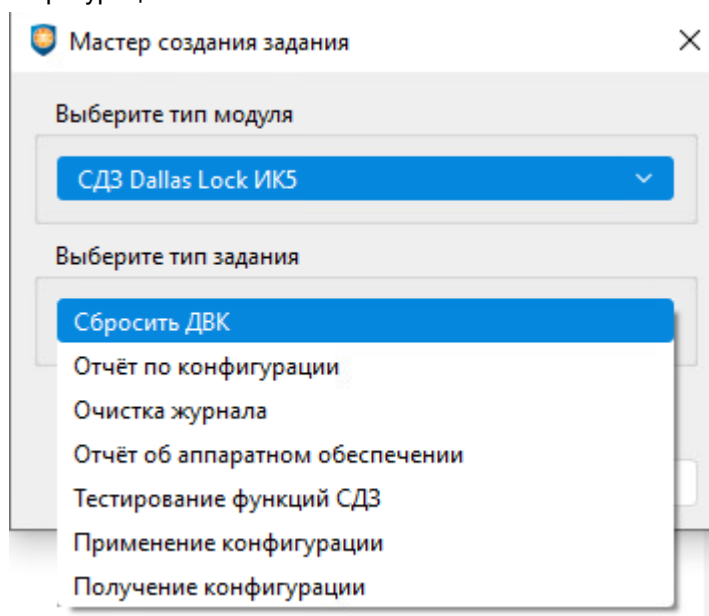


Рис. 279. Мастер создания задания для модуля СДЗ

Работа с заданиями для модуля **СДЗ Dallas Lock** производится аналогично настройке заданий для ДБ (см. [«Задания модуля»](#)).

²⁰ Задание «Сбросить ДВК» можно создать для всех исполнений **СДЗ Dallas Lock**, но данное задание отработает только для плат формата PCIe «КТ-500» (более подробно об ограничениях реализации различных вариантов исполнения **СДЗ Dallas Lock** описано в Руководстве по эксплуатации **СДЗ Dallas Lock**).

12.3.7 Журналы модуля СД3 Dallas Lock

Вкладка *Журналы* для модуля **СД3 Dallas Lock** позволяет просматривать журналы безопасности модуля (рис. 280).

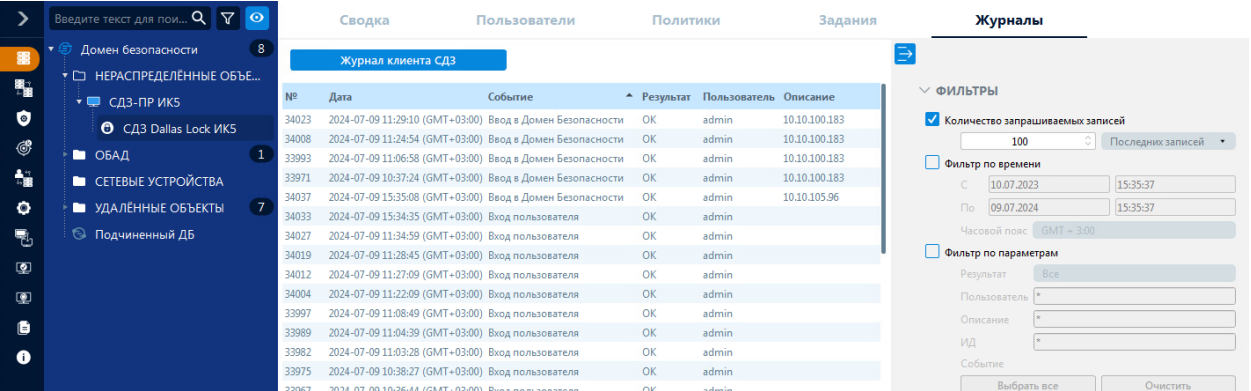


Рис. 280. Вкладка «Журналы»

Для модуля **СД3 Dallas Lock** доступны:

- «Журнал клиента СД3».

Работа с журналами модулей описана в разделе [«Журналы модуля»](#).

Для получения записей журнала с модуля требуется перезагрузка модуля **СД3 Dallas Lock**.

13 МОДУЛЬ СДЗ УБ DALLAS LOCK

13.1 Ввод модуля в ДБ

Ввести модуль **СДЗ УБ Dallas Lock** в Домен безопасности можно через оболочку администратора **СДЗ УБ Dallas Lock**.



При вводе модуля **СДЗ УБ Dallas Lock** в ДБ должен быть соблюден ряд условий:

- в ЛВС должен быть работающий сервер **ЕЦУ**;
- между модулем и сервером **ЕЦУ** должен быть свободный обмен пакетами по протоколу TCP/IP, порт 17900.



После ввода модуля **СДЗ УБ Dallas Lock** под управление **ЕЦУ Dallas Lock** значения политик безопасности подлежат синхронизации со значениями политик **ЕЦУ Dallas Lock** для базовой группы «*Нераспределенные объекты*».

Для ввода модуля в ДБ через оболочку администратора необходимо:

1. Убедиться, что сервер **ЕЦУ** доступен по сети.
2. Запустить ТС с модулем **СДЗ УБ Dallas Lock**, ввести авторизационные данные и выбрать сценарий сессии *Администрирование*.
3. Дождаться запуска оболочки администратора модуля **СДЗ УБ Dallas Lock**.
4. Перейти на вкладку *Параметры* → категория **Параметры сети** (рис. 281).

Рис. 281. Вкладка «Параметры сети» модуля СДЗ УБ Dallas Lock

5. Активировать чекбокс в поле *Сеть*, после чего станут доступны для редактирования другие поля страницы.
6. Заполнить вручную необходимые сетевые параметры или же поставить флаг в поле *запрашивать IP-адрес динамически* для автоматического назначения сетевых параметров DHCP-сервером. Нажать кнопку **Применить**.
7. Заполнить параметры ввода в ДБ на панели *Централизованное управление*:
 - указать имя клиента/АРМ, в составе которого необходимо ввести модуль;
 - указать сетевой адрес сервера **ЕЦУ**/имя сервера **ЕЦУ**;
 - ввести ключ доступа к ДБ.
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. 282).

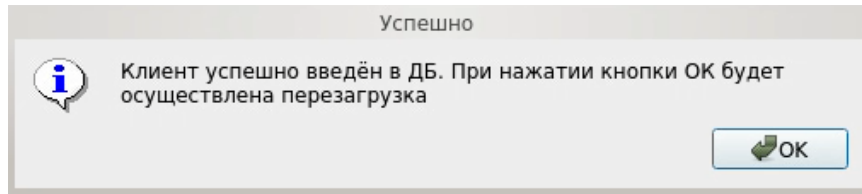


Рис. 282. Сообщение об успешном вводе модуля в ДБ

В Консоли **ЕЦУ** в группе дерева ДБ «Нераспределенные объекты» появится новый АРМ с указанным именем, в котором зарегистрирован модуль **СДЗ УБ Dallas Lock**. Если был указан уже существующий в ДБ **ЕЦУ** АРМ, то модуль СДЗ добавится в него.

13.2 Вывод модуля из ДБ

Вывести модуль **СДЗ УБ Dallas Lock** из Домена безопасности можно следующими способами:

- с помощью Консоли **ЕЦУ** (см. [«Настройка модуля»](#));
- через оболочку администратора **СДЗ УБ Dallas Lock**.

Для вывода модуля через оболочку администрирования необходимо:

1. Запустить ТС с модулем **СДЗ УБ Dallas Lock**, ввести авторизационные данные и выбрать сценарий сессии *Администрирование*.
2. Дождаться запуска оболочки администратора модуля **СДЗ УБ Dallas Lock**.
3. Перейти на вкладку *Параметры* → категория *Параметры сети*.
4. На панели *Централизованное управление* нажать кнопку **Вывести из ДБ**.
5. Если процесс вывода модуля из ДБ прошел успешно, то через некоторое время появится соответствующее сообщение (рис. 283).

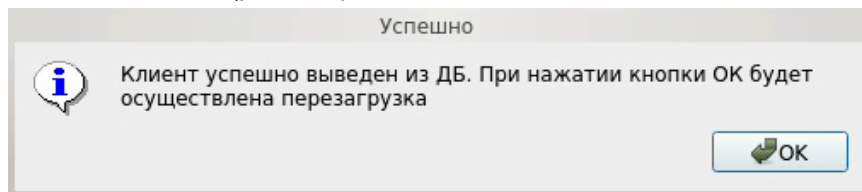


Рис. 283. Сообщение об успешном выводе модуля из ДБ

В Консоли **ЕЦУ** удаленный модуль переместится в базовую группу «Удаленные объекты» при условии наличия связи с **ЕЦУ Dallas Lock**.



При отсутствии сетевого подключения к Службе **ЕЦУ**, модуль может быть выведен из Домена безопасности **ЕЦУ** принудительно. При этом, в Консоли **ЕЦУ** такой модуль продолжит отображаться, но его статус будет «Недоступен».

Поэтому, каждый модуль, выведенный из состава ДБ во время отсутствия связи со Службой **ЕЦУ**, необходимо дополнительно удалять вручную из Консоли **ЕЦУ**.

13.3 Настройка модуля СДЗ УБ Dallas Lock

Настройка модуля **СДЗ УБ Dallas Lock** производится аналогичным образом, как и в **СДЗ Dallas Lock** (см. [«Настройка модуля СДЗ Dallas Lock»](#)).

13.3.1 Синхронизация

Для приведения в соответствие значениям параметров, выставленным на **ЕЦУ Dallas Lock**, на модуле **СДЗ УБ Dallas Lock** необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между **ЕЦУ Dallas Lock** и модулем при включении модуля.

13.3.2 Сбор журналов

Для получения в ЕЦУ Dallas Lock записей журналов, ведущихся на модуле **СДЗ УБ Dallas Lock**, необходимо проведение сбора журналов. Сбор журналов может быть проведен при условии наличия сетевого подключения между ЕЦУ и модулем при включении модуля.

13.3.3 Сводка модуля СДЗ УБ Dallas Lock

Вкладка *Сводка* на уровне модуля **СДЗ УБ Dallas Lock** отображает общее состояние модуля (рис. 284).

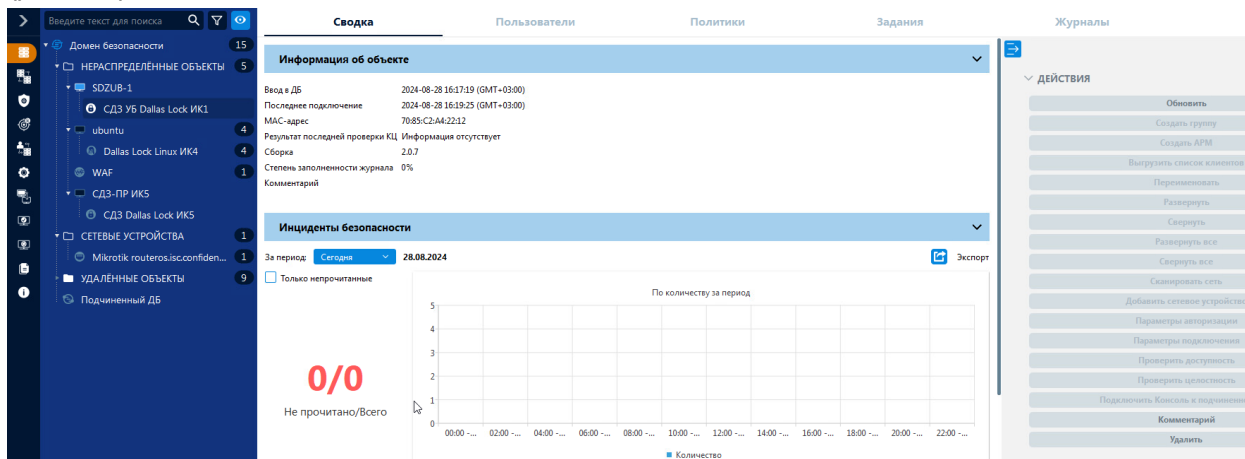


Рис. 284. Вкладка «Сводка»

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 сборки;
- степень заполненности журналов;
- MAC-адрес;
- результат последней проверки КЦ;
- комментарий к модулю.

Инциденты безопасности

Отображается список инцидентов безопасности модуля с графической панелью. Доступна фильтрация отображаемых событий по периоду и настройка отображения диаграмм (см. [«Настройка инцидентов безопасности»](#)).

Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное. Поле *Комментарий* доступно для редактирования.

Доступны следующие действия с модулем на панели инструментов:

1. Обновить.
2. Удалить модуль.
3. Комментарий.

Доступны следующие команды оперативного управления на панели инструментов:

1. Выключить.
2. Перезагрузить.
3. Разблокировать пользователей.
4. Удаленное включение.
5. Пересчитать целостность.

13.3.4 Пользователи модуля СДЗ УБ Dallas Lock

Вкладка *Пользователи* на уровне модуля **СДЗ УБ 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 УБ Dallas Lock** производится аналогично описанному управлению пользователями и группами в разделе [«Пользователи и группы модуля»](#). Для применения изменений на модулях необходима перезагрузка.

13.3.5 Политики модуля СДЗ УБ Dallas Lock

На уровне модуля **СДЗ УБ Dallas Lock** в списке на вкладке *Политики* доступны только политики, актуальные для **СДЗ УБ 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.

13.3.6 Задания модуля СДЗ УБ Dallas Lock

На уровне модуля **СДЗ УБ Dallas Lock** в списке на вкладке *Задания* доступны для создания только задания, актуальные для **СДЗ УБ Dallas Lock** (рис. 285):

- очистка журнала;
- получение конфигурации;
- получение отчета об аппаратном обеспечении;
- тестирование функций **СДЗ**;
- получение отчета по конфигурации;
- применение конфигурации.

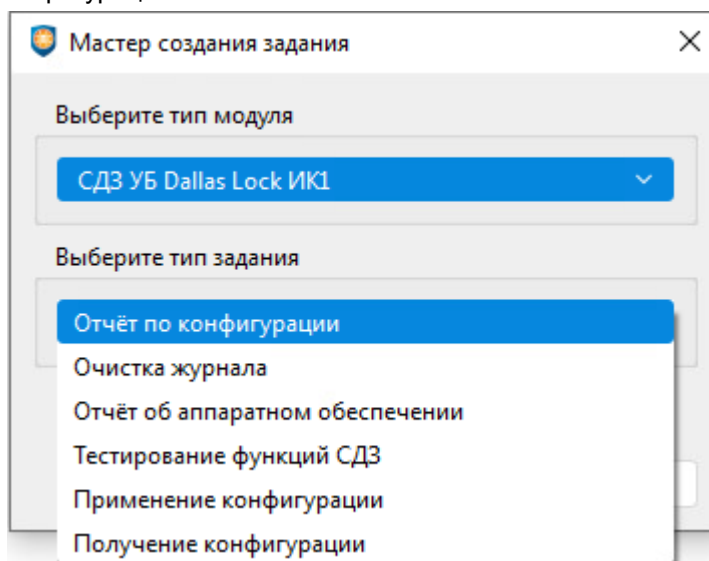


Рис. 285. Мастер создания задания для модуля СДЗ УБ

Работа с заданиями для модуля **СДЗ УБ Dallas Lock** производится аналогично настройке заданий для ДБ (см. [«Задания модуля»](#)).

13.3.7 Журналы модуля СДЗ УБ Dallas Lock

Работа с журналами для модуля **СДЗ УБ Dallas Lock** производится аналогично работе с журналами для **СДЗ Dallas Lock** (см. [«Журналы модуля СДЗ Dallas Lock»](#)).

14 МОДУЛЬ WAF DALLAS LOCK

14.1 Ввод модуля в ДБ

Ввести модуль **WAF Dallas Lock** в Домен безопасности можно через веб-интерфейс модуля.



При вводе модуля WAF Dallas Lock в ДБ должен быть соблюден ряд условий:

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

Для ввода модуля в ДБ через веб-интерфейс модуля необходимо:

1. Убедиться, что сервер **ЕЦУ** доступен по сети.
2. Запустить веб-интерфейс модуля и авторизоваться.
3. Перейти на вкладку *Настройки* → пункт **Настройки модуля ЕЦУ** (рис. 286).

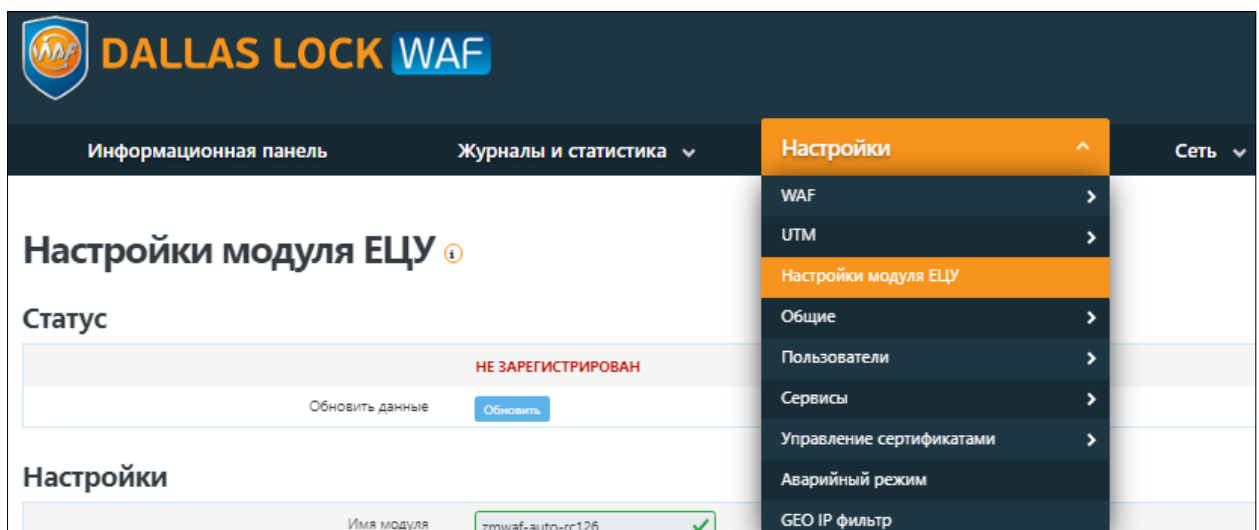
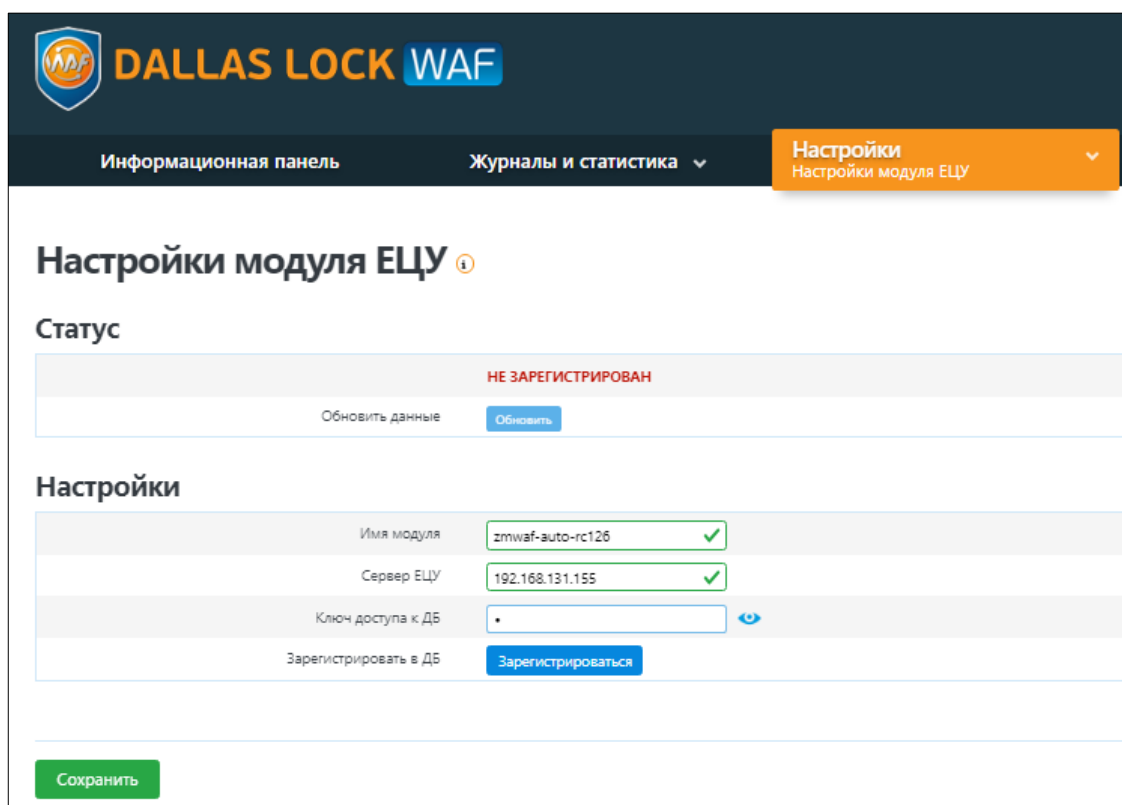


Рис. 286. Вкладка «Настройки»

4. В разделе *Настройки* заполнить параметры ввода в ДБ (рис. 287):
 - имя модуля;
 - сетевой адрес сервера **ЕЦУ**;
 - ключ доступа к ДБ.



DALLAS LOCK WAF

Информационная панель Журналы и статистика **Настройки**
Настройки модуля ЕЦУ

Настройки модуля ЕЦУ ⓘ

Статус

НЕ ЗАРЕГИСТРИРОВАН

Обновить данные Обновить

Настройки

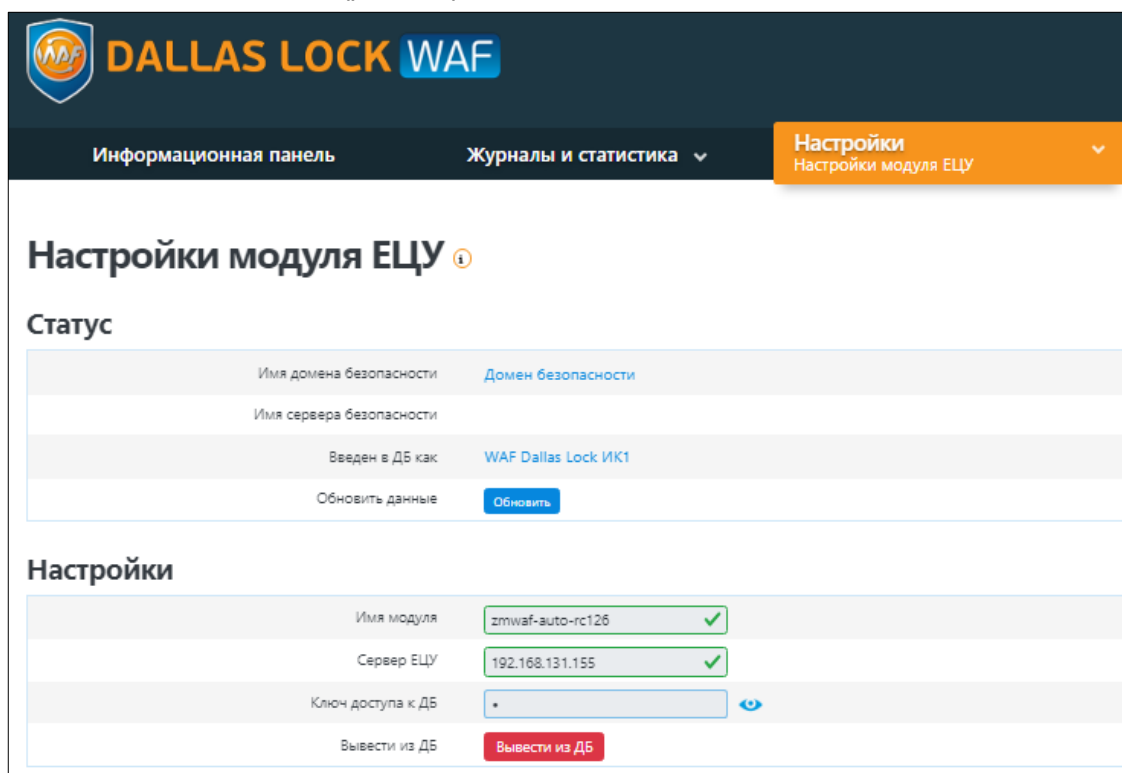
Имя модуля	znmwaf-auto-rc126 ✓
Сервер ЕЦУ	192.168.131.155 ✓
Ключ доступа к ДБ	• 🔍
Зарегистрировать в ДБ	Зарегистрироваться

Сохранить

Рис. 287. Настройки модуля ЕЦУ

5. Далее необходимо нажать кнопку **Зарегистрироваться**.

Если процесс ввода модуля в ДБ прошел успешно, то через некоторое время поля с настройками станут недоступными для редактирования, в разделе *Статус* появится информация о Домене безопасности **ЕЦУ Dallas Lock** (рис. 288).



DALLAS LOCK WAF

Информационная панель Журналы и статистика **Настройки**
Настройки модуля ЕЦУ

Настройки модуля ЕЦУ ⓘ

Статус

Имя домена безопасности	Домен безопасности
Имя сервера безопасности	
Введен в ДБ как	WAF Dallas Lock ИК1
Обновить данные	Обновить

Настройки

Имя модуля	znmwaf-auto-rc126 ✓
Сервер ЕЦУ	192.168.131.155 ✓
Ключ доступа к ДБ	• 🔍
Вывести из ДБ	Вывести из ДБ

Рис. 288. Статус

В Консоли **ЕЦУ** в дереве ДБ в группе «Нераспределенные объекты» появится модуль **WAF** (без АРМ) с соответствующим именем (рис. 289).

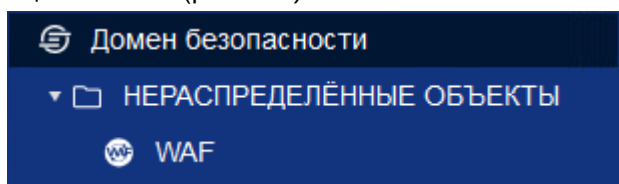


Рис. 289. Иконка модуля в дереве ДБ

После успешного ввода модуля в состав ДБ **ЕЦУ Dallas Lock**, на **WAF** автоматически настраивается синхронизация по времени с **ЕЦУ Dallas Lock**.

14.2 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. 290).

Рис. 290. Вывод из ДБ

Если процесс вывода модуля из ДБ прошел успешно, то через некоторое время поля с настройками модуля **ЕЦУ Dallas Lock** станут доступными для редактирования, в разделе *Состояние* отобразится статус «НЕ ЗАРЕГИСТРИРОВАН».

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



При отсутствии сетевого подключения к Службе **ЕЦУ**, модуль может быть выведен из Домена безопасности **ЕЦУ** принудительно. При этом, в Консоли **ЕЦУ** такой модуль продолжит отображаться, но его статус будет «Недоступен».

Поэтому, каждый модуль, выведенный из состава ДБ во время отсутствия связи со Службой **ЕЦУ**, необходимо дополнительно удалять вручную из Консоли **ЕЦУ**.



При выполнении задания с Консоли **ЕЦУ** на сброс к заводским настройкам, модуль **WAF Dallas Lock** принудительно выводится из домена безопасности **ЕЦУ**.

14.3 Настройка модуля WAF Dallas Lock

В дереве Домена безопасности **ЕЦУ Dallas Lock** присутствуют зарегистрированные в ДБ модули **WAF Dallas Lock**.

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



— модуль подключен;

— связь с модулем отсутствует.

Настройки на уровне модуля отображаются на нескольких основных вкладках.



В случае если два или более модулей **WAF** подключены к **ЕЦУ Dallas Lock**, и на одном из них происходит блокировка каких-либо атакующих узлов — данные блокировки передаются через **ЕЦУ Dallas Lock** на все подключенные к **ЕЦУ Dallas Lock** модули **WAF Dallas Lock**. После этого, все подключенные к **ЕЦУ Dallas Lock** модули **WAF Dallas Lock** — блокируют атакующий хост до истечения времени блокировки.

14.3.1 Синхронизация

Для отправки на **ЕЦУ Dallas Lock** сведений о модуле **WAF Dallas Lock** и приведения в соответствие системного времени необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между **ЕЦУ Dallas Lock** и модулем:

- при включении модуля;
- периодически (см. [«Параметры работы модулей»](#));
- по команде пользователя:
 - из Консоли **ЕЦУ**;
 - посредством веб-интерфейса модуля **WAF Dallas Lock**.

Синхронизация по команде из Консоли ЕЦУ

Команда **Синхронизировать** в Консоли **ЕЦУ** для **WAF Dallas Lock** доступна на вкладке *Сводка* на уровне модуля **WAF Dallas Lock** в дереве Домена безопасности на панели инструментов *Оперативное управление* (рис. 291).

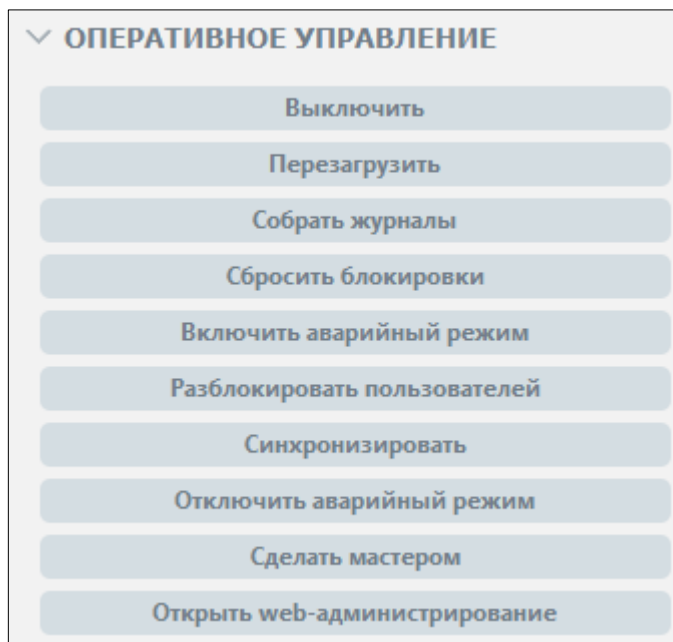


Рис. 291. Панель инструментов «Оперативное управление»

Синхронизация по команде из веб-интерфейса модуля WAF Dallas Lock

Для проведения синхронизации с Доменом безопасности **ЕЦУ Dallas Lock** по команде из веб-интерфейса модуля **WAF Dallas Lock** необходимо выполнить следующие шаги:

1. Запустить веб-интерфейс модуля и авторизоваться.
2. Перейти на вкладку *Настройки* → пункт **Настройки модуля ЕЦУ**.
3. В разделе *Статус* нажать кнопку **Обновить** (рис. 292).

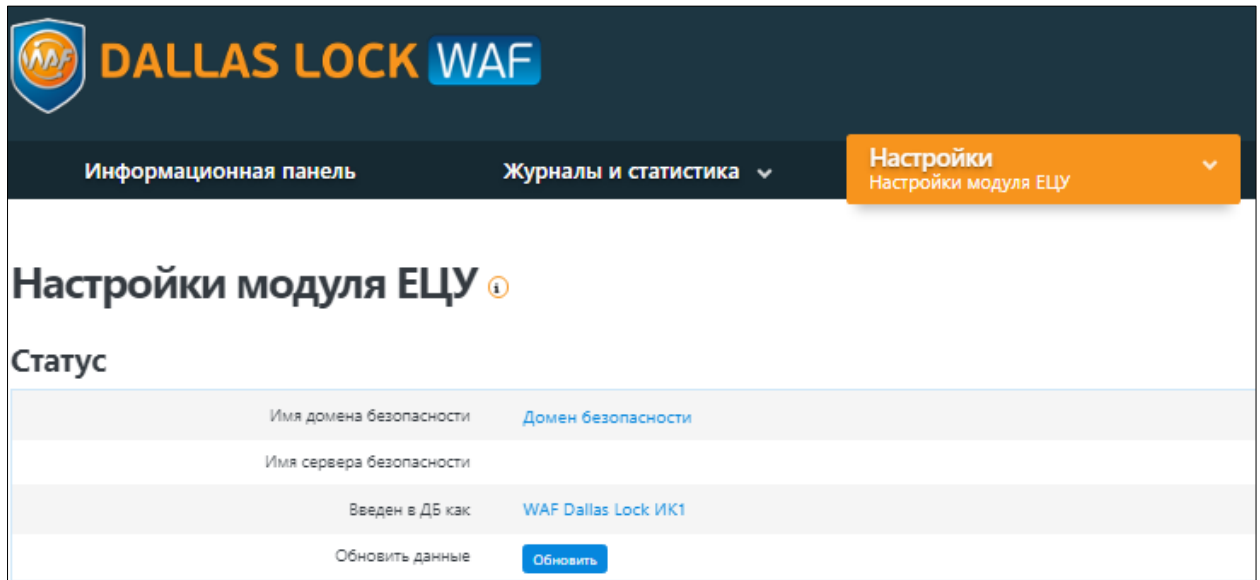


Рис. 292. Кнопка «Обновить»

14.3.2 Сбор журналов

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

- при включении модуля;
- периодически (см. [«Параметры работы модулей»](#));
- по команде пользователя из Консоли **ЕЦУ**.

Сбор журналов по команде из Консоли ЕЦУ

Команда **Собрать журналы** в Консоли **ЕЦУ** для модуля **WAF Dallas Lock** доступна на вкладке *Сводка* на уровне модуля в дереве Домена безопасности на панели инструментов *Оперативное управление* (рис. 291).

14.3.3 Сводка модуля WAF Dallas Lock

Вкладка **Сводка** на уровне модуля **WAF Dallas Lock** отображает общее состояние модуля (рис. 293).

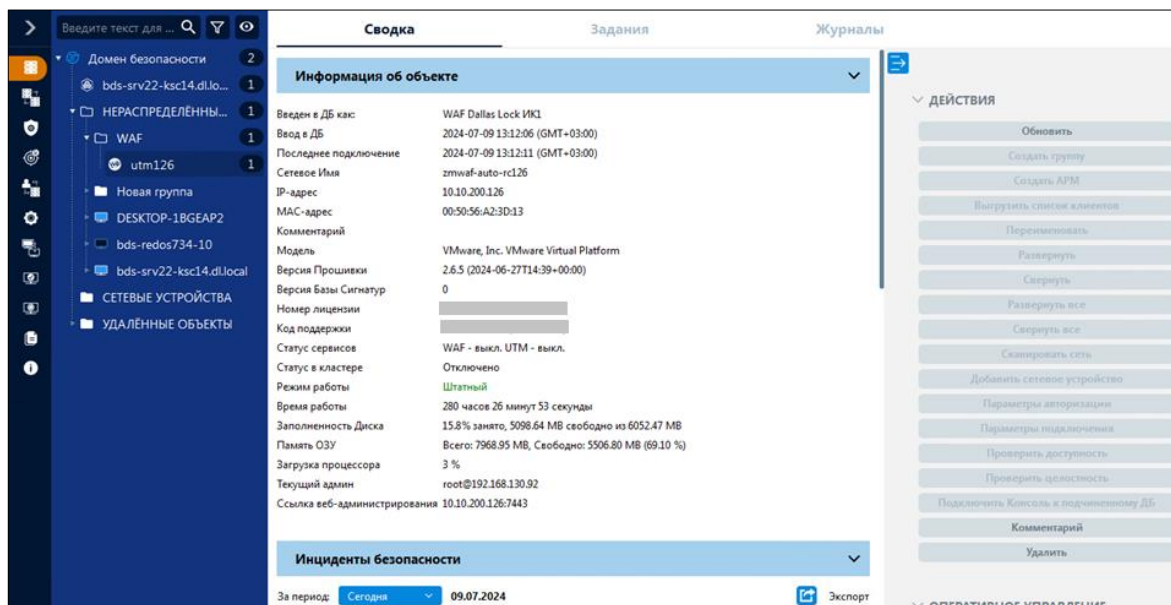


Рис. 293. Вкладка «Сводка»

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;
- последнее подключение;
- сетевое имя;
- IP-адрес;
- MAC-адрес;
- комментарий к модулю;
- модель;
- версия прошивки;
- версия базы сигнатур;
- номер лицензии и код технической поддержки;
- статус сервисов;
- статус в кластере;
- режим работы (штатный/аварийный);
- время работы;
- информация о заполненности диска;
- память ОЗУ;
- загрузка процессора;
- текущий админ;
- ссылка для веб-администрирования.

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. Комментарий.
3. Удалить.

Доступны следующие команды оперативного управления на панели инструментов:

1. Выключить.
2. Перезагрузить.
3. Собрать журналы.
4. Сбросить блокировки.
5. Включить аварийный режим.
6. Разблокировать пользователей.
7. Синхронизировать.
8. Отключить аварийный режим.
9. Сделать мастером.
10. Открыть web-администрирование.

14.3.4 Задания модуля WAF Dallas Lock

На уровне модуля **WAF Dallas Lock** в списке на вкладке *Задания* доступны для создания только задания, актуальные для **WAF Dallas Lock** (рис. 294):

- создать резервную копию;
- восстановить резервную копию;
- сбор журналов;
- сброс к заводским настройкам;
- обновление базы решающих правил;
- применение файла лицензии.

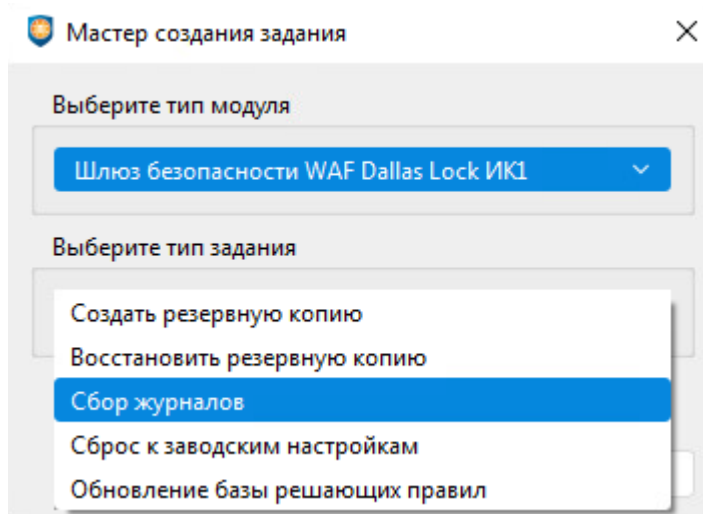


Рис. 294. Мастер создания задания для модуля WAF Dallas Lock

Работа с заданиями для модуля **WAF Dallas Lock** производится аналогично настройке заданий для ДБ (см. [«Задания ДБ»](#)).



При выполнении задания с Консоли **ЕЦУ** на сброс к заводским настройкам, модуль **WAF Dallas Lock** восстанавливает свою конфигурацию по умолчанию и принудительно выводится из домена безопасности **ЕЦУ**, при этом все выполненные задания модуля в консоли управления **ЕЦУ** удаляются.

14.3.5 Журналы модуля WAF Dallas Lock

Вкладка *Журналы* для модуля **WAF Dallas Lock** позволяет просматривать журналы безопасности модуля (рис. 295).

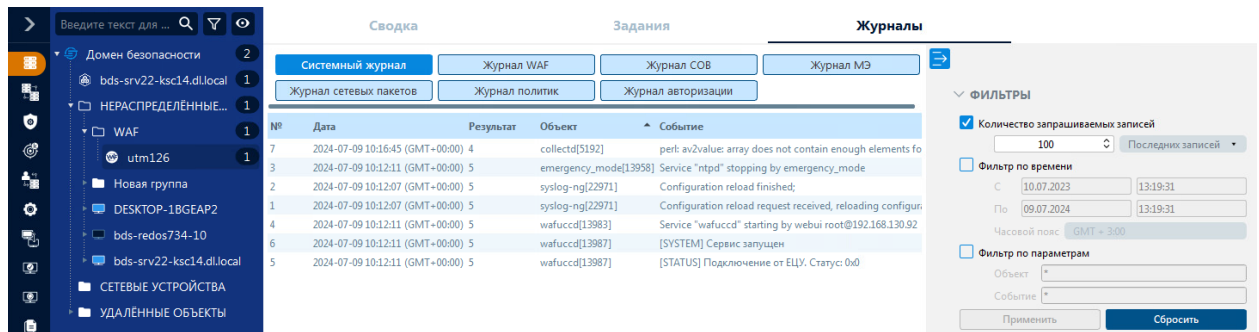


Рис. 295. Вкладка «Журналы»

Для модуля **WAF Dallas Lock** доступны:

- «Системный журнал»;
- «Журнал WAF»;
- «Журнал COB»;
- «Журнал МЭ»;
- «Журнал сетевых пакетов»;
- «Журнал политик»;
- «Журнал авторизации».

Работа с журналами модулей описана в разделе [«Журналы модуля»](#).

Для получения записей журналов с модуля требуется выполнение сбора журналов.

15 АГЕНТ ЕЦУ

Независимый агент для ПК (далее — **Агент ЕЦУ**) предназначен для передачи базовой информации об устройстве (системные журналы, версия ОС, IP- и MAC-адреса), на которое он установлен.

15.1 Требования к аппаратному и программному обеспечению

Агент ЕЦУ представляет собой службу, работающую в фоновом режиме, устанавливаемую на ПК, для последующего ввода в ДБ **ЕЦУ Dallas Lock**. **Агентом ЕЦУ** поддерживаются следующие типы операционных систем семейства Windows:

- Windows 7 x32, x64 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
- Windows Server 2012 x64 (Foundation, Essentials, Standard, Datacenter);
- Windows 8.1 x32, x64 (Core, Pro, Enterprise);
- Windows Server 2012 R2 x64 (Foundation, Essentials, Standard, Datacenter);
- Windows 10 x32, x64 (Enterprise, Education, Pro, Home);
- Windows Server 2016 x64 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server);
- Windows Server 2019 x64 (Standard, Datacenter, Essentials);
- Windows Server 2022 x64 (Standard, Datacenter);
- Windows 11 x64 (Home, Pro, Enterprise, Education);

и семейства Linux (x64):

- Debian 10.x;
- Debian 11.x;
- Debian 12.x;
- Ubuntu 18.04 LTS;
- Ubuntu 20.04 LTS;
- Ubuntu 22.04 LTS;
- Ubuntu 24.04 LTS;
- Astra Linux Common Edition (Орел) 2.12;
- Astra Linux Special Edition (Смоленск) 1.6;
- Astra Linux Special Edition (Смоленск) 1.7, 1.8;
- Альт Сервер 9;
- Альт Сервер 10.0, 10.1, 10.2, 10.4;
- Альт 8 СП Сервер 10;
- Альт Рабочая Станция 9.x;
- Альт Рабочая Станция 10.0, 10.1, 10.2, 10.4;
- Альт Рабочая Станция К 10.0, 10.1, 10.3, 10.4;
- Альт 8 СП Рабочая Станция 10;
- РЕД ОС 7.3 Муром;
- РЕД ОС 8;
- ROSA FRESH DESKTOP 12.

Агентом ЕЦУ Dallas Lock Android поддерживаются следующие процессорные архитектуры:

- armeabi-v7a;
- arm64-v8a;
- x86_64;
- x86.

Агент ЕЦУ Dallas Lock Android поддерживает версии Android8 и все более новые версии.

15.2 Установка и удаление Агента ЕЦУ

15.2.1 Локальная установка Агента ЕЦУ

До установки **Агента ЕЦУ** на ОС Linux необходимо произвести дополнительные действия в терминале:

- для Debian, Ubuntu, Astra Linux, Альт Рабочая Станция выполнить команду:
`apt-get update`
- для Red Hat Enterprise Linux, РЕД ОС выполнить команду:
`yum repolist ; yum makecache`

Для установки **Агента ЕЦУ** необходимо запустить установочный файл `uccAgentInst`, который находится в корневой директории дистрибутива (или выбрать данное действие в меню окна `autorun`).



При установке **Агента ЕЦУ** на ПК с ОС Linux, перед запуском установочного файла, необходимо проверить, является ли файл «`uccAgentInst`» исполняемым. Для этого можно воспользоваться следующей командой:
`chmod a+x <путь к файлу>.run.`



Для подключения к **Агенту ЕЦУ** по VNC требуется дополнительно открыть TCP-порт 17902, исходящее подключение.

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

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

1. После запуска приложения на экране будет выведено окно для подтверждения операции. После подтверждения запустится мастер установки **Агента ЕЦУ Dallas Lock** (рис. 296).

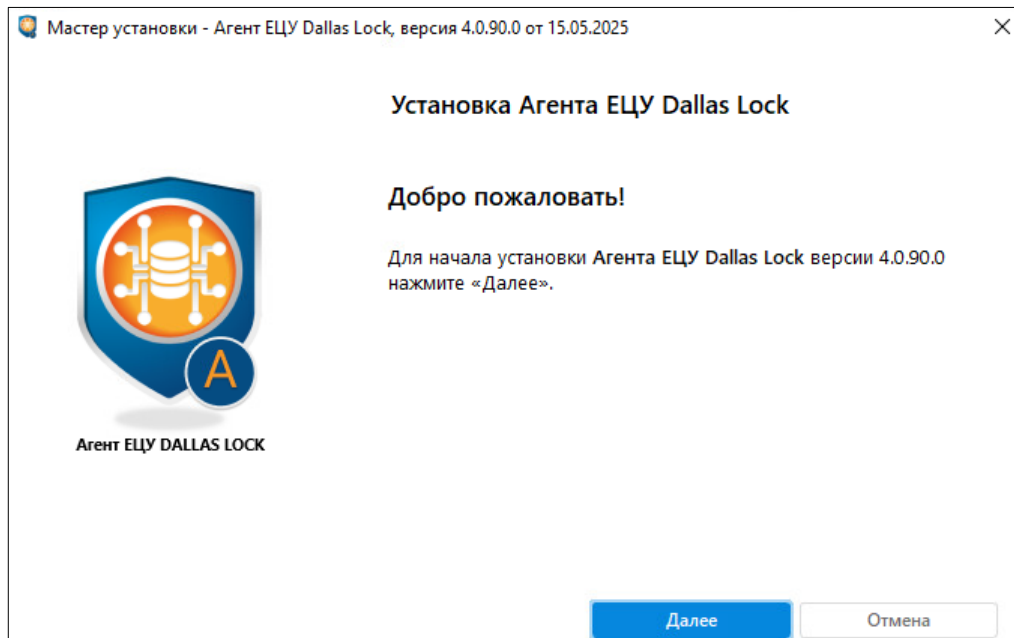


Рис. 296. Окно начала установки Агента ЕЦУ

Для продолжения установки нажать кнопку **Далее**.

2. На следующем шаге можно сразу ввести компьютер в ДБ, установив флаг напротив *Ввести*

компьютер в Домен Безопасности. После установки флага станут доступны для изменения параметры регистрации **Агента ЕЦУ** в ДБ (рис. 297).

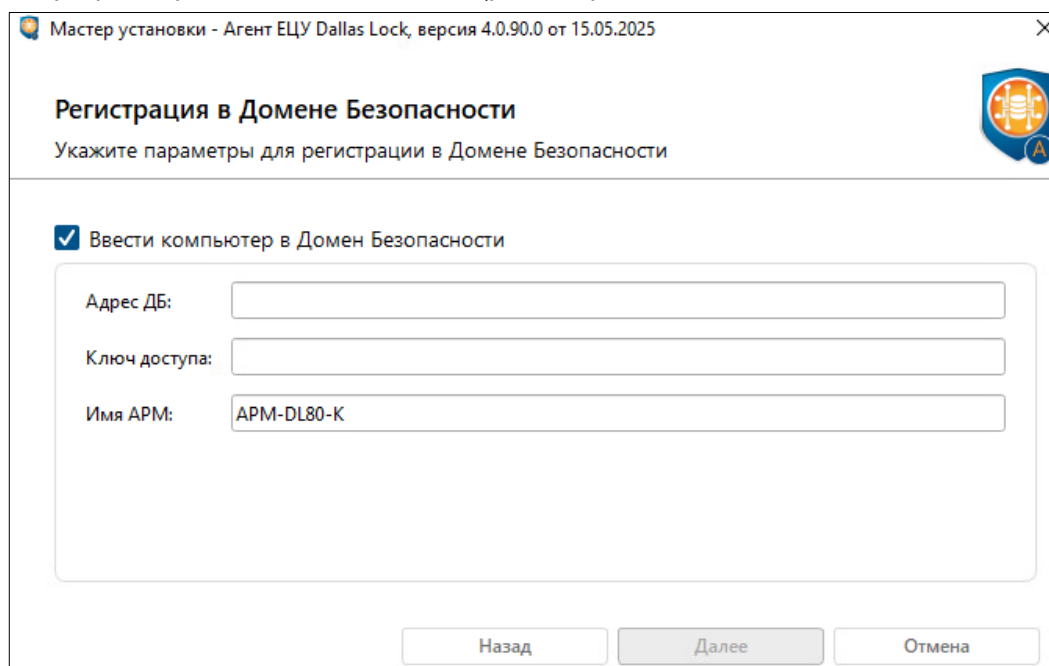


Рис. 297. Регистрация Агента ЕЦУ в ДБ

После нажатия на кнопку **Далее** выполняется проверка введенных для регистрации данных. В случае успешной проверки данных, произойдет переход к следующему шагу.

Чтобы пропустить ввод **Агента ЕЦУ** в ДБ во время установки, нужно нажать на кнопку **Далее**.

3. Затем необходимо выбрать режим работы **Агента ЕЦУ** (рис. 298):

- стандартный режим;
- скрытый режим (позволяет скрыть присутствие Агента на ПК от пользователя).



Сменить режим работы **Агента ЕЦУ** после установки невозможно.

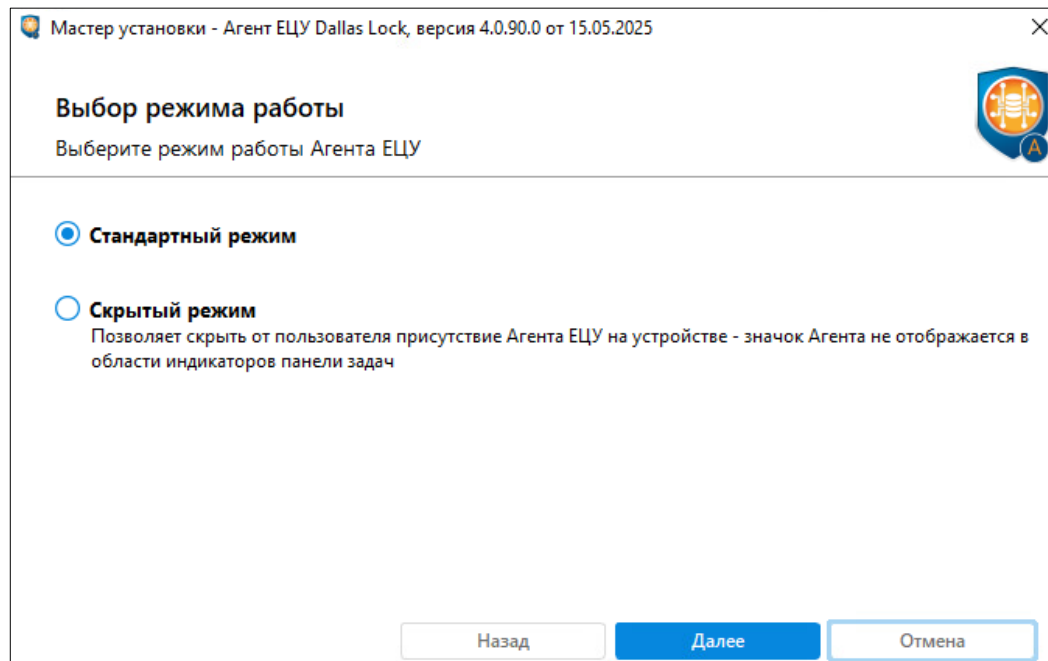


Рис. 298. Выбор режима работы Агента ЕЦУ

Для продолжения установки нажать кнопку **Далее**.

4. Следующим шагом нужно проверить параметры установки (рис. 299) и нажать кнопку **Установить**.

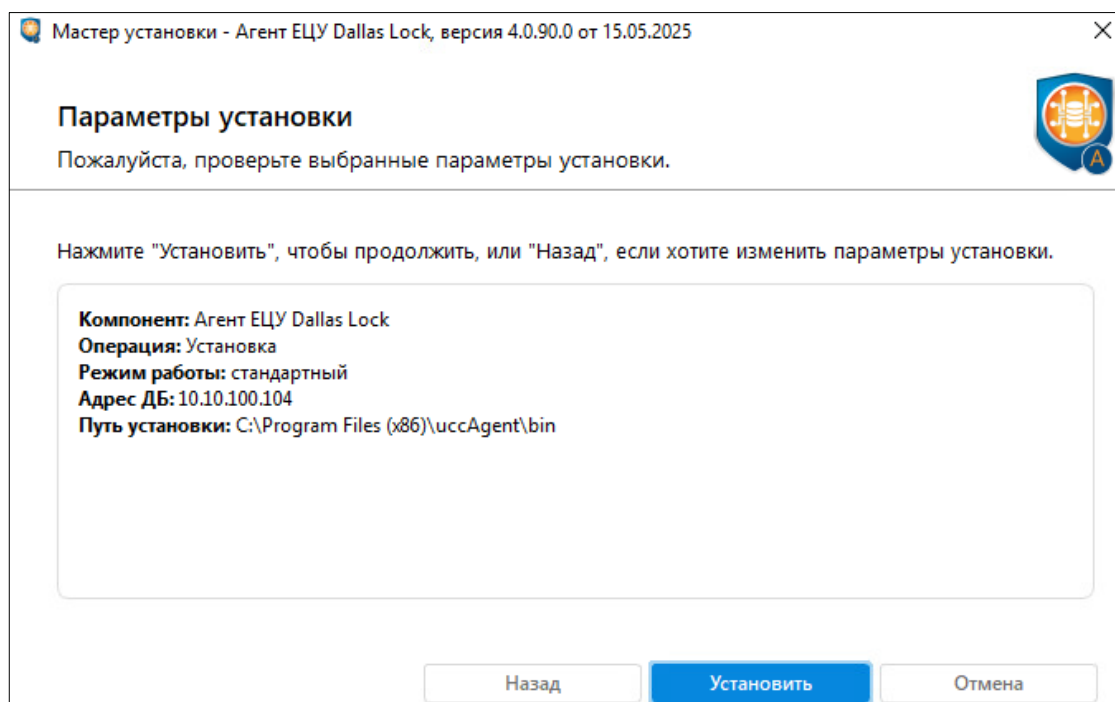


Рис. 299. Проверка параметров установки Агента ЕЦУ

В процессе установки **Агента ЕЦУ Dallas Lock** на ОС Linux выполняться проверка наличия необходимых сторонних пакетов. Для их автоматической установки необходимо нажать чекбокс *Автоматическая установка недостающих пакетов* или установить их самостоятельно:

- для Debian 10.x, Debian 11.x, Debian 12.x, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 24.04 LTS, ROSA FRESH DESKTOP 12:
 - rsyslog
 - gnome-shell-extension-appindicator (требуется только при использовании

- графической оболочки GNOME)
 - для Astra Linux Common Edition (Орел) 2.12, Astra Linux Special Edition (Смоленск) 1.6, Astra Linux Special Edition (Смоленск) 1.7, РЕД ОС 7.3 Муром и РЕД ОС 8:
 - rsyslog
 - для Альт Рабочая Станция 9.x, Альт Рабочая Станция (10.0, 10.1, 10.2), Альт Рабочая Станция К (10.0, 10.1, 10.3), Альт 8 СП Рабочая Станция 10, Альт Сервер 9, Альт Сервер (10.0, 10.1, 10.2) и Альт 8 СП Сервер 10:
 - rsyslog
 - rsyslog-journal
 - clamsmtp (если установлен, рекомендуется обновить до последней версии).
5. Далее возможно наблюдать за процессом установки (рис. 300). Если процесс прошел без ошибок, необходимо нажать кнопку **Далее**, затем **Завершить**.

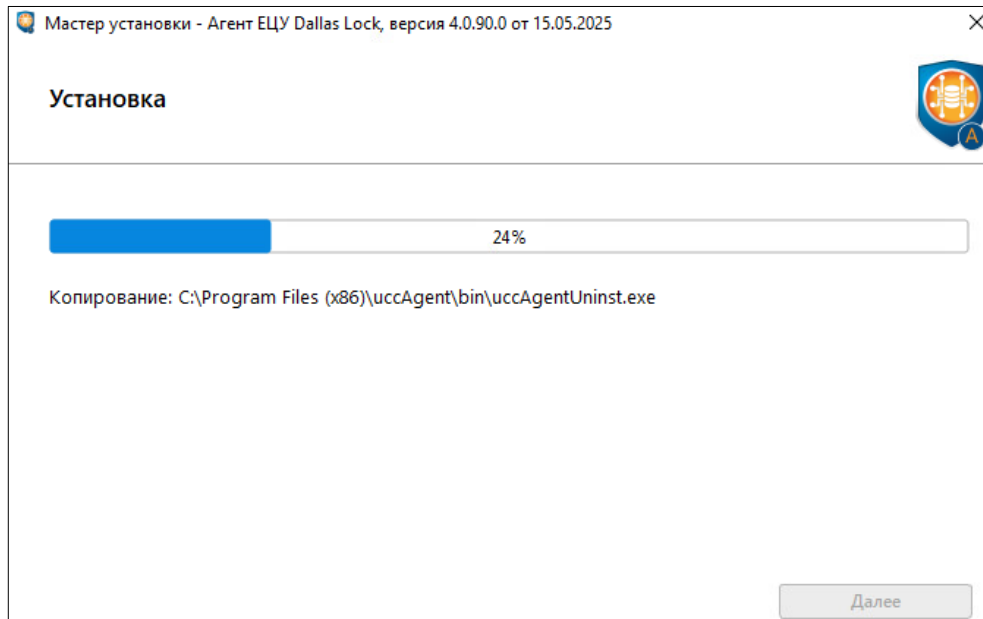


Рис. 300. Процесс установки Агента ЕЦУ



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

После успешного завершения установки **Агента ЕЦУ** на ПК, в дереве ДБ Консоли **ЕЦУ** в группе «Нераспределенные объекты» будет создан новый АРМ, в состав которого включен зарегистрированный модуль **Агент ЕЦУ Dallas Lock** (рис. 301).

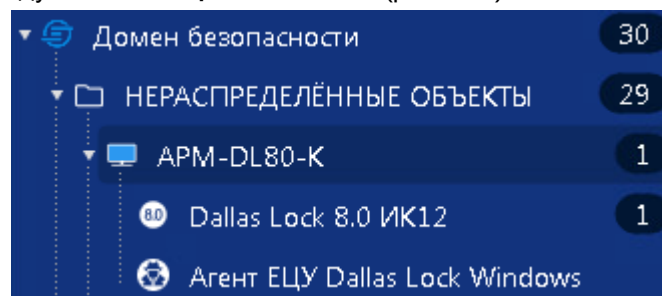


Рис. 301. Отображение Агента ЕЦУ в ДБ

В случае, если введенное имя АРМ уже было в дереве объектов ДБ, и в его составе нет другого модуля **Агент ЕЦУ**, то в данный АРМ **Агент ЕЦУ** будет добавлен как модуль **Агент ЕЦУ Windows** или **Агент ЕЦУ Linux**.



Зарегистрированный в ДБ **Агент ЕЦУ** должен поддерживать связь с сервером **ЕЦУ**. В случае, когда серверов **ЕЦУ** несколько (кластер репликации), Агент **ЕЦУ** должен иметь сетевой доступ хотя бы к одному серверу из списка кластера серверов **ЕЦУ**, который есть в списке серверов репликации у данного модуля.

15.2.2 Консольная установка Агента ЕЦУ

Установка **Агента ЕЦУ** возможна из консоли. В качестве атрибутов к команде `./uccAgentInst` можно указывать следующие (таблица 28):

Таблица 28. Атрибуты установки Агента ЕЦУ

Атрибут	Описание
<code>-install</code>	Установка Агента ЕЦУ из консоли Пример: <code>./uccAgentInst -install <enter></code>
<code>-server-name</code>	Указать имя сервера ЕЦУ для ввода в ДБ
<code>-access-key</code>	Указать ключ Домена безопасности ЕЦУ
<code>-arm-name</code>	Указать имя, с которым агент зайдет в ДБ
<code>-hidden-mode</code>	Выбор скрытого режима
<code>-install-libs</code>	Выбор автоматической установки недостающих пакетов в linux



Для присвоения параметров атрибутам `-server-name`, `-access-key` и `-arm-name` необходимо использование знака равенства.
Пример:
`./uccAgentInst -server-name=serv-us-k1-3 -access-key=password -arm-name=2134 -install`

15.2.3 Установка Агента ЕЦУ Dallas Lock Android

Для установки Агента ЕЦУ на клиентское устройство на базе Android необходимо:

1. Загрузить установочный файл `uccAgentInst.apk`.
2. В открывшемся окне нажать кнопку **Установить**, после чего будет выведена информация об успешном завершении установки.

После завершения процесса установки **Агента ЕЦУ Dallas Lock Android** в списке программ появится ярлык **Агента ЕЦУ Dallas Lock** (рис. 302).



Рис. 302. Ярлык Агента ЕЦУ Dallas Lock Android

При первоначальном открытии приложения будет выведено окно **Ввод в домен безопасности ЕЦУ** (см. [«Регистрация модуля Агент ЕЦУ Dallas Lock Android в ДБ»](#)).

15.2.4 Удаленная установка Агента ЕЦУ Windows

Удаленная установка возможна в следующих вариантах:

- для группы компьютеров, имеющих одинаковые имена и пароли администратора ОС;
- для компьютеров, имеющих индивидуальные имя и пароль администратора ОС, удаленную установку следует выполнять отдельно от других.



По умолчанию в операционных системах начиная с Windows 7 доступ к удаленному компьютеру под локальной учетной записью запрещен. Подробную информацию об этом ограничении можно найти на официальном сайте Справки и поддержки компании Microsoft по адресу <https://support.microsoft.com/kb/951016> (на английском языке).

Если ранее на данный ПК не выполнялось удаленное развертывание **Агента ЕЦУ** или модуля **СЗИ НСД Dallas Lock**, то для разрешения удаленного подключения под локальной учетной записью необходимо в редакторе реестра по пути `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` создать ключ типа `dword` с именем `LocalAccountTokenFilterPolicy` со значением «1» («LocalAccountTokenFilterPolicy»=dword:00000001) и перезагрузить компьютер. В крупных сетях с AD данное значение можно распространить через политики.



По умолчанию удаленная установка выполняется через порт 445. Если ранее на данный ПК не выполнялось удаленное развертывание **Агента ЕЦУ** или модуля **СЗИ НСД Dallas Lock**, то в Брандмауэре Windows данного ПК необходимо открыть порт 445 (создать правило для входящих подключений).



Для нескольких целевых ТС централизованную удаленную установку можно осуществить только при выполнении следующих условий:

- целевые ТС входят в тот же домен AD или LDAP, что и APM с **ЕЦУ Dallas Lock**;
- известны имя пользователя и пароль доменной учетной записи с правами администратора домена.

Для удаленной установки **Агента ЕЦУ** на клиенте для учетной записи администратора должен быть задан пароль. Установку необходимо осуществлять по протоколу IPv4, на момент обновления и установки необходимо отключить протокол IPv6 на APM с консолью **ЕЦУ**. Далее необходимо выполнить следующие шаги:

1. На удаленном APM, на который будет устанавливаться **Агент ЕЦУ** из Консоли управления **ЕЦУ**, должен быть доступен для входящих соединений TCP-порт 135 (ертар).
2. Перед централизованной установкой необходимо разместить на компьютере, на котором запущена Консоль **ЕЦУ**, дистрибутив **Агента ЕЦУ Windows**.
3. Далее необходимо открыть главное меню Консоли **ЕЦУ**  → **Удаленная установка**.

На открывшейся странице необходимо добавить целевые ТС для удаленного развертывания. ТС можно добавить одним из следующих способов, через:

- ручной ввод адреса — для этого нужно заполнить поля *Порт* и *Введите IP-адрес или сетевое имя компьютера*, затем нажать кнопку **Добавить компьютер** (рис. 303);
- файл списка клиентов — нажать **Импорт из файла** и выбрать файл со списком заранее выгруженных клиентов;
- импорт из файла — нажать **Импорт из файла** и прикрепить текстовый файл со списком IP-адресов целевых ТС.



Для файла с IP-адресами возможен только следующий формат списка: в каждой строке файла может быть указан только один IP-адрес без дополнительных символов.

Пример:

```
192.168.0.1
192.168.0.35
10.10.112.55
```

Затем нажать кнопку **Далее**.

1

2

3

4

Мастер удаленной установки Агента ЕЦУ

Список компьютеров

Установка списка компьютеров для подключения

Введите IP адрес или сетевое имя компьютера

10.10.104.124

Добавить компьютер

Порт SSH22

Порт SMB445

IP-адрес	FQDN-имя
10.10.104.124	apm-dl80-k.dl.local

Импорт из файла

Удалить

Назад

Далее

Отмена

Рис. 303. Начало удаленной установки Агента ЕЦУ Windows

4. На следующей странице (рис. 304) необходимо ввести авторизационные данные:
- логин и пароль администратора ОС на целевых ТС;
 - логин и пароль суперпользователя (опционально).

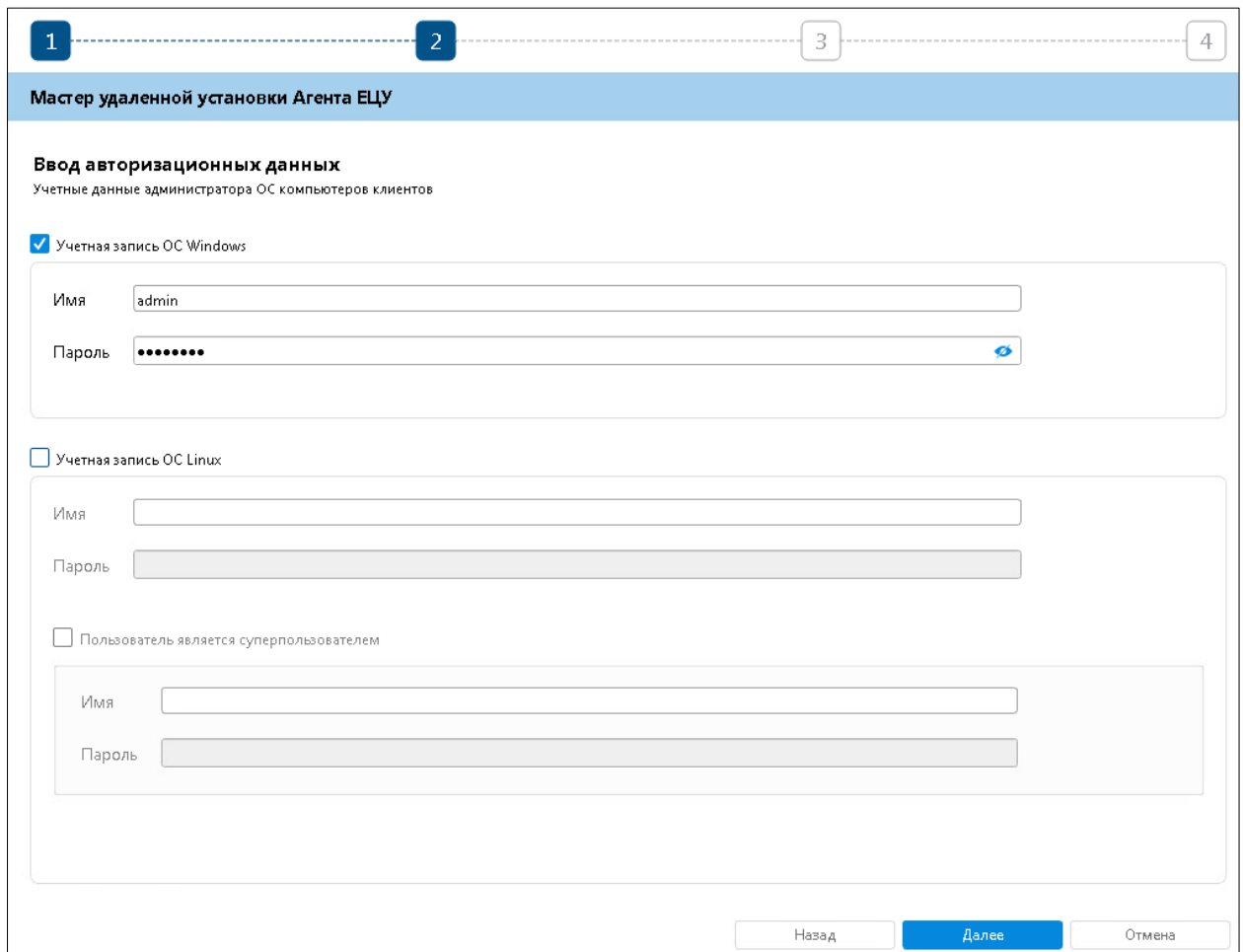


Рис. 304. Ввод авторизационных данных

После введения данных необходимо нажать кнопку **Далее**, будет выполнена проверка подключения к компьютерам. Если при подключении к хостам возникнет ошибка, появится соответствующее предупреждение с предложением продолжить установку, исключив недоступные компьютеры (рис. 305).

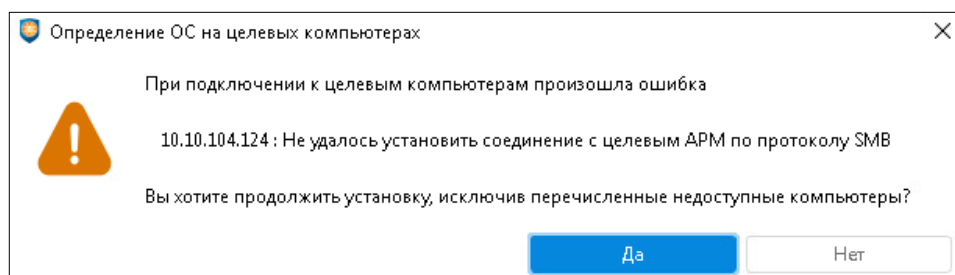


Рис. 305. Ошибка подключения

5. Далее (рис. 306) необходимо указать путь к исходному дистрибутиву **Агента ЕЦУ**.

Для того, чтобы скрыть от пользователя присутствие **Агента ЕЦУ**, можно выбрать скрытый режим установив соответствующий флаг.

Для ввода модулей в Домен безопасности **ЕЦУ Dallas Lock** сразу после установки, можно поставить флаг *Ввод в домен безопасности ЕЦУ*, указать имя сервера **ЕЦУ** и ключ доступа к ДБ **ЕЦУ**.

Затем нажать кнопку **Установить**.



Если указан неверный ключ доступа к ДБ **ЕЦУ**, то дальнейшая установка **Агента ЕЦУ** не будет выполняться.

1
2
3
4

Мастер удаленной установки Агента ЕЦУ

Параметры установки
Выбор установочного файла и параметров установки

Исходные дистрибутивы Выбрать

☐ Скрытый режим i

☐ Ввод в домен безопасности ЕЦУ

Имя сервера UCC-APM2:17900 ▼

Ключ доступа к ДБ

Назад
Установить
Отмена

Рис. 306. Параметры установки Агента ЕЦУ

6. На новой странице (рис. 307) можно наблюдать за процессом установки **Агента ЕЦУ**. По окончании процесса будет выведено сообщение о результате завершения операции.

1
2
3
4

Мастер удаленной установки

Процесс установки

IP-адрес	FQDN-имя	Процесс	Лог
10.10.112.59	ucc-lin-1.dl.local	Установка завершена успешно	Подробнее
10.10.112.135	ucc-lin-3.dl.local	Авторизация суперпользователя	Подробнее
10.10.112.153	ucc-win-10.dl.local	Установка дистрибутива	Подробнее
10.10.112.145	ucc-win-5.dl.local	Установка дистрибутива. Ошибка запуска установочного файла. Программное обеспечение уже было установлено ранее.	Подробнее
10.10.112.146	ucc-win-6.dl.local	Установка дистрибутива. Ошибка запуска установочного файла. Программное обеспечение уже было установлено ранее.	Подробнее

Рис. 307. Процесс установки Агента ЕЦУ

15.2.5 Удаленная установка Агента ЕЦУ Linux

На удаленном АРМ, на который будет устанавливаться **Агент ЕЦУ Linux** из Консоли управления **ЕЦУ**, должен быть доступен для входящих соединений TCP-порт 135 (ермар).

Перед централизованной установкой необходимо разместить на компьютере, на котором запущена Консоль **ЕЦУ**, дистрибутив **Агента ЕЦУ Linux**.

! Для выполнения удаленной установки **Агента ЕЦУ** на хост с операционными системами Альт СП требуется наличие пакета libSM на данных ОС.

Для перехода к процессу установки **Агента ЕЦУ Linux**, необходимо открыть главное меню консоли **ЕЦУ** → **Удаленная установка**.

Следующая последовательность действий для удаленной установки **Агента ЕЦУ Linux** аналогична удаленной установке **Агента ЕЦУ Windows** (см. [«Удаленная установка Агента ЕЦУ Windows»](#)).



Если в процессе установки **Агента ЕЦУ** на Linux возникает ошибка вида: «...error whiel loading shared libraries: libxcb-xkb.so.1: cannot open shared object file: No such file or directory», то необходимо перед установкой вручную установить пакет «libxcb-xkb1».

15.2.6 Удаление Агента ЕЦУ Windows

В ОС Windows необходимо открыть **Пуск** → **Панель управления** → **Программы и компоненты**. В появившемся окне из списка выбрать программу **Агент ЕЦУ Dallas Lock**, нажать **Удалить/Изменить** и подтвердить удаление (рис. 308).

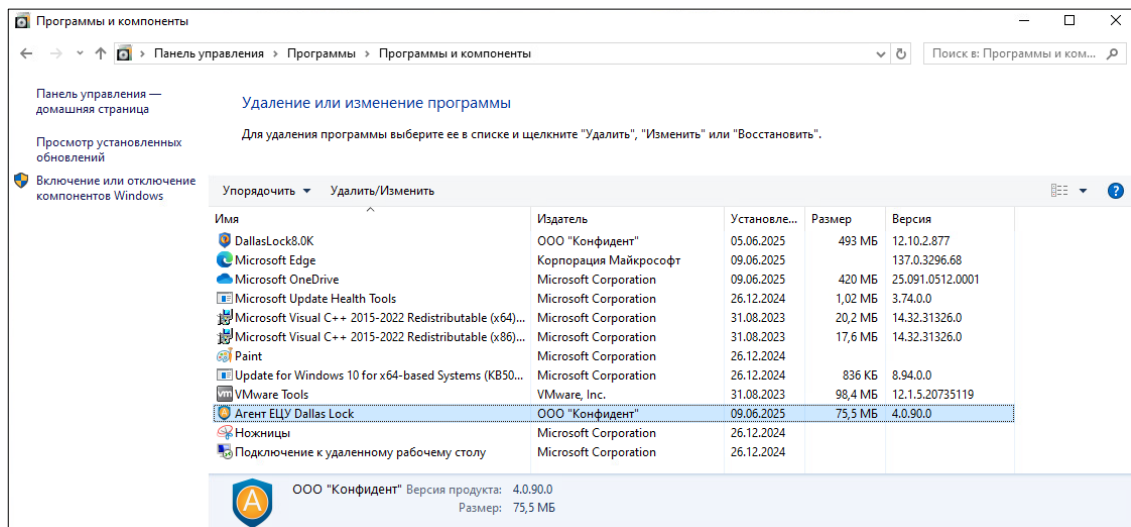


Рис. 308. Удаление Агента ЕЦУ Dallas Lock



Мастер удаления **Агента ЕЦУ** также можно вызвать с помощью запуска установочного дистрибутива.

После подтверждения запустится мастер удаления **Агента ЕЦУ Dallas Lock** (рис. 309). Для продолжения удаления нажать кнопку **Далее**.

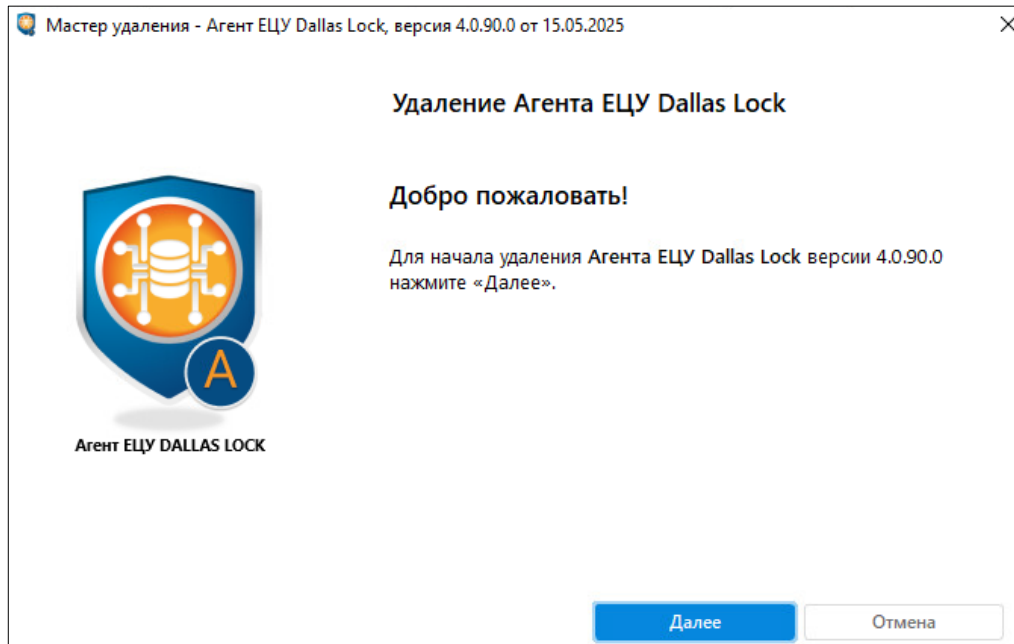


Рис. 309. Окно начала удаления Агента ЕЦУ Dallas Lock

Проверить и подтвердить удаление **Агента ЕЦУ** (рис. 306).

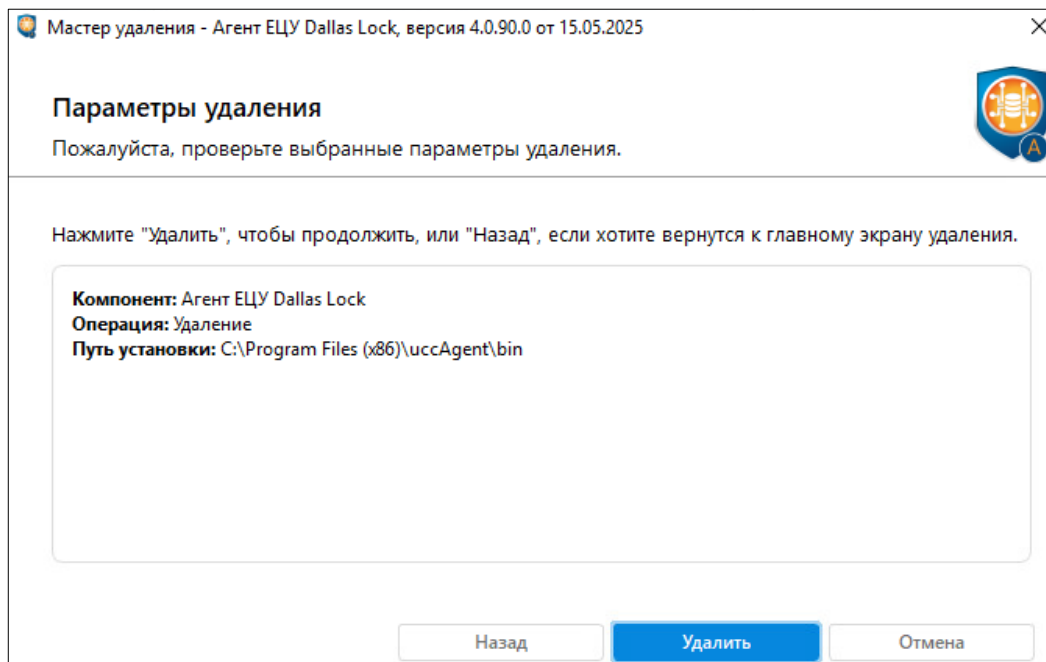


Рис. 310. Параметры удаления

Далее возможно наблюдать за процессом удаления (рис. 311). Если процесс прошел без ошибок, необходимо нажать кнопку **Далее**, затем **Завершить**.

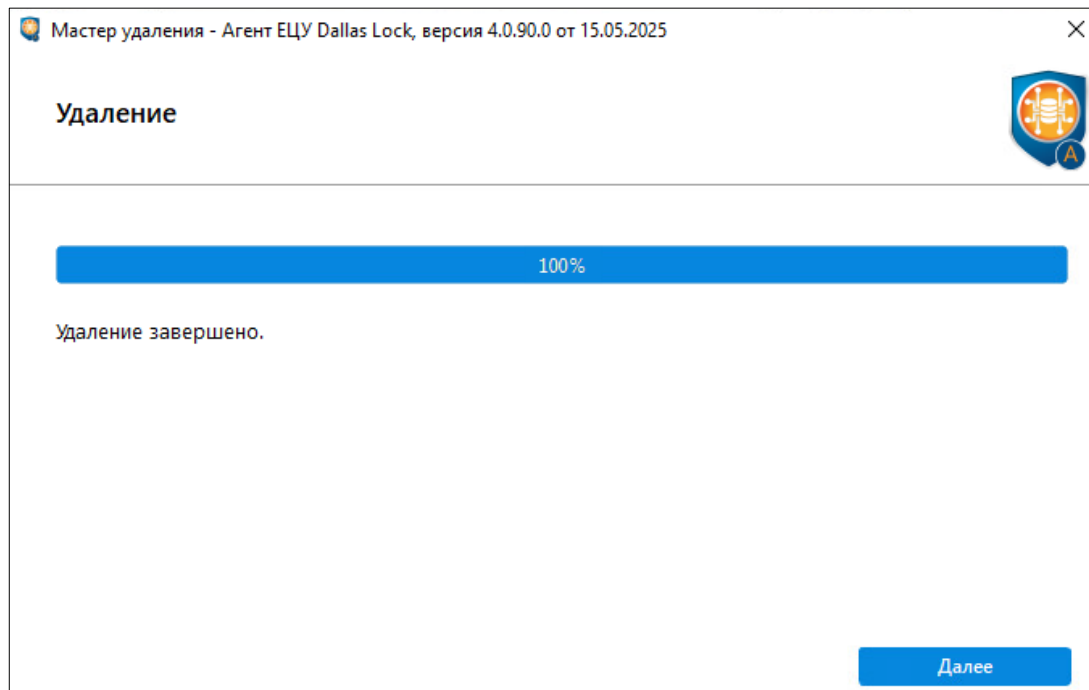


Рис. 311. Процесс удаления Агента ЕЦУ Dallas Lock

15.2.7 Удаление Агента ЕЦУ Linux

Для удаления **Агента ЕЦУ** необходимо обладать правами администратора ОС (root) на данном ПК. Далее необходимо запустить исполняемый файл «*uccAgentUninst*» (путь расположения: */opt/uccAgent/bin/uccAgentUninst*) в терминале. Для этого необходимо выполнить в терминале команду:

```
sudo /opt/uccAgent/bin/uccAgentUninst
```

После выполнения команды запустится окно мастера удаления **Агента ЕЦУ Dallas Lock** (рис. 309). Далее порядок удаления **Агента ЕЦУ Dallas Lock** аналогичен порядку удаления данной программы в ОС семейства Windows (см. [«Удаление Агента ЕЦУ Windows»](#)).

15.2.8 Удаление Агента ЕЦУ Android

Удаление **Агента ЕЦУ Dallas Lock Android** производится силами ОС через настройки приложения.

15.3 Регистрация Агента ЕЦУ в ДБ

Зарегистрировать модуль **Агент ЕЦУ Windows/Linux** в Домене безопасности можно следующими способами:

- во время локальной или удаленной установки **Агента ЕЦУ** (см. [«Локальная установка Агента ЕЦУ»](#));
- путем сканирования сети (см. [«Настройка модуля»](#)).

Ввод **Агента ЕЦУ Dallas Lock Android** в Домен безопасности возможен только со стороны устройства, на котором установлен **Агент ЕЦУ**.

15.3.1 Регистрация модуля Агент ЕЦУ Dallas Lock Android в ДБ



Для успешного ввода модуля **Агент ЕЦУ Dallas Lock Android** в ДБ **Агент ЕЦУ** и **ЕЦУ** должны находиться в одной ЛВС.

Для ввода в Домен безопасности модуля **Агент ЕЦУ Dallas Lock Android** необходимо запустить на устройстве приложение Агент ЕЦУ Dallas Lock, после чего на экране откроется окно **Ввод в домен безопасности ЕЦУ** (рис. 312), в котором требуется указать следующие данные:

- DNS-имя или IP-адреса сервера **ЕЦУ**;
- ключ доступа к ДБ;
- имя устройства, в составе которого необходимо ввести модуль.

Рис. 312. Окно ввода Агента ЕЦУ Dallas Lock Android в ДБ

Для продолжения ввода модуля в ДБ нажать кнопку **Отправка запроса**.

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

После успешного завершения установки **Агента ЕЦУ** на ПК, в дереве ДБ Консоли **ЕЦУ** в группе «Нераспределенные объекты» будет создан новый АРМ, в состав которого включен зарегистрированный модуль **Агент ЕЦУ Dallas Lock** (рис. 313).

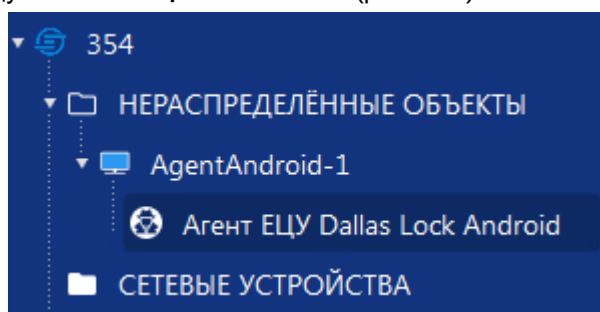


Рис. 313. Отображение Агента ЕЦУ в ДБ

Если у приложения нет соответствующего разрешения, то в окне результата ввода модуля в ДБ будет отображен статус Разрешение на уведомление не предоставлено. Предоставить данное разрешение можно следующими способами:

- из свойств приложения средствами ОС;
- нажатием кнопки **Запросить разрешение** из интерфейса **Агента ЕЦУ**.



При нажатии кнопки **Запросить разрешение** будет выведено окно подтверждения с соответствующим сообщением и кнопками **Разрешить** и **Запретить**:

- при нажатии **Разрешить** будет выведено сообщение «Разрешение предоставлено», статус Разрешение на уведомление не предоставлено и кнопка **Запросить разрешение** исчезнут с экрана, в уведомлениях устройства отобразится уведомление о статусе соединения с **ЕЦУ**;
- при нажатии **Запретить** будет выведено сообщение «Разрешение не предоставлено».

Если в процессе ввода Агента ЕЦУ возникла ошибка, на экране устройства будет выведено сообщение об ошибке с соответствующим описанием.

Вывод **Агента ЕЦУ Dallas Lock Android** возможен следующими способами:

- при очистке хранилища приложения на клиентском устройстве;
- при удалении приложения Агент ЕЦУ Dallas Lock с устройства пользователя;
- при инициировании на **ЕЦУ** команды *Удалить* на панели *Действия* или в контекстном меню дерева объектов ДБ.



Если вывод из ДБ **ЕЦУ** производится со стороны **Агента ЕЦУ** (клиентского устройства), то АРМ будет отражаться в дереве ДБ после удаления, но будет недоступен. Повторный ввод АРМ с таким же названием недоступен, предварительно необходимо удалить АРМ из дерева ДБ.

15.4 Настройка модуля Агент ЕЦУ Windows/Linux

В Консоли **ЕЦУ** в дереве ДБ **Агенты ЕЦУ** отображаются как отдельные модули **Агент ЕЦУ Dallas Lock Windows** или **Агент ЕЦУ Dallas Lock Linux** в составе АРМ. Значки Агента **ЕЦУ** зависят от состояния модуля и могут принимать следующий вид:



— модуль подключен;



— модуль не подключен.



Для корректной работы функции удаленного управления с помощью **Агента ЕЦУ** необходимо на АРМ с Linux отключить протокол *Wayland*.

15.4.1 Сводка модуля Агент ЕЦУ

Вкладка *Сводка* (рис. 314) отображает общее состояние рабочей станции, на которую установлен Агент ЕЦУ.

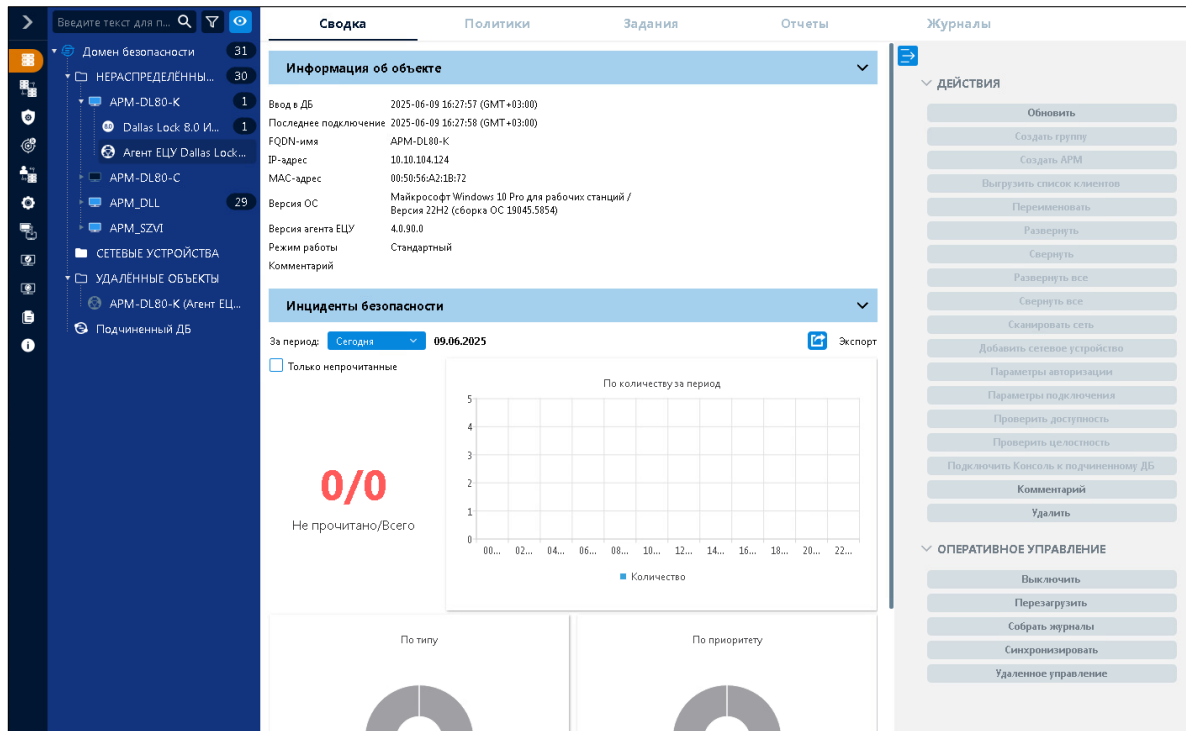


Рис. 314. Вкладка «Сводка» модуля Агент ЕЦУ

Доступны следующие разделы информационной панели.

Информация об объекте
В верхней части информационной панели отображается следующая информация о текущем состоянии модуля: • информация о дате и времени ввода в ДБ; • информация о дате и времени последнего подключения; • FQDN-имя; • IP-адрес; • MAC-адрес; • версия ОС; • версия Агента ЕЦУ; • режим работы; • комментарий.
Инциденты безопасности
Отображается список инцидентов безопасности с графической панелью. Доступна фильтрация отображаемых событий по периоду и настройка отображения диаграмм (см. «Настройка инцидентов безопасности»). Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное. Поле <i>Комментарий</i> доступно для редактирования.

На панели инструментов вкладки *Сводка* (рис. 314) доступны следующие действия:

- «Обновить» — позволяет обновить информацию на вкладке *Сводка*;
- «Удалить» — перемещает в базовую группу «Удаленные объекты» с сохранением журналов;
- «Комментарий» — добавленный комментарий отобразится в разделе *Информация об объекте* вкладки *Сводка*.

Для модуля **Агент ЕЦУ** доступны следующие команды оперативного управления (рис. 314) на панели инструментов:

- «Выключить»;
- «Перезагрузить»;
- «Собрать журналы»;
- «Синхронизировать»;
- «Удаленное управление».



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

15.4.2 Сбор журналов Агента ЕЦУ

Для получения в **ЕЦУ Dallas Lock** записей журналов, ведущихся на ТС, где установлен **Агент ЕЦУ**, необходимо проведение сбора журналов. Сбор журналов может быть проведен при условии наличия сетевого подключения между **ЕЦУ** и ТС с установленным Агентом:

- периодически (см. [«Параметры работы модулей»](#));
- по команде пользователя из Консоли **ЕЦУ**.

Команда **Собрать журналы** в Консоли **ЕЦУ** для модуля **Агент ЕЦУ** доступна на вкладке *Сводка* на панели инструментов *Оперативное управление* (рис. 314).

15.4.3 Подключение к удаленному рабочему столу

Для подключения к удаленному рабочему столу ТС, необходимо:

1. Выбрать нужный модуль **Агент ЕЦУ** в дереве ДБ.
2. На панели инструментов в разделе *Оперативное управление* выбрать пункт **Удаленное управление** (рис. 314).
3. На АРМ, где установлен **Агент ЕЦУ**, появится окно (рис. 315), в котором пользователю необходимо выбрать действие с помощью кнопок:
 - кнопка **Подключить сейчас** позволяет начать сеанс удаленного подключения;
 - кнопка **Отклонить** позволяет отклонить запрос на сеанс удаленного подключения;
 - кнопка **Закрыть** (X) позволяет отклонить запрос на сеанс удаленного подключения (работает аналогично кнопке **Отклонить**).

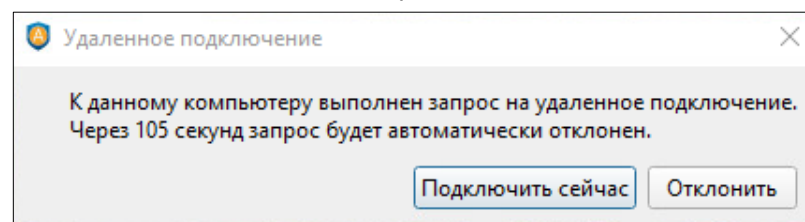


Рис. 315. Окно удаленного подключения на стороне АРМ с Агентом ЕЦУ

Если со стороны АРМ, к которому выполняется запрос на сеанс удаленного подключения, не производится никаких действий, то запрос на удаленное подключение будет прерван по истечении времени, установленного политикой **Время ожидания подключения по VNC (секунд)**.

Если подключение возможно, то на экране отобразится запущенная сессия на выбранном ТС. В ином случае появится сообщение об ошибке (рис. 316).

Для того чтобы снять блокировку экрана при подключении по VNC, необходимо нажать сочетание клавиш **Win+Del**.

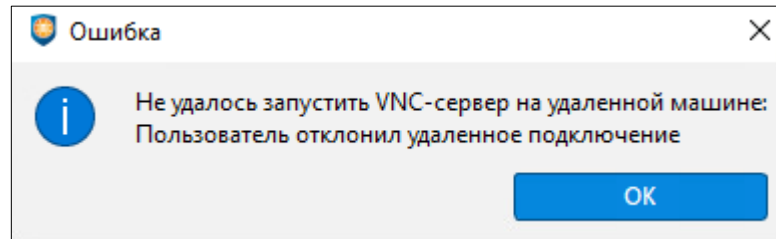


Рис. 316. Ошибка удаленного подключения

Если Сервер **ЕЦУ** и КУ **ЕЦУ** развернуты на ОС Windows, то:

- при подключении по VNC к ОС с установленным **Агент ЕЦУ** Linux происходит блокировка работы "горячих" клавиш (**Ctrl+Alt+T**) — открыть терминал невозможно;
- при подключении по VNC к ОС с установленным **Агент ЕЦУ** Linux (Astra-Брест, Орел, Смоленск) и использовании "горячих" клавиш (**Win+T** — для открытия терминала) — последующая работа в терминале блокирована;
- при подключении по VNC к ОС с установленным **Агент ЕЦУ** Windows и открытии окна **Выполнить** (**Win+R**) — ввод команд на исполнение в поле *Открыть* блокировано.



События, связанные с удаленным подключением к ТС, фиксируются в журнале *Журнал ЕЦУ* (ошибки подключения, начало и завершение удаленного подключения).



Одновременное подключение к ТС с установленным **Агентом ЕЦУ** возможно только с одной Консоли **ЕЦУ**.



При инициировании подключения по VNC консоль **ЕЦУ** блокируется до момента подключения/отказа в подключении.



Подключение к ТС (с установленным **Агентом ЕЦУ**), расположенным за NAT, по протоколу VNC не поддерживается.

15.4.4 Политики модуля Агент ЕЦУ

На уровне модуля **Агент ЕЦУ** в списке на вкладке *Политики* (рис. 317) доступны только политики, актуальные для модуля **Агент ЕЦУ** (см. [«Политики ДБ»](#)).

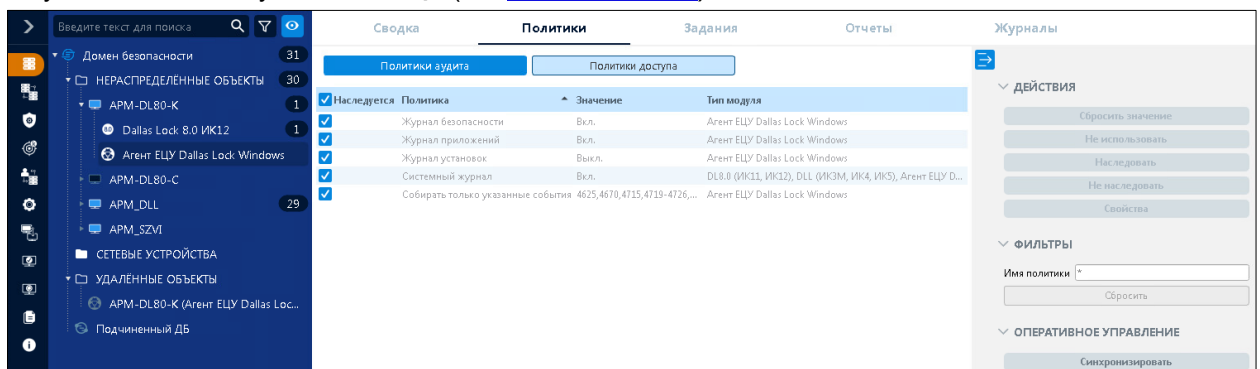


Рис. 317. Вкладка «Политики» модуля Агент ЕЦУ

Настройка политик для модуля производится аналогично настройке политик для группы ДБ (см. [«Политики для группы ДБ»](#)). Для применения параметров на модулях необходима синхронизация.

15.4.5 Задания модуля Агент ЕЦУ

На уровне модуля **Агент ЕЦУ** в списке на вкладке *Задания* доступны для создания только задания, актуальные для **Агента ЕЦУ** (рис. 318):

- отчет об аппаратном обеспечении;
- удаление **Агента ЕЦУ**;
- отчет о программном обеспечении.

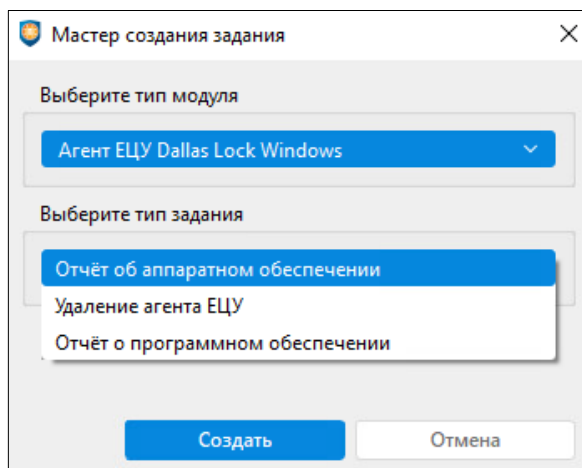


Рис. 318. Мастер создания задания для модуля **Агент ЕЦУ Windows**



Типы заданий одинаковые для модулей **Агент ЕЦУ Linux** и **Агент ЕЦУ Windows**.

Работа с заданиями для модуля **Агент ЕЦУ** производится аналогично настройке заданий для ДБ (см. [«Задания ДБ»](#)).

Для выполнения задания требуется синхронизация с модулем.

15.4.6 Отчеты модуля Агент ЕЦУ

На уровне модуля **Агент ЕЦУ** на вкладке *Отчеты* (рис. 319) доступны следующие отчеты модуля:

- отчет об аппаратном обеспечении (содержит информацию о материнской плате, BIOS, процессорах, оперативной памяти, PCI-устройствах и о накопителях);
- отчет о программном обеспечении (содержит информацию обо всех установленных программах (для модулей **Агент ЕЦУ Windows**) или пакетах (для модулей **Агент ЕЦУ Linux**)).

Первые полученные для **Агента ЕЦУ** (отчеты об аппаратном обеспечении и ПО) становятся эталонными. Следующие получаемые отчеты сравниваются с эталонным. Первый отчет будет получен **ЕЦУ Dallas Lock** сразу после процесса регистрации модуля **Агент ЕЦУ** в ДБ.

Над таблицей есть поле *Показать только отличия*, установка флага напротив этого поля приводит к переходу в режим отображения отличия отчета, текущего от эталонного. Снятие флага возвращает к просмотру всех параметров.

На панели инструментов *Действия* вкладки *Отчеты* доступны следующие команды по работе с отчетами модуля **Агент ЕЦУ**:

- «Обновить» (получить текущий отчет с модуля и сравнить с эталоном);
- «Применить изменения» (сделать текущий отчет эталонным);
- «Сохранить в файл» (позволяет сохранить текущий отчет в текстовом формате).

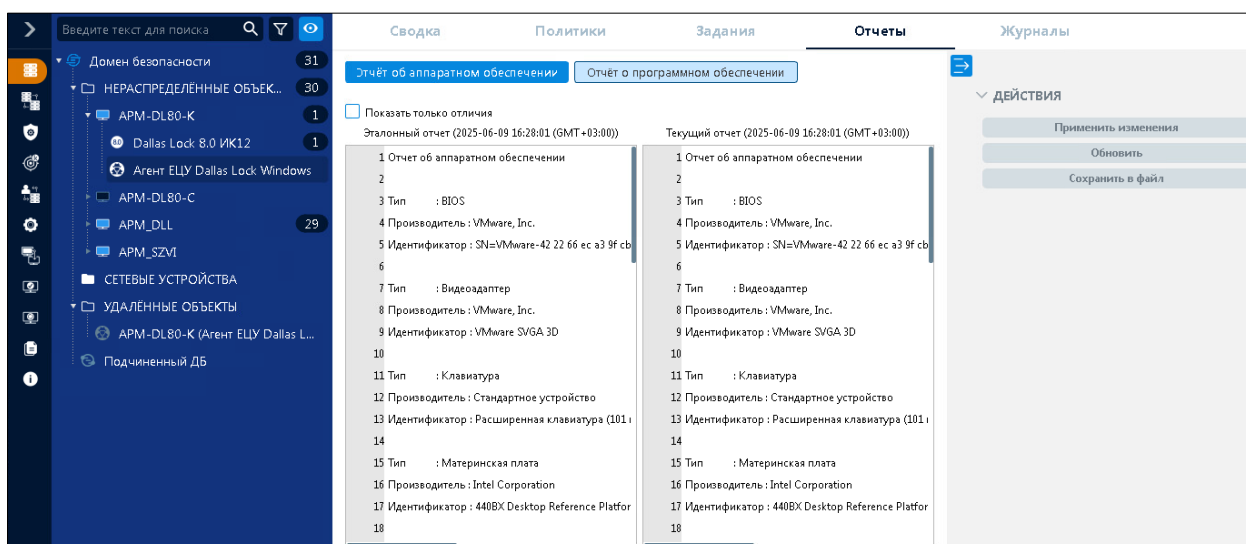


Рис. 319. Отчеты модуля Агент ЕЦУ



Периодическое сравнение отчетов можно настроить в разделе [«Параметры работы модулей»](#).

Полученный текущий отчет от **Агента ЕЦУ** сравнивается с эталонным. Результат сравнения отображается в рабочей области вкладки *Отчеты*.

Если полученный отчет отличается от эталонного, то происходит нарушение целостности. В таком случае появляется уведомление об инциденте безопасности, а отличия в отчете будут выделены цветом.

При выборе на панели инструментов *Действия* команды **Сохранить в файл**, открывается окно **Сохранить отчет об аппаратном обеспечении** или **Сохранить отчет о программном обеспечении**, соответственно.

В окне необходимо указать путь для сохранения, и задать имя файла (по необходимости, заполнить информацию о подразделениях и автоматизированной системе).

В шапке отчета дополнительно будет зафиксирована информация о пользователе, инициировавшем составление отчета, дата составления отчета и имя компьютера.

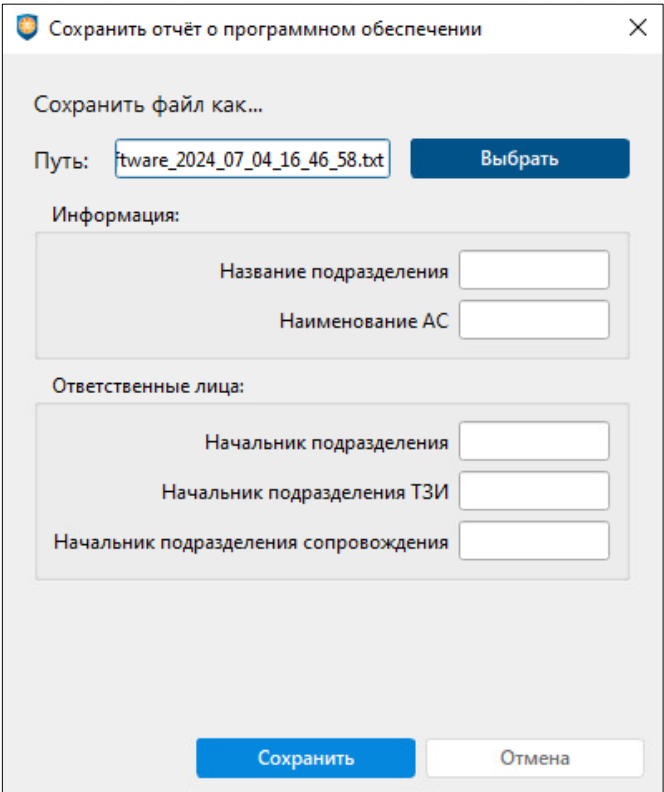


Рис. 320. Команда «Сохранить в файл»

15.4.7 Журналы Агента ЕЦУ

Вкладка *Журналы* для **Агента ЕЦУ** позволяет просматривать журналы безопасности модуля. Для модуля **Агент ЕЦУ Windows** (рис. 321) доступны:

- «Системный журнал»;
- «Журнал приложений»;
- «Журнал безопасности»;
- «Журнал установок».

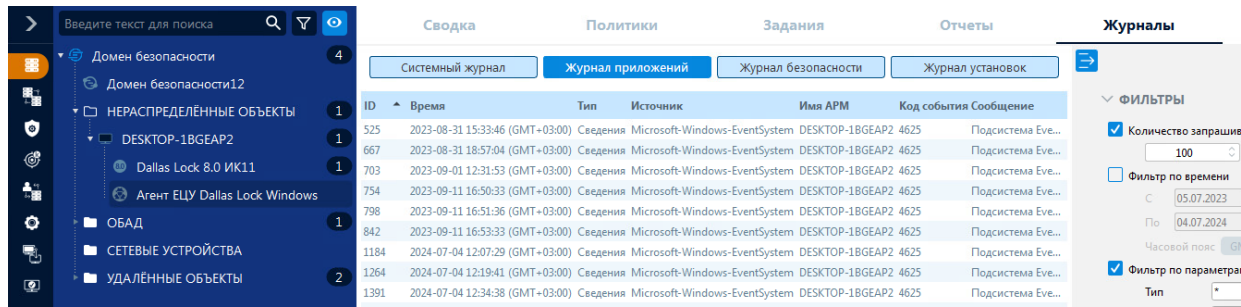


Рис. 321. Журналы Агента ЕЦУ Windows

Для модуля **Агент ЕЦУ Linux** (рис. 322) доступны:

- «Системный журнал»;
- «Журнал аутентификации»;
- «Журнал пользовательских сообщений»;
- «Журнал печати»;

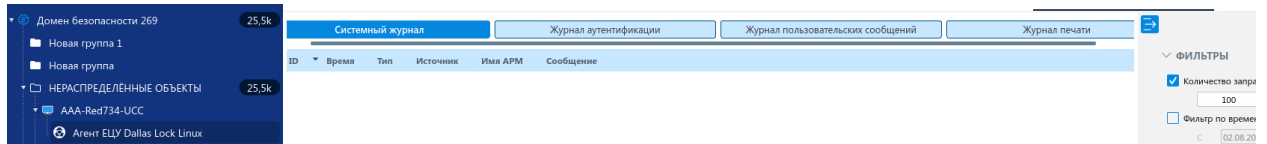


Рис. 322. Журналы Агента ЕЦУ Linux

Работа с журналами модулей описана в разделе [«Журналы модуля»](#).

Для получения записей журналов с модуля требуется выполнение сбора журналов.

15.5 Настройка модуля Агент ЕЦУ Android

В Консоли **ЕЦУ** в дереве ДБ **Агент ЕЦУ** отображаются как модули **Агент ЕЦУ Dallas Lock Android** в составе АРМ. Значки **Агента ЕЦУ** зависят от состояния модуля и могут принимать следующий вид:



— модуль подключен;



— модуль не подключен.

15.5.1 Сводка модуля Агент ЕЦУ

Вкладка **Сводка** (рис. 323) отображает общее состояние рабочей станции, на которую установлен **Агент ЕЦУ**.

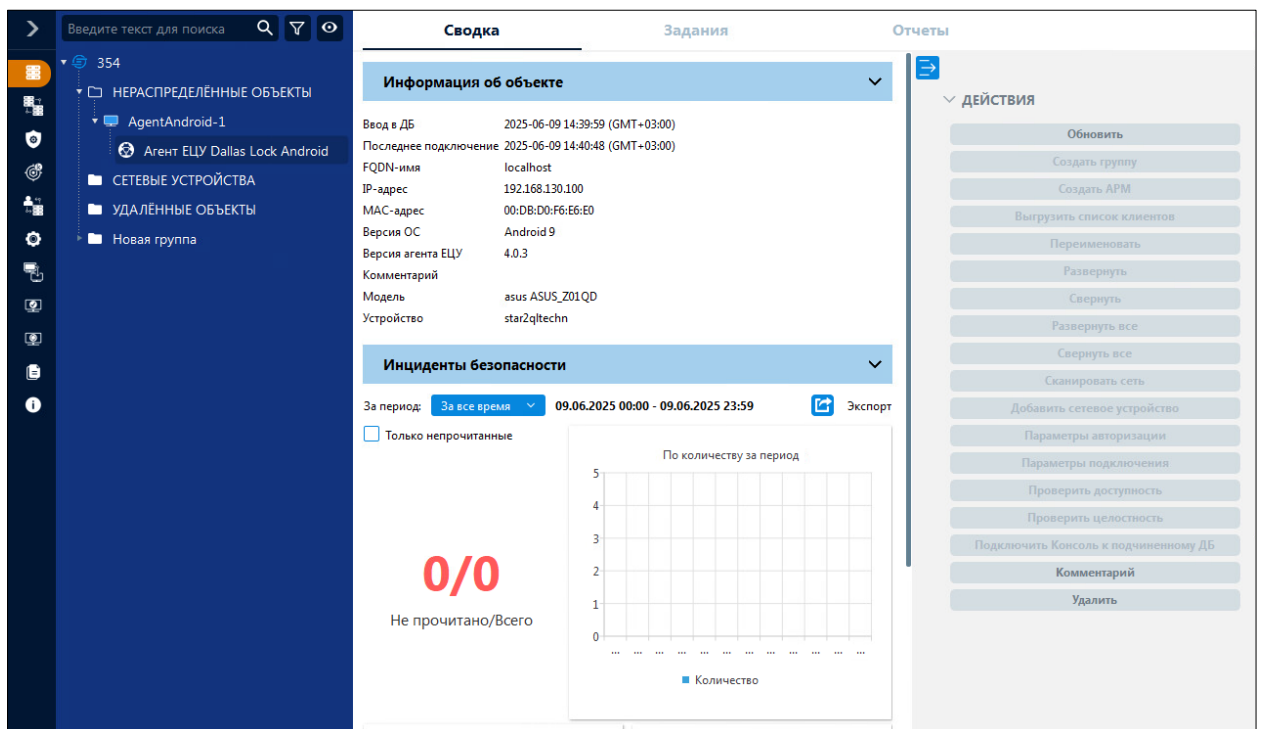


Рис. 323. Вкладка «Сводка» модуля Агент ЕЦУ

Доступны следующие разделы информационной панели.

Информация об объекте

В верхней части информационной панели отображается следующая информация о текущем состоянии модуля:

- информация о дате и времени ввода в ДБ;
- информация о дате и времени последнего подключения;
- FQDN-имя;

- IP-адрес;
- MAC-адрес;
- версия ОС;
- версия **Агента ЕЦУ**;
- комментарий;
- модель устройства;
- общее название аппаратного устройства, обозначающее серийное семейство / тип устройства.

Инциденты безопасности

Отображается список инцидентов безопасности с графической панелью. Доступна фильтрация отображаемых событий по периоду и настройка отображения диаграмм (см. [«Настройка инцидентов безопасности»](#)).

Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное. Поле *Комментарий* доступно для редактирования.

На панели инструментов вкладки *Сводка* (рис. 323) доступны следующие действия:

- «Обновить» — позволяет обновить информацию на вкладке *Сводка*;



Информация на вкладке *Сводка* также обновляется при каждом подключении **Агента ЕЦУ Dallas Lock Android** к ДБ ЕЦУ.

- «Удалить» — перемещает в базовую группу «Удаленные объекты»;
- «Комментарий» — добавленный комментарий отобразится в разделе *Информация об объекте* вкладки *Сводка*.

15.5.2 Задания модуля Агент ЕЦУ

На уровне модуля **Агент ЕЦУ** в списке на вкладке *Задания* доступны для создания только задания, актуальные для **Агента ЕЦУ** (рис. 324):

- Информация об устройстве — задание на создание отчета об аппаратной части устройства, которое включает в себя данные о процессоре, сетевом адаптере, памяти, аккумуляторе и экране;
- Отчет о программном обеспечении — задание на создание отчета об установленных на устройстве приложениях.

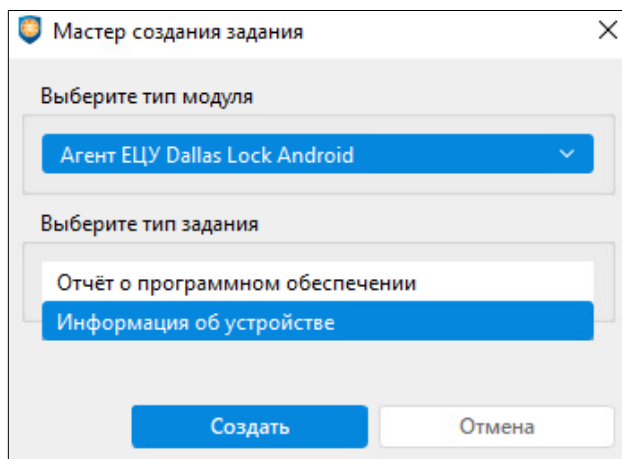


Рис. 324. Мастер создания задания для модуля Агент ЕЦУ Dallas Lock Android

Работа с заданиями для модуля **Агент ЕЦУ** производится аналогично настройке заданий для ДБ (см. [«Задания ДБ»](#)).

15.5.3 Отчеты модуля Агент ЕЦУ

На уровне модуля **Агент ЕЦУ** на вкладке *Отчеты* (рис. 325) доступны следующие отчеты модуля:

- информация об устройстве (содержит информацию об аппаратной части устройства, которая включает в себя данные о процессоре, сетевом адаптере, памяти, аккумуляторе и экране);



Отчет **Информация об устройстве** может не содержать сведений о компонентах, доступ к которым ограничен или отсутствует.

- отчет о программном обеспечении (содержит информацию об установленных на устройство приложениях).



Для отображения данных об объеме установленного ПО в отчете **Отчет о программном обеспечении** необходимо выдать разрешение **Агенту ЕЦУ** в настройках ОС.

Первые полученные для **Агента ЕЦУ** (отчеты об аппаратном обеспечении и ПО) становятся эталонными. Следующие получаемые отчеты сравниваются с эталонным. Первый отчет будет получен **ЕЦУ Dallas Lock** сразу после процесса регистрации модуля **Агент ЕЦУ** в ДБ.

Над таблицей есть поле *Показать только отличия*, установка флага напротив этого поля приводит к переходу в режим отображения отличия отчета, текущего от эталонного. Снятие флага возвращает к просмотру всех параметров.

На панели инструментов *Действия* вкладки *Отчеты* доступны следующие команды по работе с отчетами модуля **Агент ЕЦУ**:

- «Обновить» (получить текущий отчет с модуля и сравнить с эталоном);
- «Применить изменения» (сделать текущий отчет эталонным);
- «Сохранить в файл» (позволяет сохранить текущий отчет в текстовом формате).

Рис. 325. Отчеты модуля Агент ЕЦУ



Периодическое сравнение отчетов можно настроить в разделе [«Параметры работы модулей»](#).

Полученный текущий отчет от **Агента ЕЦУ** сравнивается с эталонным. Результат сравнения отображается в рабочей области вкладки *Отчеты*.

Если полученный отчет отличается от эталонного, то происходит нарушение целостности. В таком случае появляется уведомление об инциденте безопасности, а отличия в отчете будут выделены цветом.

При выборе на панели инструментов *Действия* команды **Сохранить в файл**, открывается окно сохранения отчета, в котором необходимо указать путь для сохранения, и задать имя файла (по необходимости, заполнить информацию о подразделениях и автоматизированной системе).

В шапке отчета дополнительно будет зафиксирована информация о пользователе, инициировавшем составление отчета, дата составления отчета, имя компьютера, способ создания отчета, версия **Агента ЕЦУ** и операционная система.

Сохранить отчет о программном обеспечении

Сохранить файл как...

Путь:

Информация:

Название подразделения

Наименование АС

Ответственные лица:

Начальник подразделения

Начальник подразделения ТЗИ

Начальник подразделения сопровождения

Рис. 326. Команда «Сохранить в файл»

16 KASPERSKY SECURITY CENTER

16.1 Настройка Kaspersky Security Center

Для настройки параметров Kaspersky, необходимо в главном меню консоли **ЕЦУ** выбрать пункт **Настройка KSC**. При нажатии, откроется страница **Настройка Kaspersky Security Center** (рис. 327).

Рис. 327. Страница Настройки Kaspersky Security Center

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

16.2 Подключение к Kaspersky Security Center

Для подключения к KSC необходимо открыть главное меню Консоли **ЕЦУ** и выбрать пункт → **Настройка KSC**.

В блоке *Подключение к Kaspersky Security Center* (рис. 328) нажать кнопку **Добавит новый KSC**, в открывшемся окне указать:

- сервер KSC (формат ввода *<адрес>:<порт>*. В качестве адреса можно указать DNS-имя, NetBIOS-имя, либо IP-адрес);
- имя администратора KSC;
- пароль.

Нажать кнопку **Подключение** для подтверждения подключения к KSC. Для отмены подключения нажать **Отмена**.

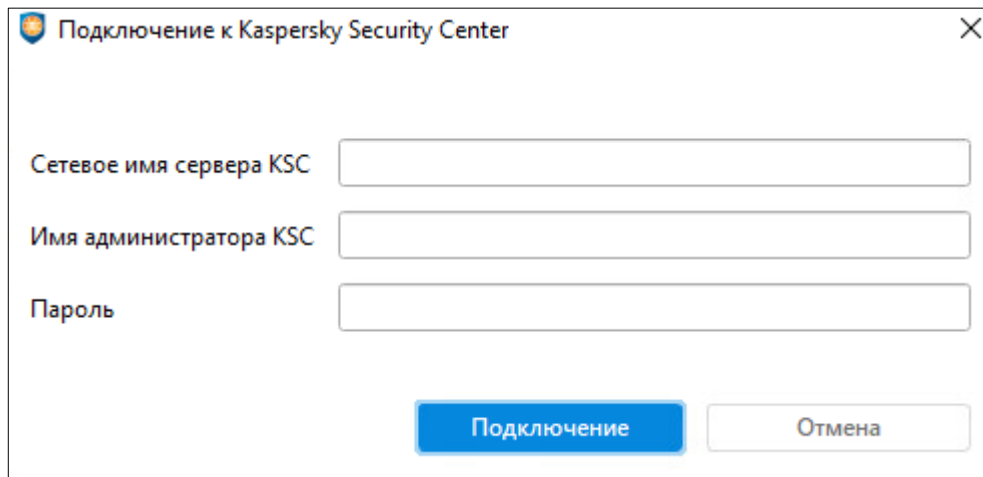


Рис. 328. Подключение к Kaspersky Security Center

Если подключение прошло успешно — в следующем окне (рис. 329) отобразится базовая информация о сервере KSC.

Установка флага *Автоматический ввод в ДБ новых клиентов KES* — позволяет зарегистрировать всех клиентов KES, входящих в состав подключаемого сервера KSC, в Домене **ЕЦУ Dallas Lock**. После редактирования параметров нажать кнопку **Ввести в ДБ**.

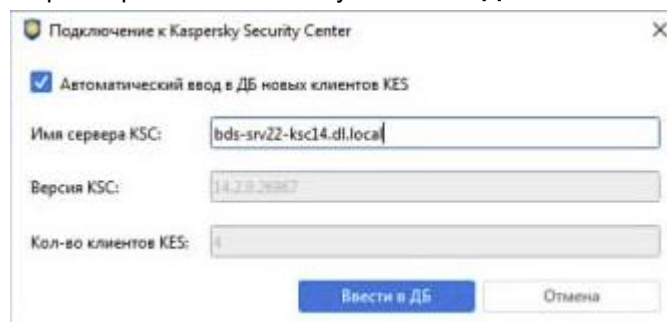


Рис. 329. Подключение к Kaspersky Security Center

В Консоли **ЕЦУ** в корне дерева Домена безопасности появится запись с соответствующим именем сервера KSC (рис. 330).

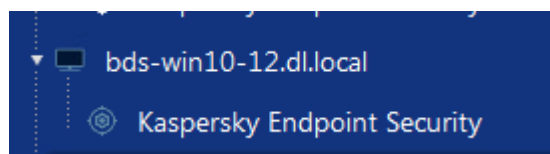


Рис. 330. KSC в дереве Домена безопасности

Клиенты KES в дереве Домена безопасности отображаются как отдельные модули в составе АРМ (рис. 331). Для регистрации в ДБ **ЕЦУ** незарегистрированных клиентов KES или удаления зарегистрированных модулей KES, необходимо установить/снять флаг в столбце *Состояние* (см. [«Клиенты Kaspersky Security Center»](#)). Все изменения отображаются в дереве Домена безопасности.

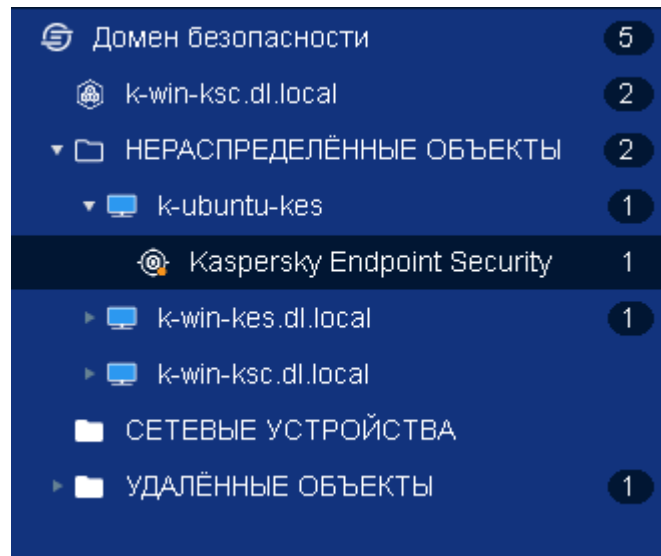


Рис. 331. KES в дереве Домена безопасности



Для регистрации в ДБ **ЕЦУ** клиентов KES, входящих в состав подключаемого сервера KSC, необходимо наличие установленного на регистрируемых АРМ ПО «Агент администрирования KSC».

16.3 Отключение Kaspersky Security Center

Вывести сервер KSC и входящие в него модули KES из Домена безопасности **ЕЦУ Dallas Lock** можно следующими способами:

- на вкладке **Сводка** выбрать действие **Удалить**;
- открыть контекстное меню в дереве объектов для данного узла, выбрать **Удалить**.

При выборе действия **Удалить** появится окно с предупреждением (рис. 332). Если подтвердить удаление — сервер KSC и модули KES будут перемещены в базовую группу Домена безопасности «Удаленные объекты».

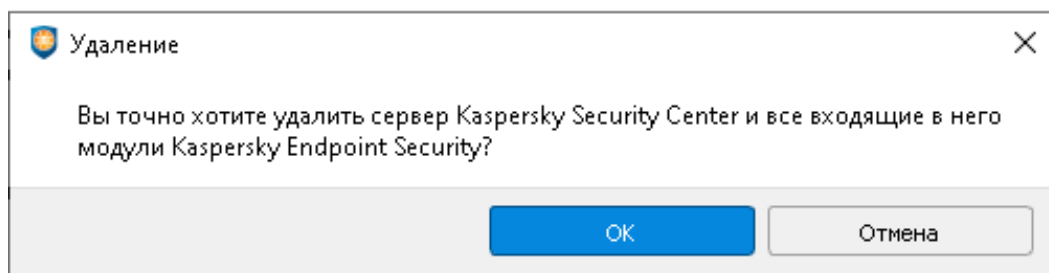


Рис. 332. Отключение Kaspersky Security Center

16.4 Настройка Kaspersky Security Center

В корне дерева Домена безопасности **ЕЦУ Dallas Lock** отображается подключение к серверу KSC. Значки подключенного сервера KSC, зависят от состояния и могут принимать следующий вид:



— сервер подключен;



— сервер не подключен.

16.4.1 Синхронизация

Для отправки на **ЕЦУ Dallas Lock** сведений о сервере KSC и приведения в соответствие системного времени необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между **ЕЦУ Dallas Lock** и сервером KSC:

- периодически (см. [«Настройка Kaspersky Security Center»](#));
- по команде пользователя из Консоли **ЕЦУ**.

Команда **Синхронизировать** в Консоли **ЕЦУ** для сервера KSC доступна на вкладке *Сводка* на панели инструментов *Оперативное управление* (рис. 333).

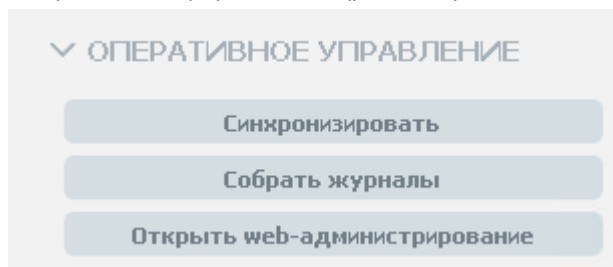


Рис. 333. Оперативное управление

16.4.2 Сбор журналов

Для получения в **ЕЦУ Dallas Lock** записей журналов, ведущихся на сервере KSC, необходимо проведение сбора журналов. Сбор журналов может быть проведен при условии наличия сетевого подключения между **ЕЦУ Dallas Lock** и сервера KSC:

- периодически (см. [«Настройка Kaspersky Security Center»](#));
- по команде пользователя из Консоли **ЕЦУ**.

Команда **Собрать журналы** в Консоли **ЕЦУ** для KSC доступна на вкладке *Сводка* на панели инструментов *Оперативное управление* (рис. 333).

16.4.3 Открыть web-администрирование

Для перехода в веб-интерфейс Kaspersky Security Center, необходимо выбрать команду **Открыть web-администрирование** на панели инструментов *Оперативное управление* (рис. 333).

При нажатии на кнопку **Открыть web-администрирование**, в браузере откроется окно ввода, где необходимо заполнить следующие поля:

- имя пользователя;
- пароль;
- имя Сервера администрирования, к которому нужно подключиться.

Затем нажать кнопку **Войти**.

16.4.4 Сводка Kaspersky Security Center

Вкладка *Сводка* (рис. 334) отображает общее состояние сервера KSC.

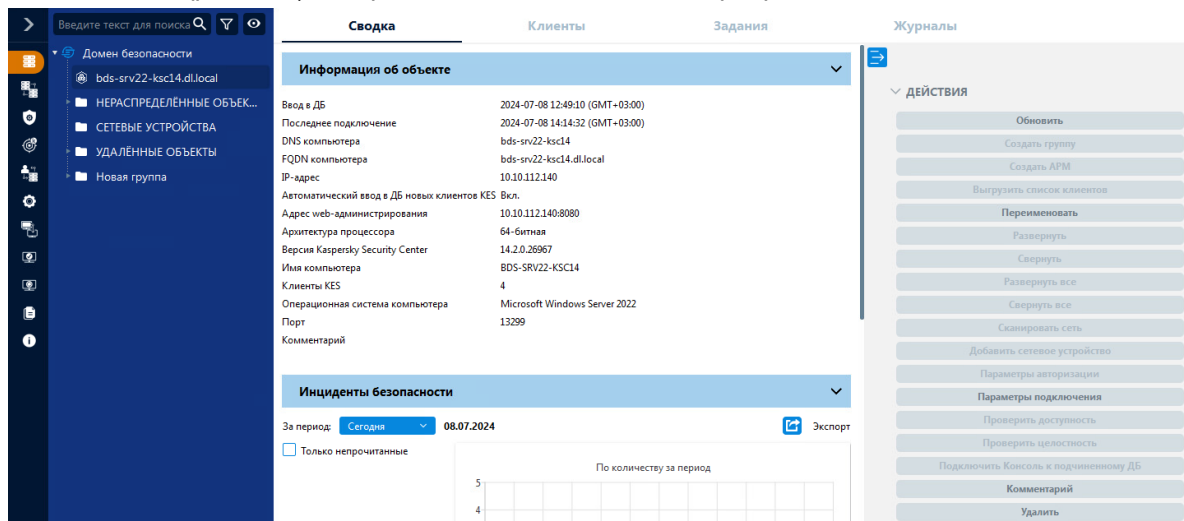


Рис. 334. Вкладка «Сводка» Kaspersky Security Center

Доступны следующие разделы информационной панели.

Информация об объекте

В верхней части информационной панели отображается следующая информация о текущем состоянии модуля:

- информация о дате и времени ввода в ДБ;
- версия Kaspersky Security Center;
- имя компьютера KSC;
- DNS компьютера KSC;
- FQDN компьютера KSC;
- ОС компьютера KSC;
- архитектура процессора;
- информация о дате и времени последнего подключения;
- информация о количестве клиентов KES;
- статус параметра **Автоматический ввод в ДБ новых клиентов KES**;
- IP-адрес;
- порт;
- адрес web-администрирования;
- комментарий.

Инциденты безопасности

Отображается список инцидентов безопасности с графической панелью. Доступна фильтрация отображаемых событий по периоду и настройка отображения диаграмм (см. [«Настройка инцидентов безопасности»](#)).

Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное. Поле *комментарий* доступно для редактирования.

На панели инструментов вкладки *Сводка* (рис. 334) доступны следующие действия:

- «Обновить» (обновить информацию на вкладке *Сводка*);
- «Переименовать» (переименовать имя сервера);
- «Удалить» (вывести сервер KSC и все входящие в него модули KES из ДБ **ЕЦУ Dallas Lock**);
- «Параметры подключения» (рис. 335) (редактировать адрес сервера, логин и пароль администратора, включать/отключать чекбоксом автоматический ввод в ДБ новых клиентов KES, которые появились в составе сервера KSC);
- «Комментарий» (добавленный комментарий отобразится в разделе *Информация об объекте* вкладки *Сводка*).

Рис. 335. Параметры подключения

Для сервера KSC доступны следующие команды оперативного управления (рис. 333) на панели инструментов:

- «Синхронизировать»;
- «Собрать журналы»;
- «Открыть web-администрирование».



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

16.4.5 Клиенты Kaspersky Security Center

Вкладка *Клиенты* содержит список клиентов KES, полученных от сервера KSC (рис. 336). Поле *Состояние* отражает состояние регистрации клиентов KES в ДБ:

☒ — отмеченное флагом поле означает, что данная учетная запись пользователя имеет доступ на уровне группы ДБ, при этом *Состояние* задано (переопределено) на данном уровне дерева;

☐ — пустое поле означает, что клиент KES не зарегистрирован в ДБ.

Для регистрации в ДБ ЕЦУ Dallas Lock незарегистрированных клиентов KES или удаления зарегистрированных модулей KES, необходимо установить/снять флаг в столбце *Состояние*, соответственно. При регистрации и удалении модулей KES изменения отображаются в дереве Домена безопасности.

Состояние	Клиент KES	Версия	APM	IP-адрес	Описание
☒	KES	12.4.0.467	bds-srv22-ksc14.dl.local	10.10.112.140	Kaspersky Endpoint Security для Windows
☒	KES	12.4.0.467	bds-win10-13.dl.local	10.10.112.230	Kaspersky Endpoint Security для Windows
☒	KES	12.4.0.467	bds-win10-12.dl.local	10.10.112.229	Kaspersky Endpoint Security для Windows
☒	KES	12.4.0.467	bds-win1123h2-12.dl.local	10.10.105.50	Kaspersky Endpoint Security для Windows

Рис. 336. Клиенты Kaspersky Security Center

16.4.6 Задания Kaspersky Security Center

На уровне модуля Kaspersky Endpoint Security в списке на вкладке *Задания* доступны для создания только задания, актуальные для KES (рис. 337):

- обновление антивирусных баз;
- сканирование клиентских APM.

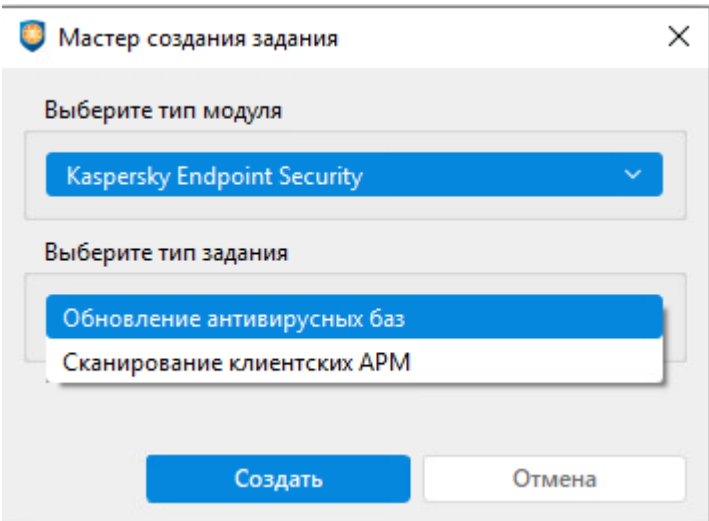


Рис. 337. Мастер создания задания

Работа с заданиями для модуля KES производится аналогично настройке заданий для ДБ (см. «Задания ДБ»).

16.4.7 Журналы Kaspersky Security Center

На вкладке *Журналы* для KSC доступен **Журнал Kaspersky** (рис. 338). В журнале отображаются все события, которые приходят с определенного сервера KSC на **ЕЦУ Dallas Lock**. Справа на панели инструментов можно задать параметры фильтрации. В разделе *Действия* можно сохранить отфильтрованные записи журнала с помощью команды **Экспортировать журнал**. Для очистки выбранного журнала модуля используется команда **Очистить журнал**.

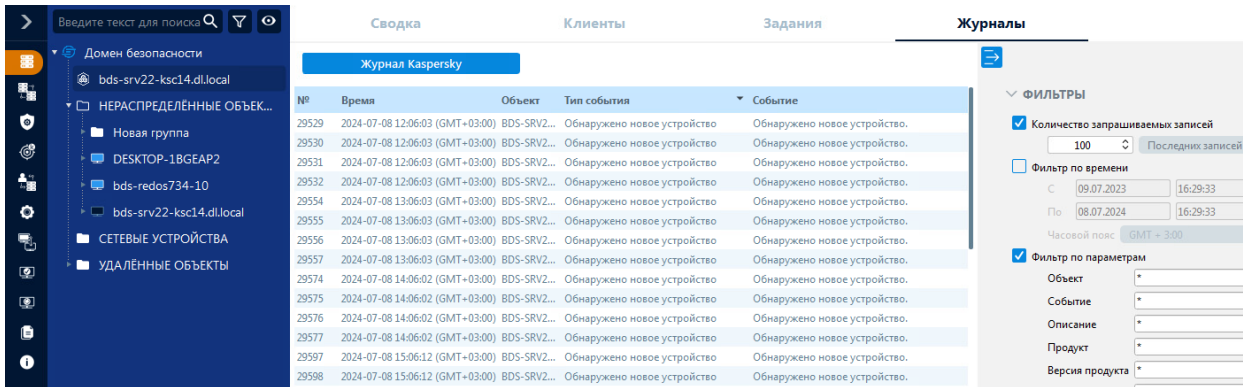


Рис. 338. Журналы Kaspersky Security Center

16.5 Настройка модуля Kaspersky Endpoint Security

KES отображаются как отдельные модули в составе APM, и могут принимать следующий вид:

-  — модуль подключен, защита включена;
-  — модуль подключен, защита выключена;
-  — модуль не подключен.

16.5.1 Сводка модуля Kaspersky Endpoint Security

Вкладка *Сводка* отображает общее состояние модуля KES (рис. 339).



Рис. 339. Сводка модуля Kaspersky Endpoint Security

Доступны следующие разделы информационной панели.

Информация об объекте
В верхней части информационной панели отображается следующая информация о текущем состоянии модуля: • информация о дате и времени последнего подключения модуля; • информация о дате и времени ввода модуля в ДБ; • версия Kaspersky Security Center; • имя компьютера KSC; • DNS компьютера KSC; • FQDN компьютера KSC; • ОС компьютера; • Архитектура процессора; • IP-адрес; • статус защиты KES; • информация о дате и времени последнего обновления антивирусных баз; • статус антивирусных баз; • информация о дате и времени последнего полного сканирования; • комментарий к модулю.
Инциденты безопасности
Отображается список инцидентов безопасности модуля с графической панелью. Доступна фильтрация отображаемых событий по периоду и настройка отображения диаграмм (см. «Настройка инцидентов безопасности»). Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное. Поле <i>Комментарий</i> доступно для редактирования.

Доступны следующие действия с модулем на панели инструментов:

1. Обновить.
2. Удалить.
3. Комментарий.

16.5.2 **Задания модуля Kaspersky Endpoint Security**

На уровне модуля Kaspersky Endpoint Security в списке на вкладке *Задания* доступны для создания только задания, актуальные для KES (рис. 340):

- обновление антивирусных баз;
- сканирование клиентских APM.

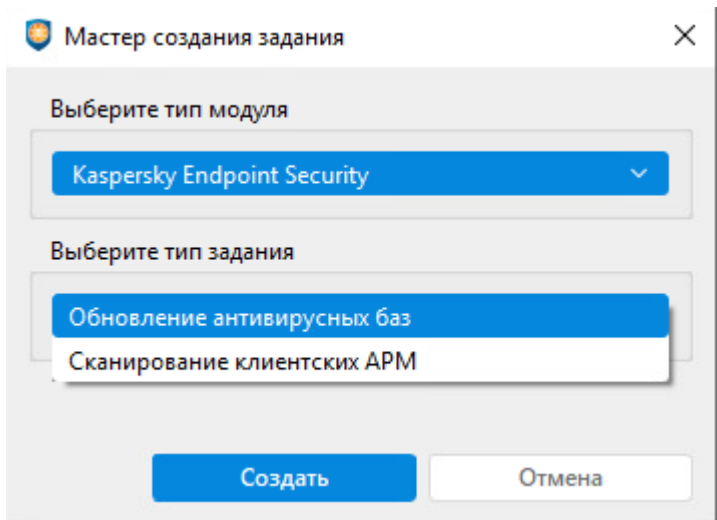


Рис. 340. Мастер создания задания

Работа с заданиями для модуля KES производится аналогично настройке заданий для ДБ (см. «Задания ДБ»).

16.5.3 Журналы модуля Kaspersky Endpoint Security

На вкладке *Журналы* для KES доступен **Журнал Kaspersky** (рис. 341). В журнале отображаются только те события, которые приходят с выбранного модуля KES. На панели инструментов можно задать параметры фильтрации. В разделе *Действия* можно сохранить отфильтрованные записи журнала с помощью команды **Экспортировать журнал**. Для очистки выбранного журнала модуля используется команда **Очистить журнал**.

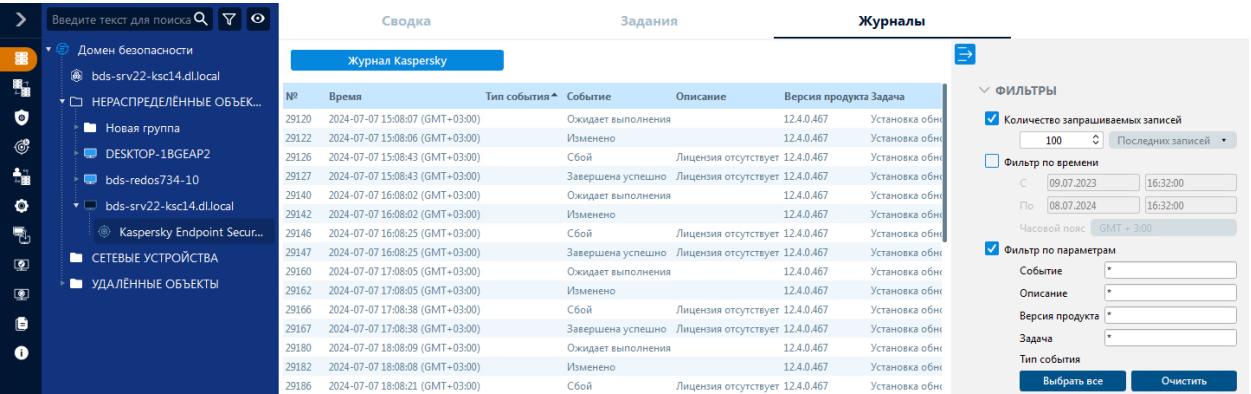


Рис. 341. Журналы модуля Kaspersky Endpoint Security

17 СЕТЕВОЕ ОБОРУДОВАНИЕ

17.1 Регистрация сетевого устройства в ДБ

Зарегистрировать сетевое устройство в Домене безопасности можно следующими способами:

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

Оба способа позволяют зарегистрировать сетевое устройство в Домене безопасности **ЕЦУ Dallas Lock** по следующим протоколам: SNMP и SSH.



Для корректного взаимодействия **ЕЦУ Dallas Lock** с сетевыми устройствами требуется дополнительно открыть следующие порты:

- SNMP: порт 161/UDP, исходящее подключение;
- SSH: порт 22/TCP, исходящее подключение;
- Syslog:
 - порт 514/UDP, входящее подключение;
 - порт 1468/TCP, входящее подключение (при необходимости).



В рамках контроля СУ по протоколу SSH обеспечена поддержка СУ Cisco IOS, Cisco ASA, D-Link DGS и ZyXel ZyNOS.

17.1.1 Добавление сетевого устройства по IP

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

1. Убедиться, что сетевое устройство поддерживает один из протоколов (SNMP/SSH), и доступно по сети для всех серверов кластера ДБ.
2. Запустить Консоль **ЕЦУ** и авторизоваться.
3. На уровне Домена безопасности или группы (подгруппы) на вкладке *Сводка* на панели инструментов *Действия* выбрать команду **Добавить сетевое устройство** (рис. 342).

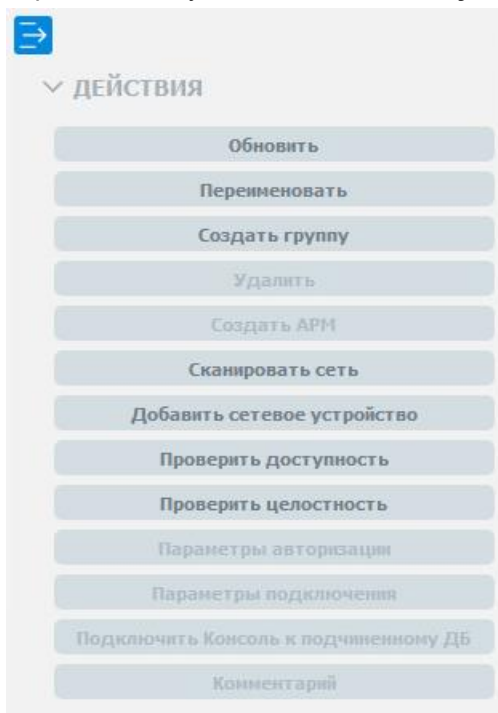


Рис. 342. Добавить сетевое устройство

4. Появится окно **Добавление сетевого устройства** (рис. 343) в котором необходимо указать IPv4-адрес и выбрать тип протокола сетевого устройства. Для выбора типа протокола, необходимо установить флаг напротив нужного (SNMP или SSH). По умолчанию включен флаг *Использовать SNMP*.

Далее необходимо заполнить параметры подключения выбранного протокола:

- | <u>SNMP</u> | <u>SSH</u> |
|-------------------------|----------------------------|
| • версия протокола SNMP | • порт |
| • порт | • таймаут подключения (мс) |
| • таймаут (мс) | • таймаут ответа (мс) |
| • сообщество (пароль) | • имя пользователя |
| | • пароль |
| | • привилегированный пароль |

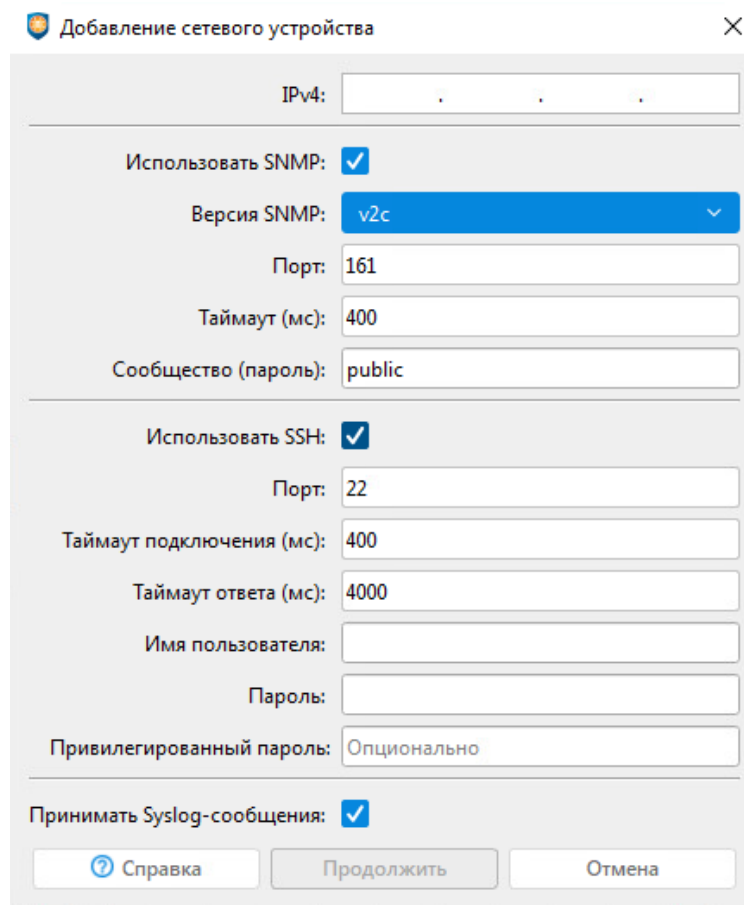


Рис. 343. Окно параметров подключения

5. После заполнения всех полей нажать кнопку **Продолжить**. При регистрации устройства по протоколу SNMP появится окно **Предупреждение** (рис. 344). Для продолжения процесса регистрации необходимо нажать кнопку **Ок**, при нажатии кнопки **Отмена** будет произведен возврат на шаг назад, где можно будет внести изменения в параметры подключения.

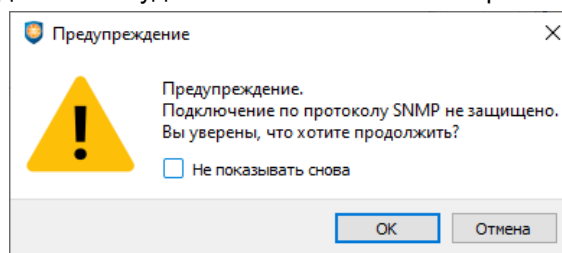


Рис. 344. Предупреждение о подключении по протоколу SNMP



При установке флага *Не показывать снова*, следующие предупреждения будут скрыты. Восстановить предупреждения можно нажав на кнопку «Восстановить предупреждения» в главном меню консоли **ЕЦУ** → **Параметры** → **Общие** (см. [«Параметры работы»](#)).

Если процесс регистрации сетевого устройства в ДБ прошел успешно, то через некоторое время в дереве Домена на уровне, на котором была вызвана команда **Добавить сетевое устройство**, появится иконка зарегистрированного сетевого устройства (рис. 345).

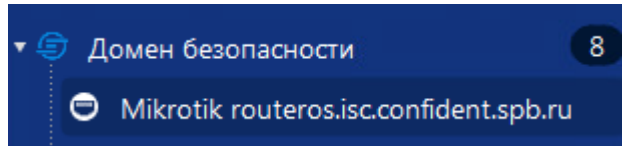


Рис. 345. Иконка зарегистрированного сетевого устройства в дереве ДБ

17.1.2 Сканирование диапазона сетевых адресов

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

1. Убедиться, что сетевое устройство поддерживает один из протоколов (SNMP/SSH), и доступно по сети для всех серверов кластера ДБ.
2. Запустить Консоль **ЕЦУ** и авторизоваться.
3. На уровне Домена безопасности или группы (подгруппы) на вкладке *Сводка* на панели инструментов *Действия* выбрать команду **Сканировать сеть** (рис. 346).

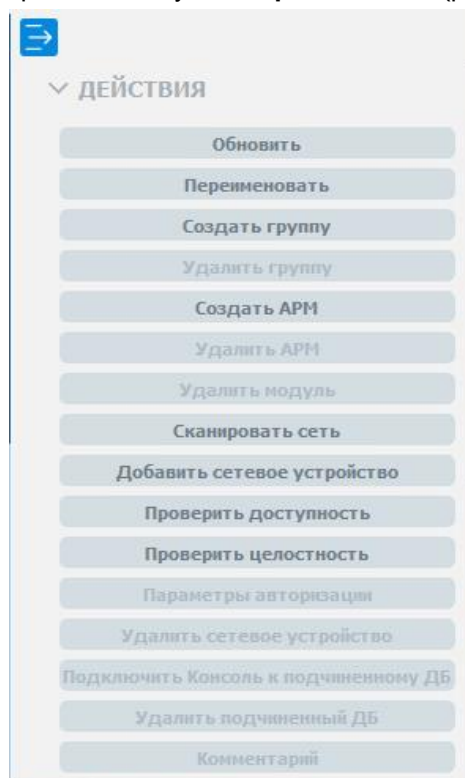


Рис. 346. Сканировать сеть

4. Появится окно **Сканирование сети**, в котором нужно перейти на вкладку *Сетевое устройство* и указать диапазон IPv4-адресов для сканирования (рис. 347). Затем выбрать один из протоколов (SNMP/SSH) и заполнить требуемые для него поля:

SNMP

- версия протокола SNMP
- порт
- таймаут (мс)
- сообщество (пароль)

SSH

- порт
- таймаут подключения (мс)
- таймаут ответа (мс)
- имя пользователя
- пароль
- привилегированный пароль

Сканирование сети

Модуль

Сетевое устройство

IPv4: . . . -

Использовать SNMP: ☒

Версия SNMP: v2c

Порт: 161

Таймаут (мс): 400

Сообщество (пароль): public

Использовать SSH: ☒

Порт: 22

Таймаут подключения (мс): 400

Таймаут ответа (мс): 4000

Имя пользователя:

Пароль:

Привилегированный пароль: Опционально

Принимать Syslog-сообщения: ☒

Справка Сканировать Отмена

Рис. 347. Окно сканирование сети

В этом же окне с помощью постановки флага можно настроить прием Syslog-сообщений.

5. После заполнения всех полей нажать кнопку **Сканировать** и далее можно просматривать состояние процесса сканирования для каждого диапазона сетевых адресов.



При сканировании сети по протоколу SNMP появится окно **Предупреждение** (рис. 344). Для продолжения процесса сканирования необходимо нажать кнопку **Ок**, при нажатии кнопки **Отмена** будет произведен возврат на шаг назад, где можно внести изменения в параметры сканирования.

6. По завершении процесса сканирования из списка обнаруженных объектов можно выбрать те объекты, которые необходимо зарегистрировать в ДБ (рис. 348).

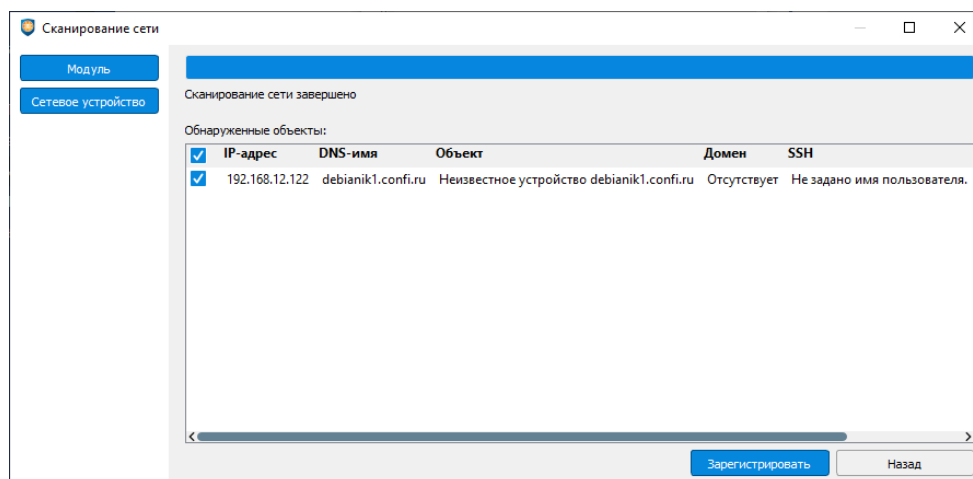


Рис. 348. Выбор объектов для регистрации в ДБ

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 регистрируются в дереве Домена безопасности в базовой группе «Сетевые устройства» (рис. 349).

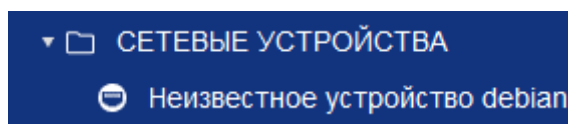


Рис. 349. Иконка зарегистрированного сетевого устройства в дереве ДБ

17.2 Удаление сетевого устройства из ДБ

Для удаления сетевого устройства из Домена безопасности **ЕЦУ Dallas Lock** необходимо:

1. Выбрать пункт **Удалить** из контекстного меню, нажав правой кнопкой мыши на нужное устройство в дереве ДБ (рис. 350), или воспользоваться командой **Удалить** на панели инструментов **Действия** вкладки **Сводка** на уровне устройства в дереве ДБ (рис. 351).

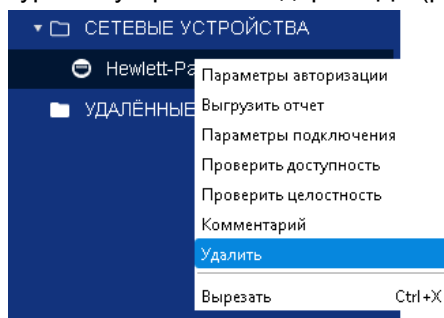


Рис. 350. Удаление устройства посредством контекстного меню

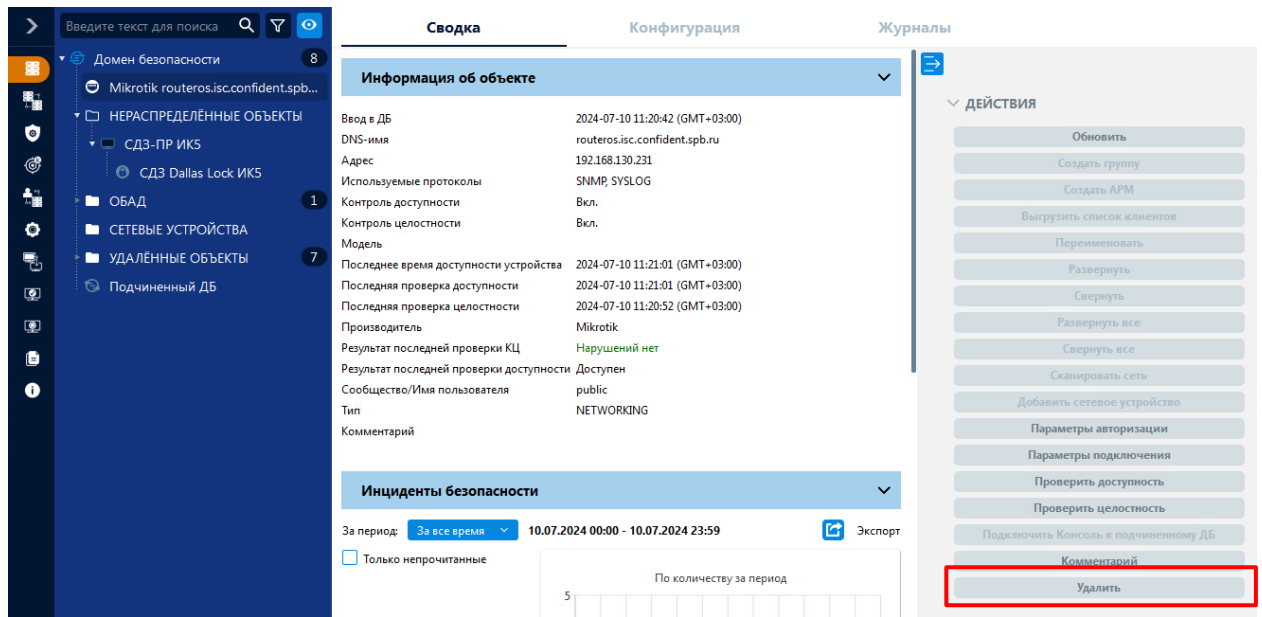


Рис. 351. Удаление посредством панели «Действия»

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

17.3 Настройка сетевого устройства

В дереве Домена безопасности **ЕЦУ Dallas Lock** присутствуют зарегистрированные сетевые устройства.

Значки объектов, обозначающих сетевые устройства, зависят от состояния сетевого устройства и могут принимать следующий вид:

-  — сетевое устройство доступно;
-  — сетевое устройство недоступно;
-  — на сетевом устройстве зафиксировано нарушение целостности конфигурации, при этом сетевое устройство доступно;
-  — на сетевом устройстве зафиксировано нарушение целостности конфигурации, при этом сетевое устройство недоступно;
-  — связь с сетевым устройством отсутствует свыше заданного на **ЕЦУ Dallas Lock** времени, которое определяется параметром **Оповещения при отсутствии связи с объектом (в днях)** (при условии, что настроено оповещение об отсутствии связи с объектом).

Настройки на уровне сетевого устройства отображаются на нескольких основных вкладках.

17.3.1 Сводка сетевого устройства

Вкладка *Сводка* на уровне сетевого устройства отображает общее состояние сетевого устройства (рис. 352).

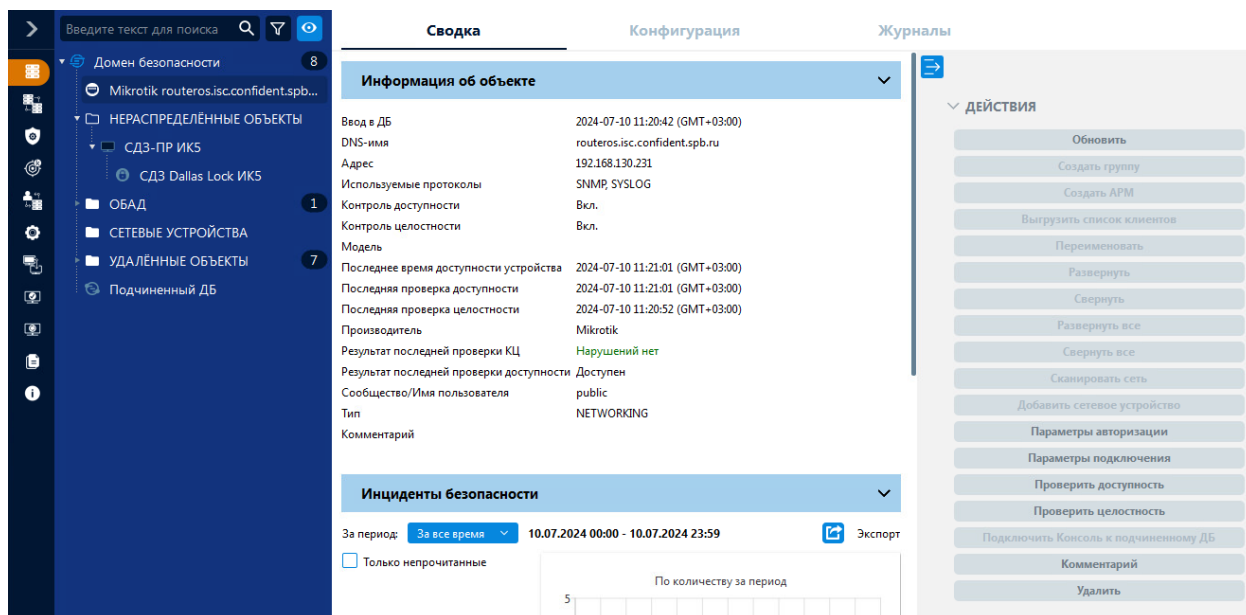


Рис. 352. Сводка сетевого устройства

Доступны следующие разделы информационной панели:

Информация об объекте
В верхней части информационной панели отображается следующая информация о текущем состоянии сетевого устройства: • дата и время регистрации сетевого устройства в ДБ; • DNS-имя устройства; • сетевой адрес устройства; • используемые протоколы; • состояние контроля доступности; • состояние контроля целостности; • информация о производителе, типе и модели сетевого устройства; • дата и время последней доступности устройства; • дата и время последней проверки доступности; • дата и время последней проверки целостности; • информация о результатах проверки целостности; • информация о результатах проверки доступности устройства; • сообщество/имя пользователя, под которым зарегистрировано устройство; • комментарий к устройству.
Инциденты безопасности
Отображается список инцидентов безопасности сетевого устройства с графической панелью. Доступна фильтрация отображаемых событий по периоду и настройка отображения диаграмм (см. «Настройка инцидентов безопасности»). Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное. Поле <i>Комментарий</i> доступно для редактирования.

Доступны следующие действия с сетевым устройством на панели инструментов:

1. Обновить.
2. Параметры авторизации.
3. Параметры подключения.

4. Проверить доступность.
5. Проверить целостность.
6. Комментарий.
7. Удалить.

На панели инструментов доступна команда оперативного управления **Перезагрузить**.

Не все сетевые устройства поддерживают управление питанием по SNMP, но даже такие устройства будут добавлены в группу сетевых устройств ДБ. Для корректной возможности перезагрузки сетевого устройства по SNMP требуется настроить параметры авторизации. В поле *Управление питанием* должно быть прописано *public* (рис. 353).



Рис. 353. Настройки параметров авторизации



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

17.3.2 Конфигурация сетевого устройства

Вкладка *Конфигурация* на уровне сетевого устройства отображает параметры сетевого устройства (рис. 354).

№	Состояние	Параметр	Эталонное значение	Последнее значение
1	✓	Описание	RouterOS CHR	RouterOS CHR
2	✓	Идентификатор вендора	1.3.6.1.4.1.14988.1	1.3.6.1.4.1.14988.1
3	✓	Контакты	Ø	Ø
4	✓	Имя узла	RouterOS	RouterOS
5	✓	Расположение	Ø	Ø
6	✓	Сетевой уровень сервиса	78	78
7	✓	Количество сетевых интерфейсов	1	1

Рис. 354. Конфигурация сетевого устройства

В таблице на вкладке *Конфигурация* содержатся параметры и их значения, полученные от сетевого устройства по протоколу SNMP или SSH.

Список параметров сетевого устройства представляется собой таблицу с полями:

- | SNMP | SSH |
|----------------------|----------------------|
| • номер | • номер |
| • состояние | • состояние |
| • параметр | • имя |
| • эталонное значение | • команда |
| • последнее значение | • эталонное значение |
| | • последнее значение |

Над таблицей есть поле *Показать только отличия*, установка флага напротив этого поля приводит к переходу в режим отображения параметров конфигурации, целостность которых нарушена. Снятие флага возвращает к просмотру всех параметров.



MIB — база управляющей информации. OID — это уникальный идентификатор объекта в SNMP (объектом может быть модель устройства или конкретный параметр). OID записывается как последовательность чисел, разделенных точкой. Например, «1.3.6.3.2.1». MIB-файлы позволяют использовать текстовое представление OID. Например, для OIda «1.3.6.1.2.1.31.1.1.1.10» текстовое представление — «ifHCOutOctets».

При регистрации сетевого устройства в Домене безопасности в Базе конфигураций **ЕЦУ Dallas Lock** осуществляется поиск конфигурации для данного устройства.

Конфигурационные файлы — рекомендованные списки параметров устройств, нарушение целостности которых считается инцидентом безопасности.

В **ЕЦУ Dallas Lock** есть несколько видов конфигурационных файлов устройств:

- конфигурация для определенных моделей устройств;
- конфигурация для определенных производителей;
- конфигурация по умолчанию.

После добавления устройства в Базе конфигураций производится поиск наиболее подходящей конфигурации для данной модели устройства. Если конфигурация для данной модели не обнаружена, производится поиск конфигурации для производителя. Если не обнаружена конфигурация для производителя, используется конфигурация по умолчанию (о том, как пополнить Базу конфигураций **ЕЦУ Dallas Lock** см. [«Параметры сетевого оборудования»](#)).

Найденная в базе конфигурация представляет собой список OID. Устройство опрашивается по списку OID из конфигурации, далее полученные при первом опросе значения используются в качестве эталонных.

Если в ответ на запрос значения параметра у сетевого устройства **ЕЦУ Dallas Lock** получает пустое значение, в таблице напротив названия такого параметра будет содержаться символ «Ø». Если устройство не ответило на запрос значения параметра — в таблице будет содержаться 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. 355).



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

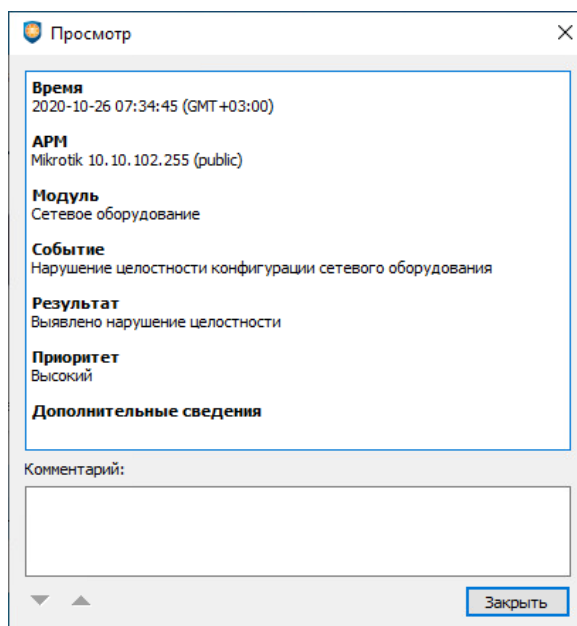


Рис. 355. Просмотр сведений об инциденте безопасности

На вкладке *Конфигурация* соответствующий параметр, отличный от эталонного, будет выделен цветом:

- эталонное значение соответствующего параметра – красным;
- последнее значение соответствующего параметра – зеленым.



Рис. 356. Отображение значений параметров сетевого оборудования на вкладке «Конфигурация»

На вкладке *Конфигурация* на панели инструментов *Действия* доступны следующие команды (рис. 356):

1. «Применить изменения», предназначена для принятия последних полученных значений конфигурации за эталонные.
2. «Поиск...», позволяет искать параметры конфигурации.
3. «Обновить», предназначена для получения актуальных значений конфигурации от устройства.
4. «Сохранить в файл», предназначена для сохранения отчета о текущей конфигурации сетевого устройства в формате «.txt».
5. «Включить/Выключить контроль доступности», предназначена для изменения состояния контроля доступности сетевого устройства.
6. «Включить/Выключить контроль целостности», предназначена для изменения состояния контроля целостности сетевого устройства.
7. «Добавить параметр», для нового контролируемого параметра позволяет установить флаг «Контролировать параметр», а также задать имя и OID.

При добавлении параметра, он записывается в файл конфигурации и отображается для всех связанных с ним устройств (влияет на новые и добавленные ранее сетевые устройства ДБ).

8. «Удалить выделенные параметры».

Для отображения только отличий между эталонным значением и последним значением доступен фильтр *Показать только отличия*.

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

17.3.3 Журналы сетевого устройства

На вкладке *Журналы* для сетевого устройства доступен **Журнал Syslog**. В журнале отображаются только Syslog-сообщения, полученные от сетевого устройства.

На панели инструментов можно задать параметры фильтрации. На панели инструментов в разделе *Действия* можно сохранить отфильтрованные записи журнала с помощью команды **Экспортировать журнал**.

18 ПОДЧИНЕННЫЙ ДОМЕН БЕЗОПАСНОСТИ



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.



В ЕЦУ Dallas Lock должно выполняться правило создания связей между главным и подчиненным доменом, которое заключается в запрете организации «циклов администрирования доменов», когда главный домен является подчиненным доменом для одного и того же домена.



Подчиненный домен безопасности может иметь только один главный ДБ на один уровень выше по иерархии ЕЦУ Dallas Lock (существует возможность создавать несколько уровней подчинения). Ограничения по количеству подчиненных у главного домена безопасности устанавливаются лицензией.

18.1 Ввод ДБ в подчинение

18.1.1 Ввод ДБ в подчинение в процессе установки

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

1. Убедиться, что Домен безопасности, в подчинение которому осуществляется ввод, доступен по сети.
2. Запустить процесс установки ЕЦУ Dallas Lock.
3. На шаге **Выбор типа домена** выбрать пункт *Подчиненный домен безопасности* (рис. 357).

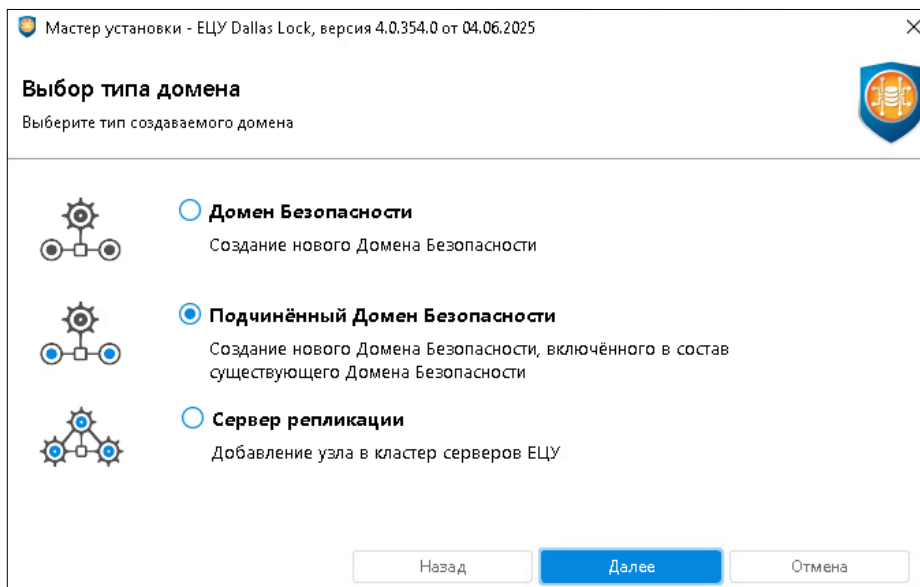


Рис. 357. Шаг «Выбор типа домена» в мастере установки ЕЦУ Dallas Lock

4. Задать параметры главного ДБ (рис. 358):
 - адрес главного ДБ;
 - ключ доступа к ДБ.

Мастер установки - ЕЦУ Dallas Lock, версия 4.0.354.0 от 04.06.2025

Параметры удалённого сервера
Укажите параметры удалённого сервера

Адрес главного ДБ:

Ключ доступа:

Назад Далее Отмена

Рис. 358. Параметры удаленного сервера

5. Далее продолжить и завершить установку **ЕЦУ Dallas Lock**.
6. После завершения установки подчиненного ДБ в дереве главного ДБ появится введенный в подчинение ДБ (рис. 359).

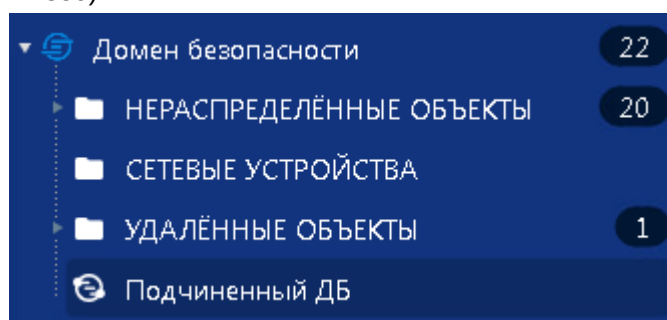


Рис. 359. Подчиненный ДБ в дереве родительского

18.1.2 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** > выбрать пункт **Параметры ДБ**.
4. В блоке *Ввод в подчинение* указать сетевое имя сервера из главного домена и ключ доступа к главному домену безопасности (рис. 360).

Ввод в подчинение

Сетевое имя сервера

Ключ доступа

Ввести

Рис. 360. Ввод в подчинение

5. Нажать кнопку **Ввести**.

Если процесс ввода в подчинение прошел успешно, то через некоторое время появится соответствующее сообщение (рис. 361).

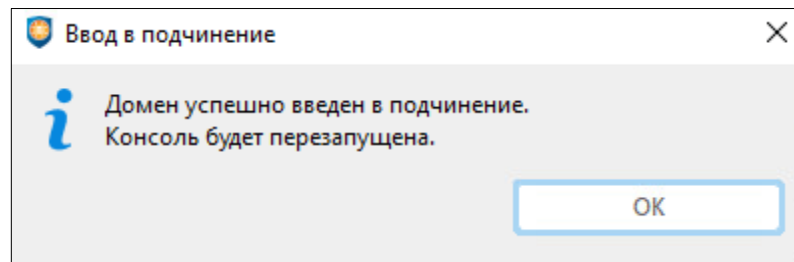


Рис. 361. ДБ успешно введен в подчинение

После перезапуска Консоли на уровне ДБ на вкладке **Сводка** → **Информация об объекте** отобразится информация о родительском домене (рис. 362).

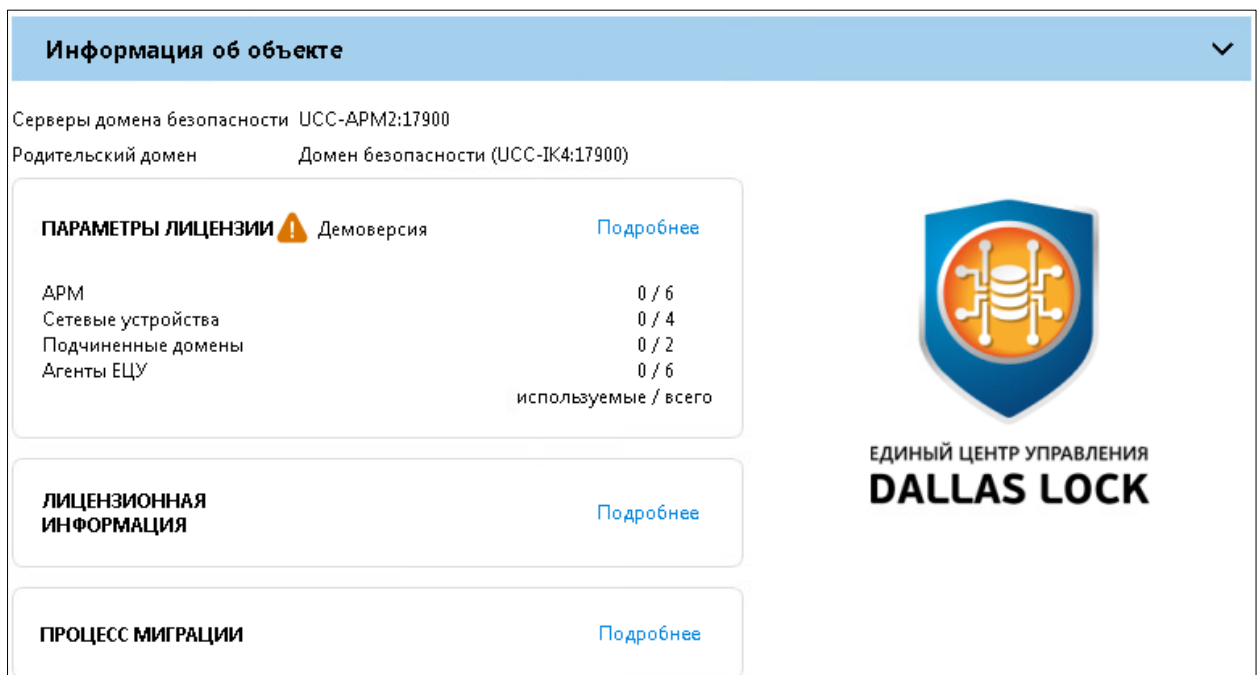


Рис. 362. Информация о родительском домене

Также в дереве главного ДБ появится введенный в подчинение ДБ (рис. 359).

18.2 Вывод ДБ из подчинения

18.2.1 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** → **Параметры ДБ**.
3. В блоке *Ввод в подчинение* (рис. 363) нажать кнопку **Вывод из подчинения**.

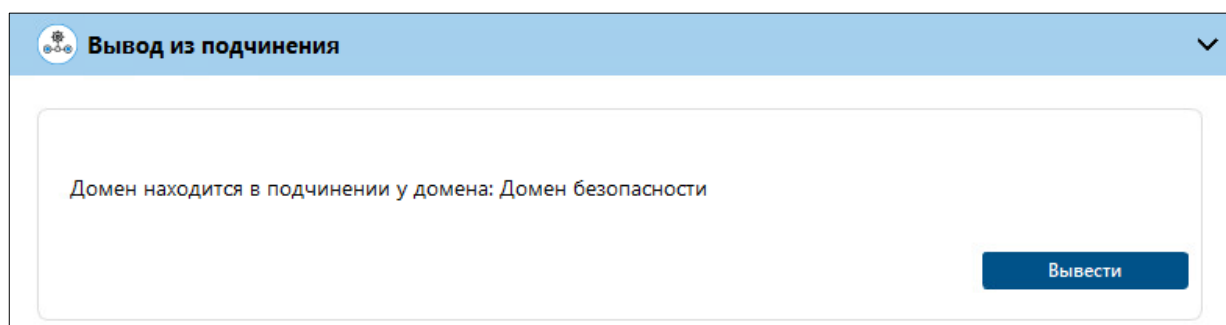


Рис. 363. Вывод из подчинения

Если процесс вывода домена из подчинения прошел успешно, то через некоторое время появится соответствующее сообщение (рис. 364).

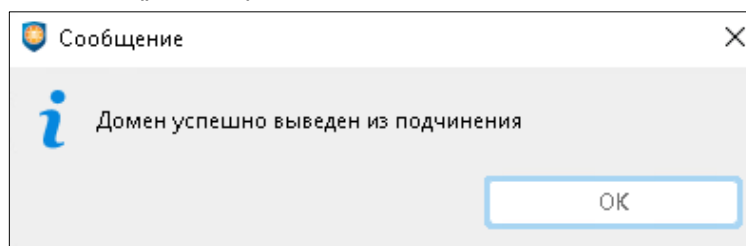


Рис. 364. ДБ успешно выведен из подчинения

18.2.2 Вывод ДБ из подчинения через консоль главного ДБ

Для вывода из подчинения ДБ через Консоль **ЕЦУ** главного ДБ необходимо:

1. Подключить Консоль **ЕЦУ** к главному ДБ.
2. Выбрать подчиненный ДБ в дереве и на вкладке *Сводка* нажать на панели инструментов *Действия* кнопку **Удалить** (рис. 366) или выбрать соответствующую команду из контекстного меню, нажав правой кнопкой мыши на подчиненный ДБ в дереве (рис. 365).

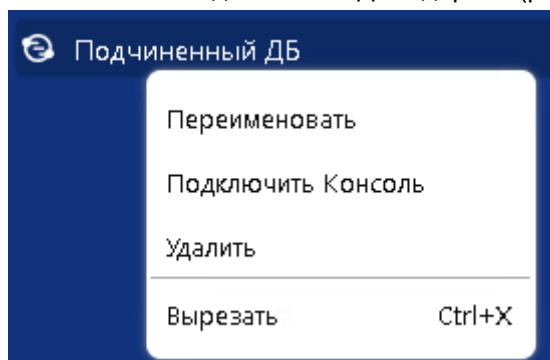


Рис. 365. Контекстное меню подчиненного ДБ

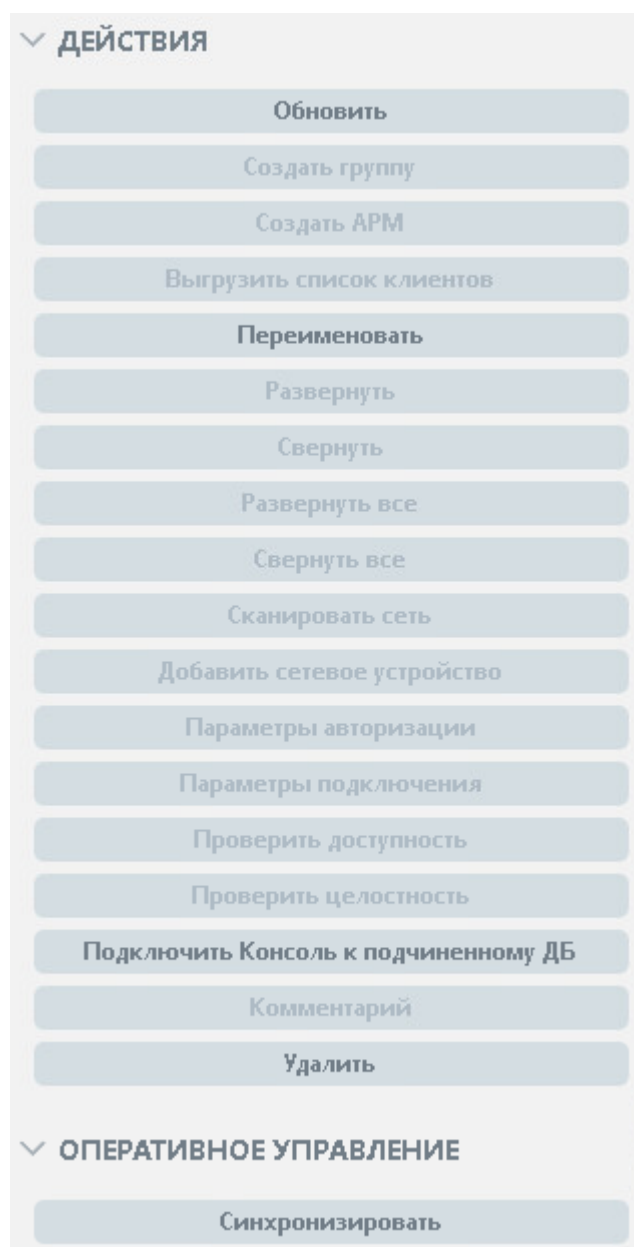


Рис. 366 Команды панели инструментов для подчиненного ДБ

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

18.3 Настройка подчиненного домена безопасности

В дереве главного Домена безопасности **ЕЦУ Dallas Lock** присутствуют подчиненные ДБ.

Значки объектов, обозначающих подчиненные ДБ, зависят от состояния ДБ и могут принимать следующий вид:



— подчиненный ДБ подключен;



— связь с подчиненным ДБ отсутствует;



— связь с подчиненным ДБ отсутствует свыше заданного в главном ДБ времени, которое определяется параметром **Оповещения при отсутствии связи с объектом (в днях)** (при условии, что настроено оповещение об отсутствии связи с объектом).

Администратор **ЕЦУ Dallas Lock** может перемещать подчиненные ДБ в группы (подгруппы) дерева ДБ. Для этого необходимо перетащить значок нужного подчиненного ДБ кнопкой мыши в поле другого значка (**Drag-and-drop**).

Настройки на уровне подчиненного ДБ отображаются на нескольких основных вкладках.

18.3.1 Синхронизация

Для приведения в соответствие значениям параметров, выставленным на главном ДБ, на подчиненном ДБ необходимо проведение синхронизации. Синхронизация может быть проведена при условии наличия сетевого подключения между главным и подчиненным доменом:

- при включении подчиненного ДБ;
- периодически (см. [«Параметры работы модулей»](#));
- по команде пользователя из Консоли **ЕЦУ** главного ДБ.

Команда **Синхронизировать** в Консоли **ЕЦУ** доступна на вкладке *Сводка* на уровне подчиненного ДБ в дереве ДБ на панели инструментов *Оперативное управление*.

18.3.2 Сводка подчиненного ДБ

Вкладка *Сводка* на уровне подчиненного ДБ отображает общее состояние подчиненного ДБ (рис. 367).

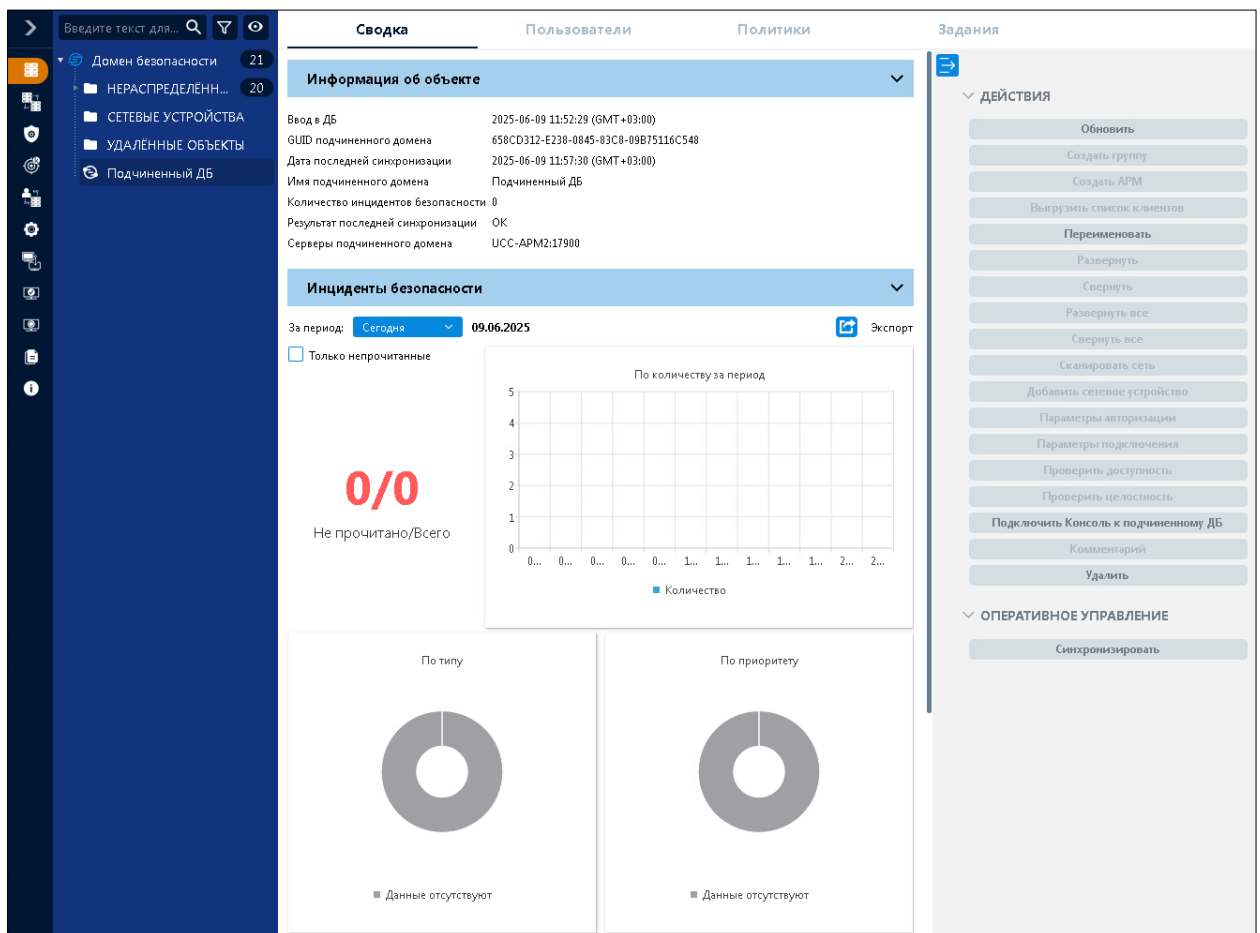


Рис. 367. Вкладка «Сводка»

Доступны следующие разделы информационной панели.

Информация об объекте

В информационной панели отображается следующая информация о текущем состоянии модуля:

- информация о дате и времени ввода в ДБ;
- имя подчиненного домена;
- GUID подчиненного домена;
- сервера кластера **ЕЦУ**;
- информация о дате и времени последней синхронизации;
- результат последней синхронизации;
- количество инцидентов безопасности.

Доступны следующие действия с подчиненным ДБ на панели инструментов:

1. Обновить.
2. Переименовать.
3. Удалить подчиненный домен.
4. Подключить Консоль к подчиненному ДБ.

Доступны следующие команды оперативного управления на панели инструментов:

1. Синхронизировать.



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

Открыть Консоль **ЕЦУ Dallas Lock** подчиненного ДБ можно с Консоли **ЕЦУ Dallas Lock** Главного ДБ. Для этого нужно:

1. Нажать **Подключить Консоль к подчиненному ДБ** (рис. 367) на панели инструментов *Действия* вкладки *Сводка*.
Подключить Консоль подчиненного ДБ можно также с помощью одноименной функции контекстного меню (рис. 365)
2. Появится окно **Подключение к серверу** (рис. 368). Далее необходимо заполнить следующие поля:
 - имя консоли;
 - сетевое имя сервера;
 - ключ доступа к ДБ.

Рис. 368. Окно «Подключение к серверу»

Затем нажать **Зарегистрировать**.

3. В следующем окне (рис. 369), необходимо ввести авторизационные данные и нажать **Подключиться**.

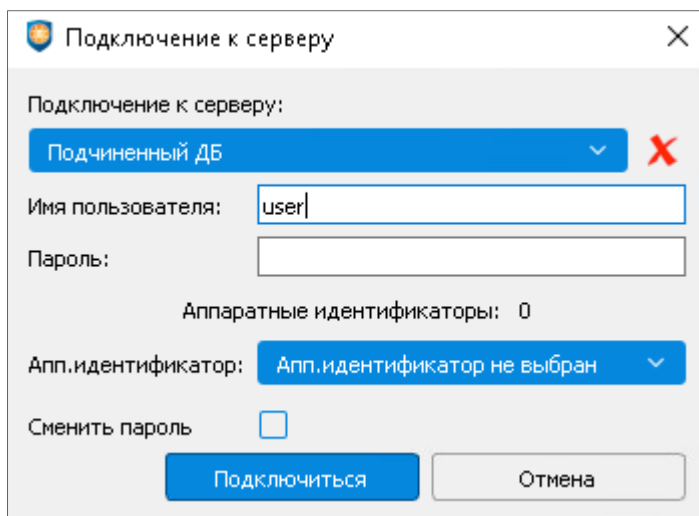


Рис. 369. Ввод авторизационных данных

Если данные введены верно, будет открыто новое окно Консоли управления **ЕЦУ** Подчиненного ДБ.

18.3.3 Пользователи и группы подчиненного ДБ

Вкладка *Пользователи* 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.



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.



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.

18.3.4 Политики подчиненного ДБ

Вкладка *Политики* на уровне подчиненного ДБ позволяет редактировать политики на подчиненном ДБ (рис. 370).

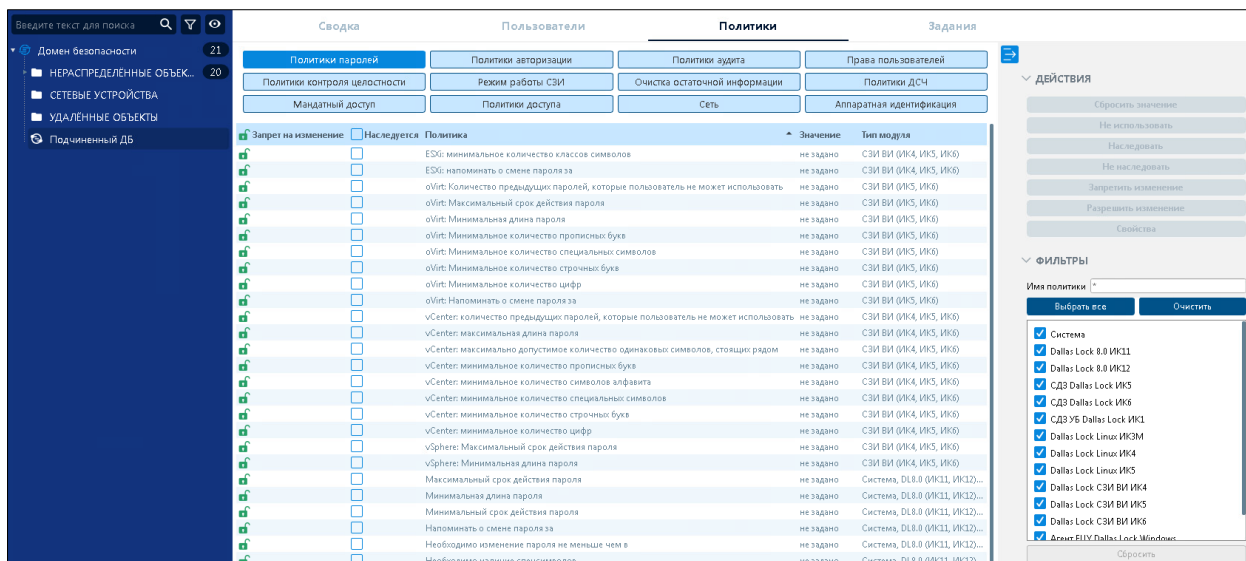


Рис. 370. Вкладка «Политики»



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.

18.3.5 Задания подчиненного ДБ

На уровне подчиненного ДБ в списке на вкладке *Задания* доступны для создания задания, актуальные для модулей данного подчиненного ДБ.

При создании задания на главном ДБ данное задание автоматически создается на подчиненном ДБ. Просмотр результатов выполнения задания доступен по кнопке **Сохранить в файл**.



В главном ДБ можно также создать задания для модулей, не актуальных для данного подчиненного ДБ, но такие задания выполнены не будут.

Работа с заданиями для подчиненного ДБ производится аналогично настройке заданий для ДБ (см. [«Задания ДБ»](#)).

Приложение А

Предустановленные значения политик безопасности

А.1 Шаблоны автоматизированных систем

Параметры	Значения параметров			
	«Базовая для 1Б»	«Базовая для 1В»	«Базовая для 1Г»	«Базовая для 1Д»
Категория «Политики паролей»				
Минимальная длина пароля	8 симв.	6 симв.		
Необходимо наличие спецсимволов	Да	—		
Необходимо наличие строчных и прописных букв	Да	—		
Необходимо наличие цифр	Да			
oVirt: Минимальная длина пароля	8 симв.	6 симв.		
vCenter: максимальная длина пароля	20			
vSphere: Минимальная длина пароля	8 симв.	6 симв.		
Категория «Политики аудита»				
Журнал печати	Вкл.			—
Журнал управления пользователями и группами	Вкл.		—	
Журнал управления политиками безопасности	Вкл.		—	
Журнал ресурсов	Вкл.			—
Журнал входов/выходов	Вкл.			
Журнал запуска/завершения процессов	Вкл.			—
Заносить в журнал события запуска и остановки ОС	Да			
Заносить в журнал события запуска и остановки модулей администрирования DL	Да			—
Аудит событий зачистки	Вкл.			—
Аудит устройств	Вкл.			—
Фиксировать в журнале неправильные пароли	Да			—
Печатать/редактировать штамп	Да		—	
Системный журнал	Вкл.			
Журнал безопасности	Вкл.		—	

Параметры	Значения параметров			
	«Базовая для 1Б»	«Базовая для 1В»	«Базовая для 1Г»	«Базовая для 1Д»
Категория «Политики контроля целостности»				
Проверять целостность прогр. апп. среды при загрузке ОС	Вкл.			
Проверять целостность реестра при загрузке ОС	Вкл.			
Проверять целостность ФС при загрузке ОС	Вкл.			
Виртуальная машина: Проверять целостность при загрузке ОС	Да			
Категория «Режим работы СЗИ»				
Система обнаружения вторжений	Вкл.			
Межсетевой экран	Вкл.			
Категория «Очистка остаточной информации»				
Затирающая последовательность	00 00 00 00			
Количество циклов затирания	2		1	
Очищать освобождаемое дисковое пространство	Да			—
Очищать данные в конфиденциальных сеансах доступа	Да		—	
Очищать файл подкачки виртуальной памяти	Да			—
Категория «Политики ДСЧ»				
Тестировать ДСЧ при входе	Да			
Число попыток самотестирования ДСЧ	1			

А.2 Шаблоны государственных информационных систем

Параметры	Значения параметров		
	«Базовая для К1»	«Базовая для К2»	«Базовая для К3»
Категория «Политики паролей»			
Максимальный срок действия пароля	60 дн.	90 дн.	120 дн.
Минимальная длина пароля	8 симв.	6 симв.	
Минимальный срок действия пароля	30 дн.		
Необходимо изменение пароля не меньше, чем в	10 симв.		
Необходимо наличие спецсимволов	Да		
Необходимо наличие строчных и прописных букв	Да		

Параметры	Значения параметров		
	«Базовая для K1»	«Базовая для K2»	«Базовая для K3»
Необходимо наличие цифр	Да		
oVirt: Минимальная длина пароля	8 симв.	6 симв.	
oVirt: Максимальный срок действия пароля	60 дн.	90 дн.	120 дн.
vCenter: максимальная длина пароля	20		
vSphere: Минимальная длина пароля	8 симв.	6 симв.	
vSphere: Максимальный срок действия пароля	60 дн.	90 дн.	120 дн.
Категория «Политики авторизации»			
Максимальное количество ошибок ввода пароля	4	8	10
Время блокировки учетной записи в случае ввода неправильных паролей	15 мин.	10 мин.	5 мин.
Максимальное количество сессий	2	—	
Время бездействия, после которого будет заблокирован сеанс доступа	5 мин.	—	
Категория «Политики аудита»			
Журнал входов/выходов	Вкл.		
Заносить в журнал события запуска и остановки ОС	Да		
Заносить в журналы ошибки ОС	Вкл.	—	
Журнал контроля приложений COB	Вкл.		
Системный журнал	Вкл.		
Срок хранения журналов в месяцах	3		
Категория «Политики контроля целостности»			
Проверять целостность прогр. апп. среды при загрузке ОС	Вкл.		
Проверять целостность реестра при загрузке ОС	Вкл.		
Проверять целостность ФС при загрузке ОС	Вкл.		
Генерация событий аудита аппаратной целостности	Да		
Виртуальная машина: Проверять целостность при загрузке ОС	Да		
Категория «Режим работы СЗИ»			
Система обнаружения вторжений	Вкл.		
Межсетевой экран	Вкл.		
Категория «Очистка остаточной информации»			
Затирающая последовательность	00 00 00 00		
Количество циклов затирания	1		

Параметры	Значения параметров		
	«Базовая для К1»	«Базовая для К2»	«Базовая для К3»
Категория «Политики ДСЧ»			
Тестировать ДСЧ при входе	Да		
Число попыток самотестирования ДСЧ	1		

А.3 Шаблоны информационных систем персональных данных

Параметры	Значения параметров			
	«Базовая для 1 УЗ»	«Базовая для 2 УЗ»	«Базовая для 3 УЗ»	«Базовая для 4 УЗ»
Категория «Политики паролей»				
Максимальный срок действия пароля	60 дн.	90 дн.	120 дн.	180 дн.
Минимальная длина пароля	8 симв.	6 симв.		
Минимальный срок действия пароля	30 дн.			
Необходимо изменение пароля не меньше, чем в	10 симв.			
Необходимо наличие спецсимволов	Да			
Необходимо наличие строчных и прописных букв	Да			
Необходимо наличие цифр	Да			
oVirt: Минимальная длина пароля	8 симв.	6 симв.		
oVirt: Максимальный срок действия пароля	60 дн.	90 дн.	120 дн.	180 дн.
vCenter: максимальная длина пароля	20			
vSphere: Минимальная длина пароля	8 симв.	6 симв.		
vSphere: Максимальный срок действия пароля	60 дн.	90 дн.	120 дн.	180 дн.
Категория «Политики авторизации»				
Максимальное количество ошибок ввода пароля	4	8	10	
Время блокировки учетно записи в случае ввода неправильных паролей	30 мин.	15 мин.		
Категория «Политики аудита»				
Журнал входов/выходов	Вкл.			
Заносить в журналы ошибки ОС	Вкл.	—		
Журнал контроля приложений СОВ	Вкл.			

Параметры	Значения параметров			
	«Базовая для 1 УЗ»	«Базовая для 2 УЗ»	«Базовая для 3 УЗ»	«Базовая для 4 УЗ»
Системный журнал	Вкл.			
Срок хранения журналов в месяцах	3			
Категория «Политики контроля целостности»				
Проверять целостность прогр. апп. среды при загрузке ОС	Вкл.			
Проверять целостность реестра при загрузке ОС	Вкл.			
Проверять целостность ФС при загрузке ОС	Вкл.			
Периодический контроль ФС	3 ч.			
Виртуальная машина: Проверять целостность при загрузке ОС	Да			
Категория «Режим работы СЗИ»				
Система обнаружения вторжений	Вкл.			
Межсетевой экран	Вкл.			
Категория «Очистка остаточной информации»				
Затирающая последовательность	00 00 00 00			
Количество циклов затираня	1			
Категория «Политики ДСЧ»				
Тестировать ДСЧ при входе	Да			
Число попыток самотестирования ДСЧ	1			