Сергей Кузнецов

Коммерческий директор
Центра защиты информации ГК «Конфидент»

Образование

Окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения по специальности «Инженер-системотехник» (компьютерные системы автоматизации) с красным дипломом.

Опыт работы

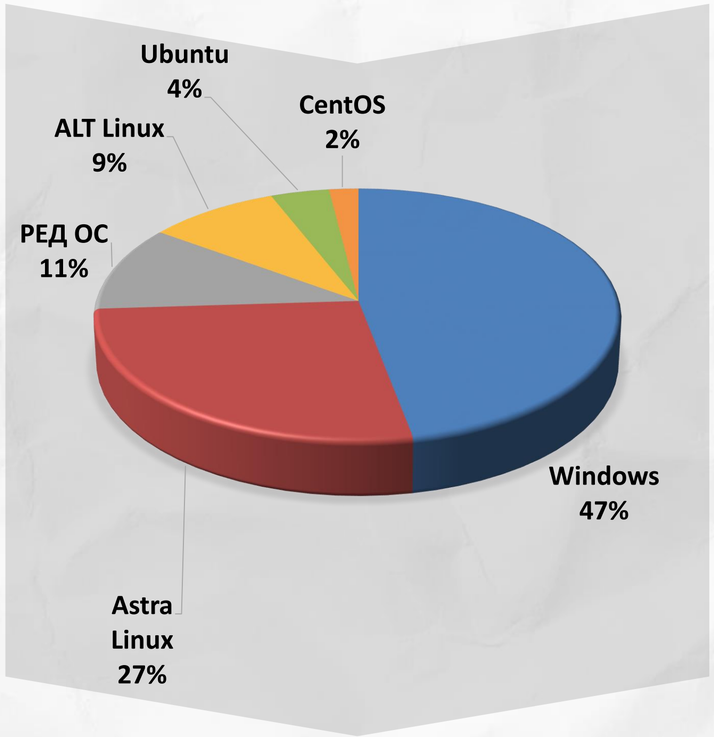
После окончания университета работал в российских и международных ИТ-компаниях. Опыт работы в ИТ-сфере более 30 лет – дистрибуция ПО и оборудования, разработка ПО. Пришел в компанию «Конфидент» в 2011 году. Управляет продажами СЗИ Dallas Lock через партнеров ГК «Конфидент» конечным пользователям – органам власти, организациям ВПК, предприятиям, финансовым организациям и т. п.

Награды

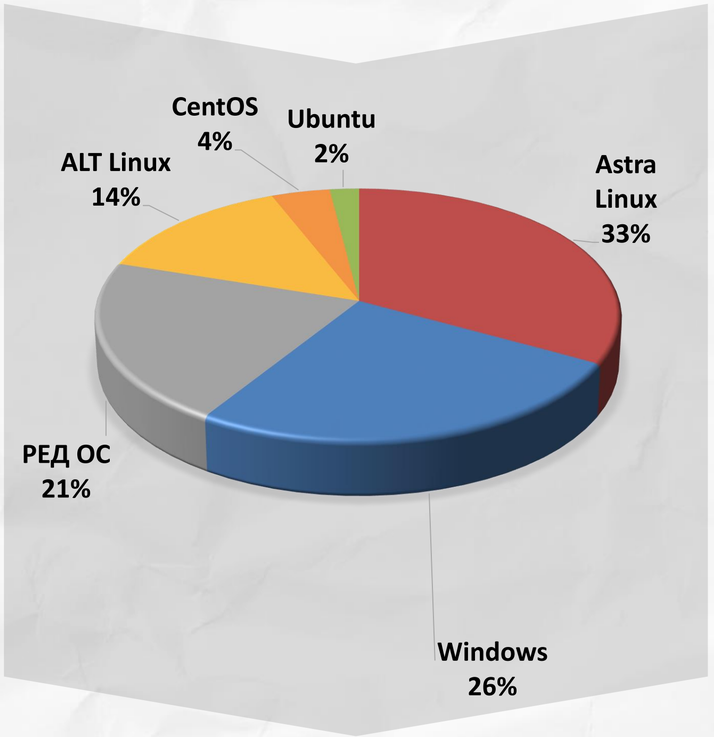
Медаль ФСТЭК России «За укрепление государственной системы защиты информации» II степени.

Актуальные вопросы защиты информации с использованием СЗИ Dallas Lock

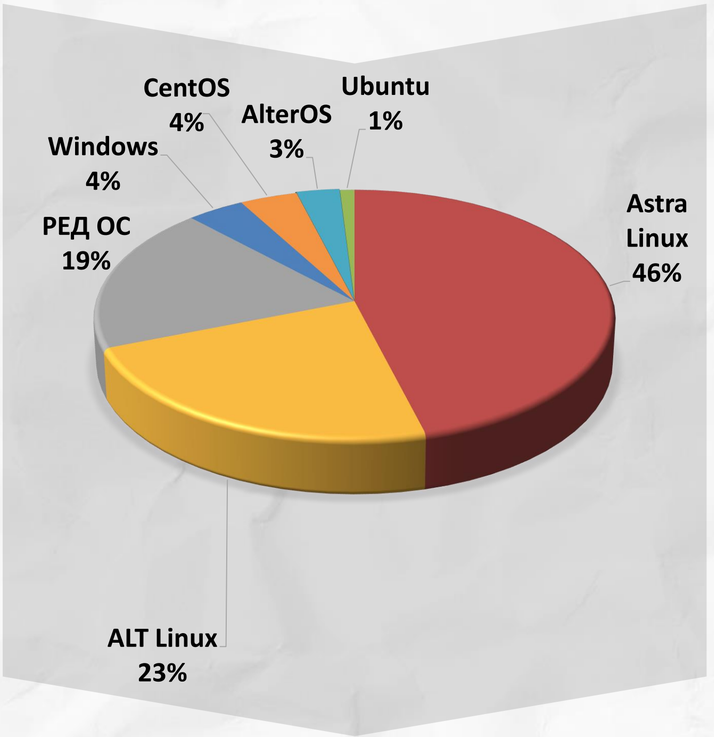
Востребованность ОС в проектах по защите информации в 2021, 2022, 2023 (прогноз)



2021



2022

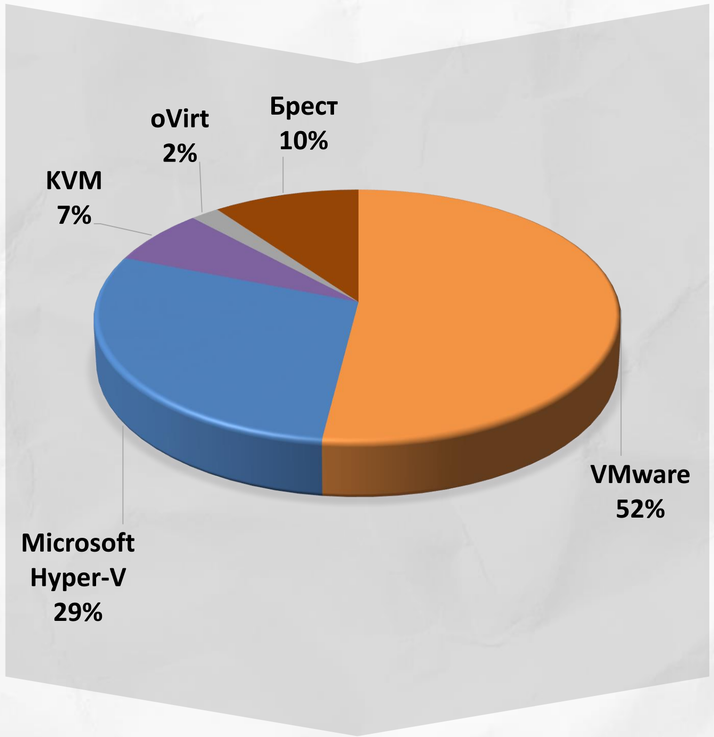


2023
(прогноз)

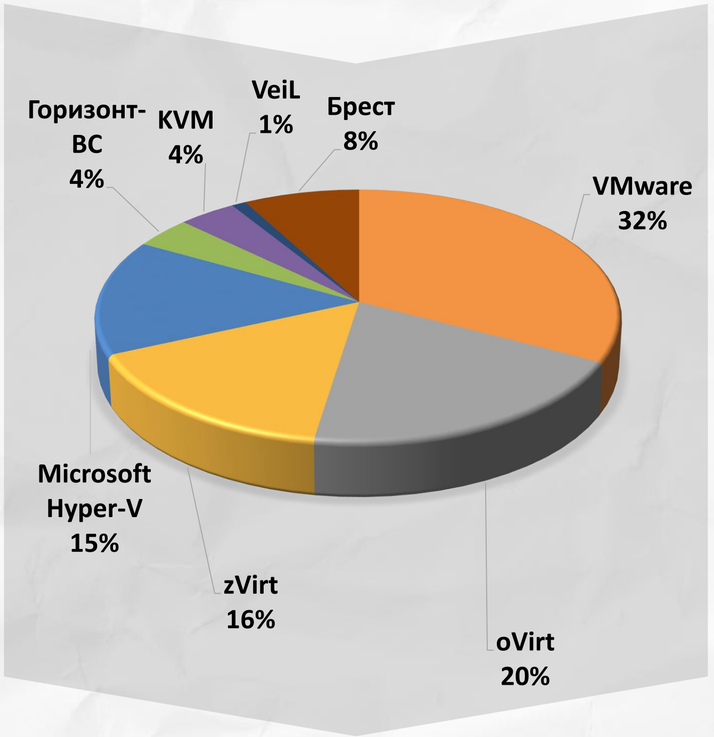
Результаты опроса ключевых партнёров ЦЗИ ГК «Конфидент», январь – февраль 2023 г.

КОНФИДЕНТ®
ГРУППА КОМПАНИЙ

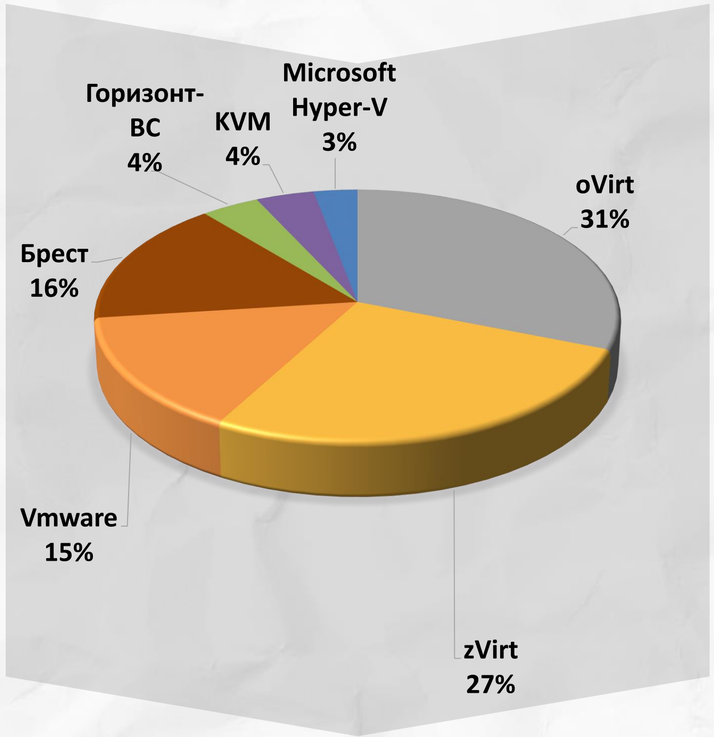
Востребованность систем виртуализации в проектах по защите информации в 2021, 2022, 2023 (прогноз)



2021



2022



2023
(прогноз)

Результаты опроса ключевых партнёров ЦЗИ ГК «Конфидент», январь – февраль 2023 г.

КОНФИДЕНТ®
ГРУППА КОМПАНИЙ

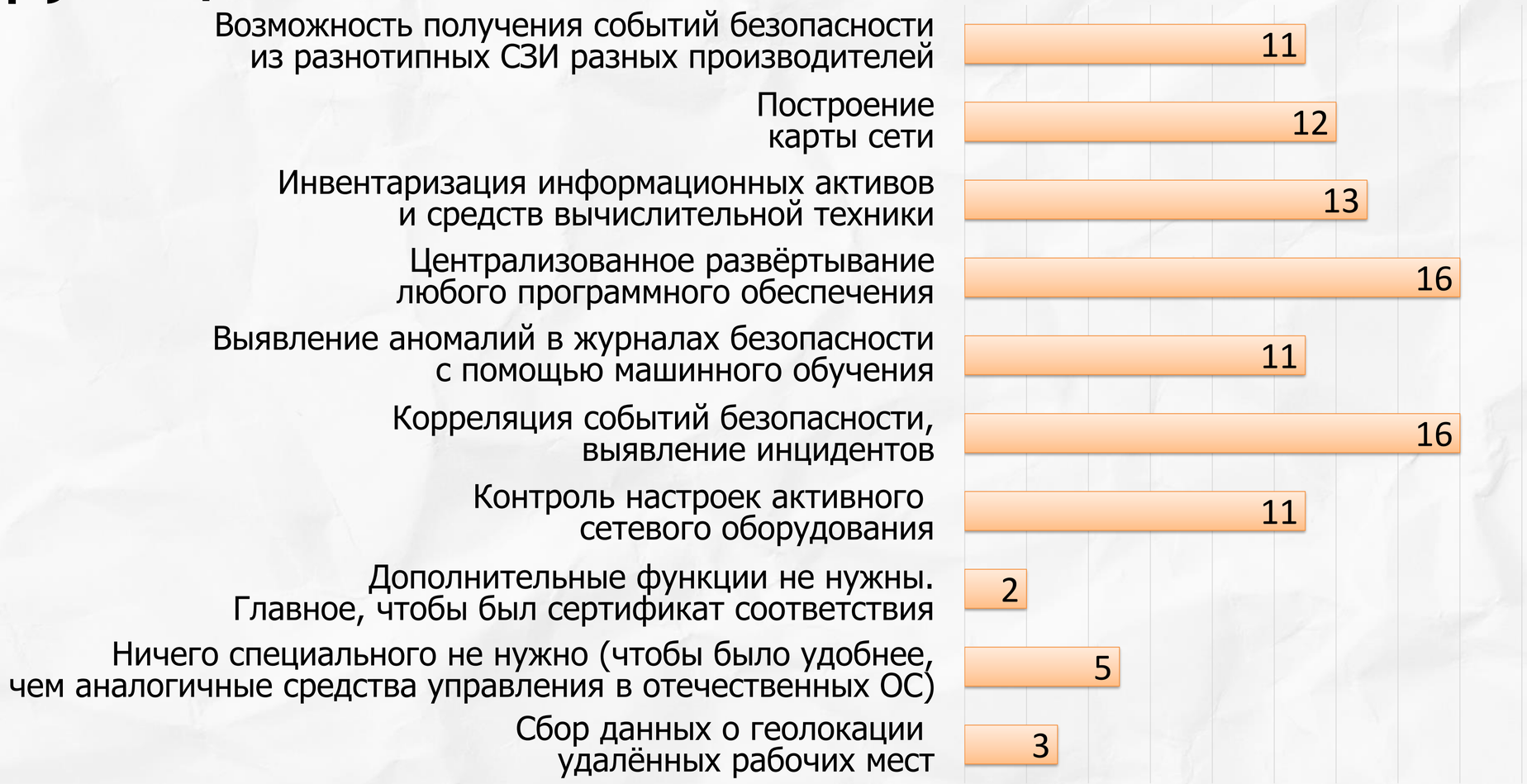
Тренды импортозамещения

Защита рабочих станций и серверов	Windows	→ Linux	→ Отечественные операционные системы
Защита среды виртуализации	VMware, Hyper-V	→ KVM, oVirt	→ Отечественные платформы виртуализации

Выводы

1. Процесс перевода ИТ-инфраструктур заказчиков на отечественные решения близок к завершению
2. Некоторые сегменты ИТ-инфраструктуры остаются реализованными на старых решениях/платформах

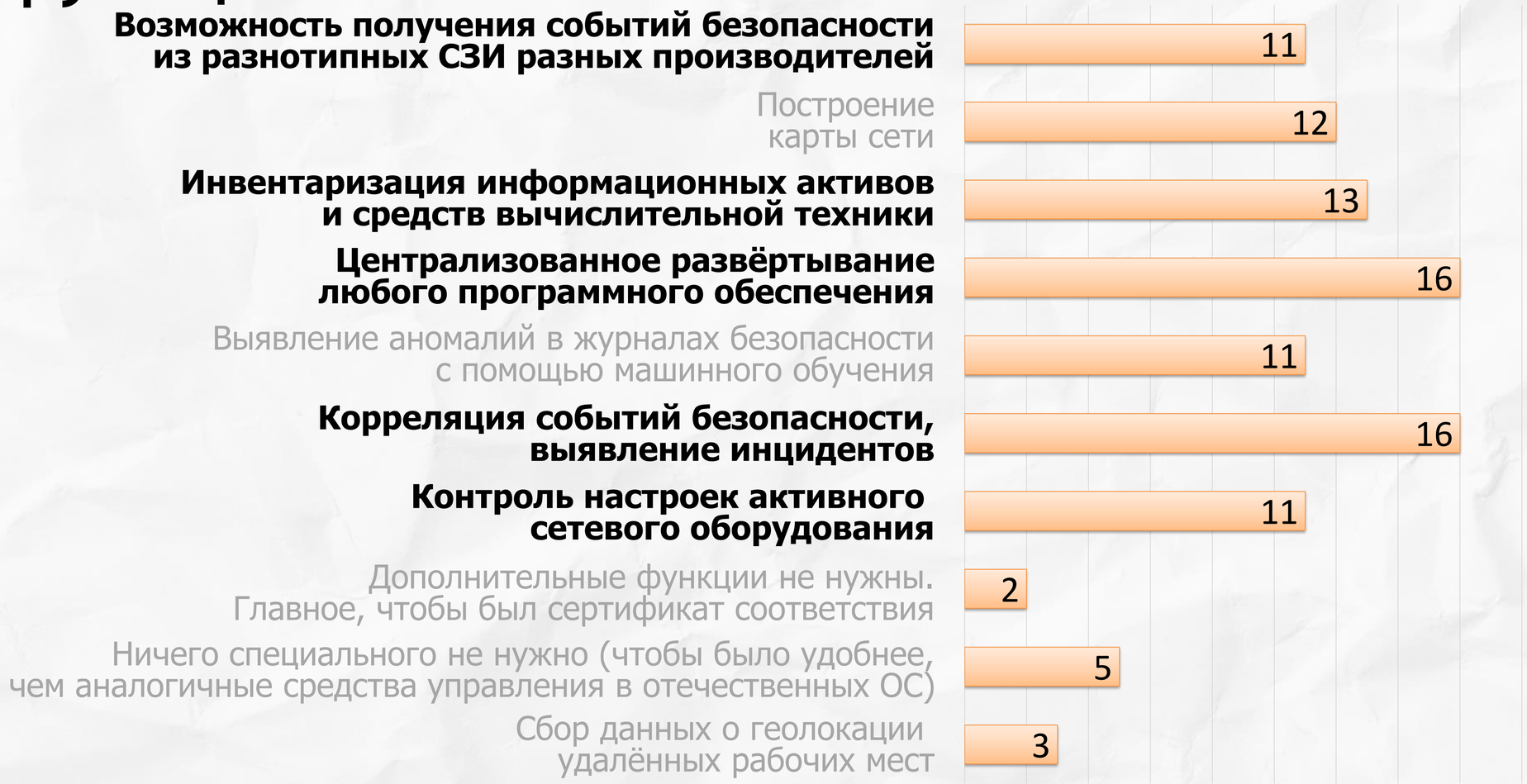
Востребованные у заказчиков дополнительные функции СЗИ



Результаты опроса авторизованных пользователей портала dallaslock.ru, сентябрь 2022 – январь 2023 г.

КОНФИДЕНТ® ГРУППА КОМПАНИЙ

Востребованные у заказчиков дополнительные функции СЗИ



Результаты опроса авторизованных пользователей портала dallaslock.ru, сентябрь 2022 – январь 2023 г.

КОНФИДЕНТ® ГРУППА КОМПАНИЙ

Выводы

1. Процесс перевода ИТ-инфраструктур заказчиков на отечественные решения близок к завершению
2. Некоторые сегменты ИТ-инфраструктуры остаются реализованными на старых решениях/платформах
3. Заказчики предъявляют повышенные требования к централизованному управлению ИБ и ИТ
4. Заказчики отмечают недостаток встроенных в ОС/платформы защитных механизмов

Система защиты информации должна отвечать новым вызовам

Центр управления

Современные требования к Центру управления информационной безопасностью:

- поддержка сертифицированных отечественных ОС
- управление клиентскими частями под Windows и Linux, СДЗ, поддержка российских ОС, а также возможность удалённого подключения к ним
- возможность получать журналы с незащищённых АРМ
- наличие встроенного VNC-клиента
- работа за NAT (Network Address Translation)
- бесперебойная работа в больших инфраструктурах и при «слабом» сетевом соединении
- дополнительные возможности, помимо встроенных в ОС/платформу

Единый центр управления Dallas Lock

ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ DALLAS LOCK

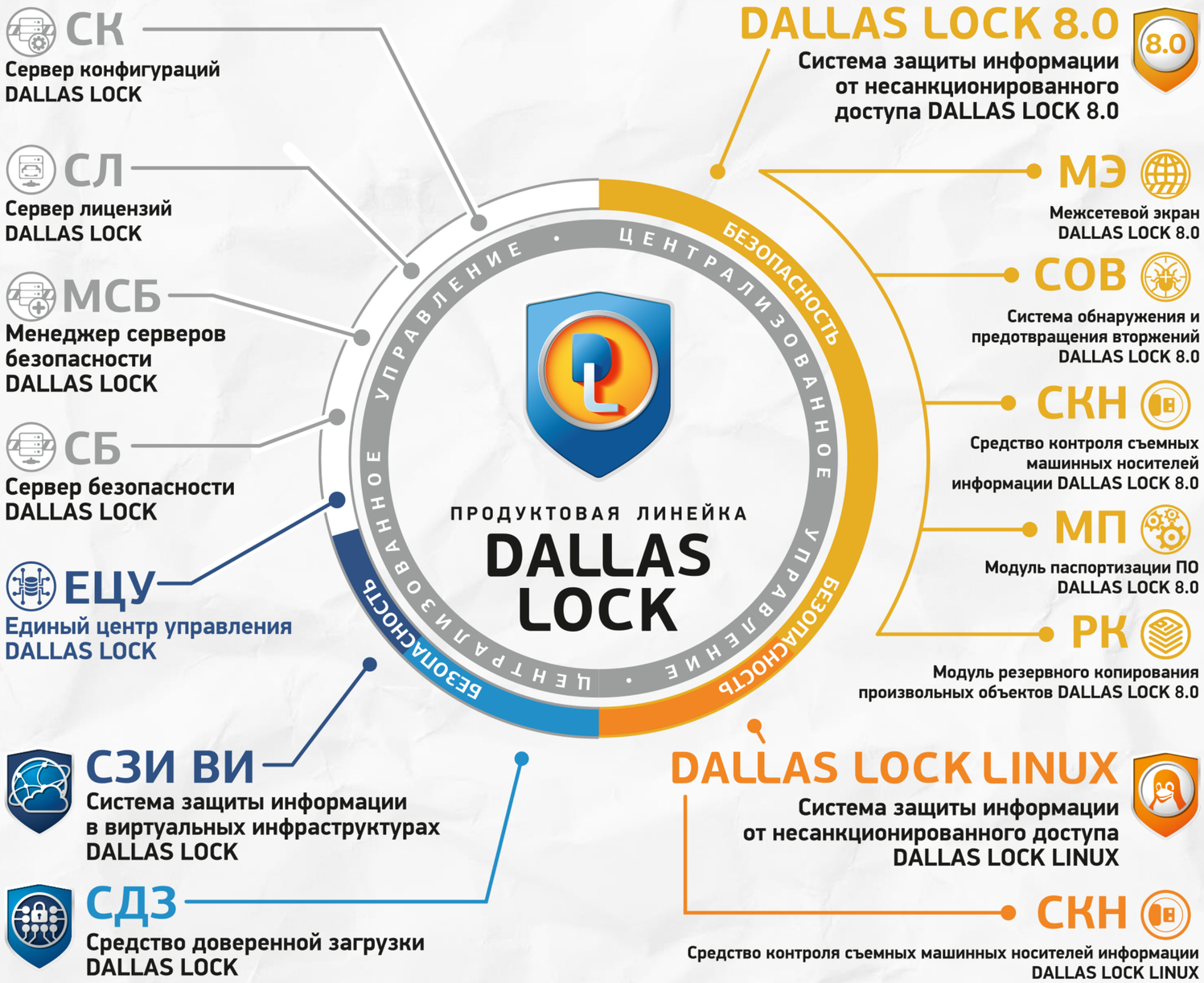
Кросс-платформенное решение для централизованного управления ИБ предприятия

1. **Поддержка российских ОС, в т ч сертифицированных ФСТЭК России**
2. **Управление СЗИ под Windows, Linux, российскими ОС, в т ч СДЗ**
3. **Работа за NAT (Network Address Translation)**
4. **Управление не только СЗИ Dallas Lock – агент Windows/Linux/рос. ОС**

Иерархическая структура доменов безопасности, контроль целостности настроек сетевого оборудования, не требователен к ресурсам

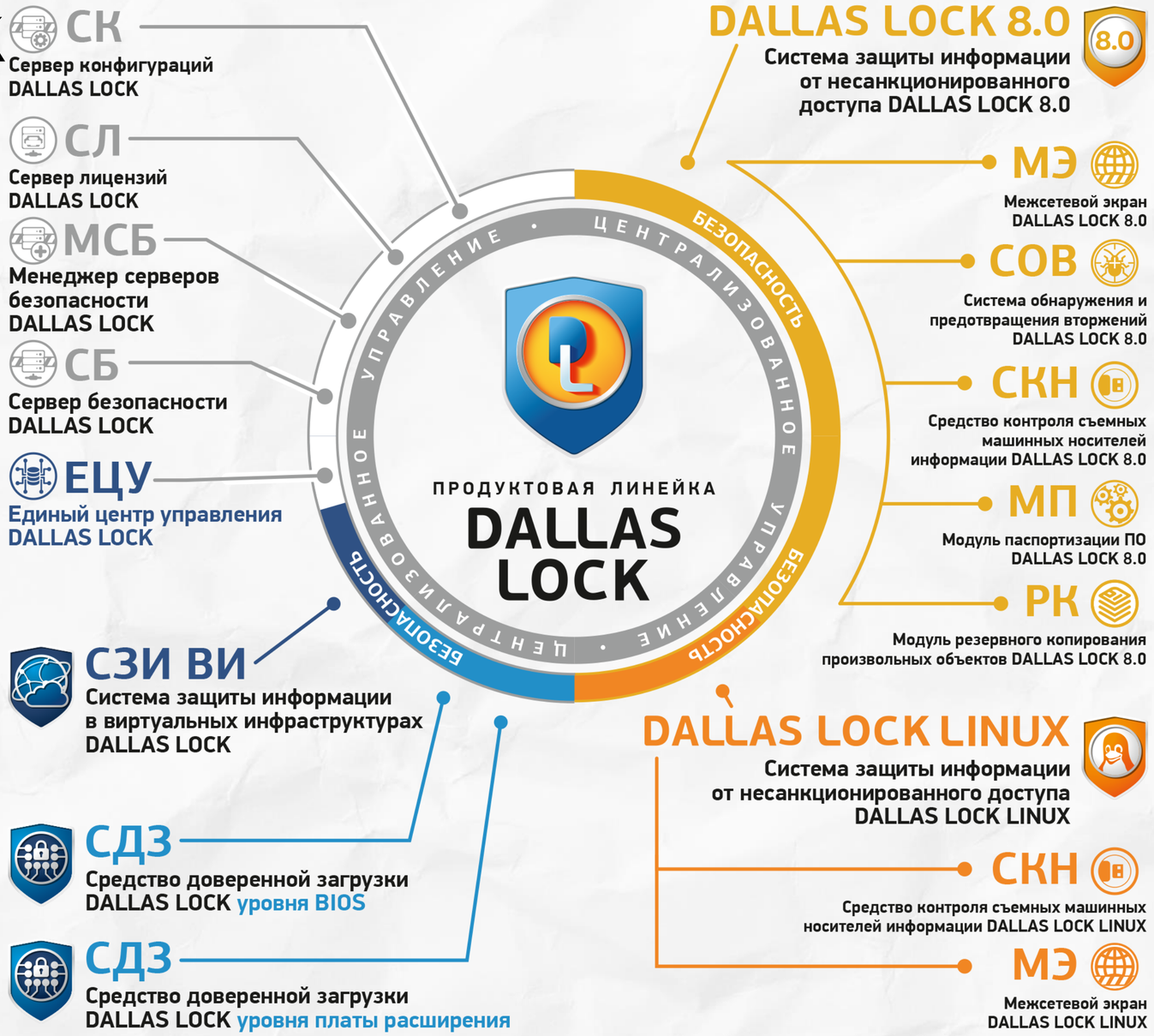
КОНФИДЕНТ® ГРУППА КОМПАНИЙ

Dallas Lock



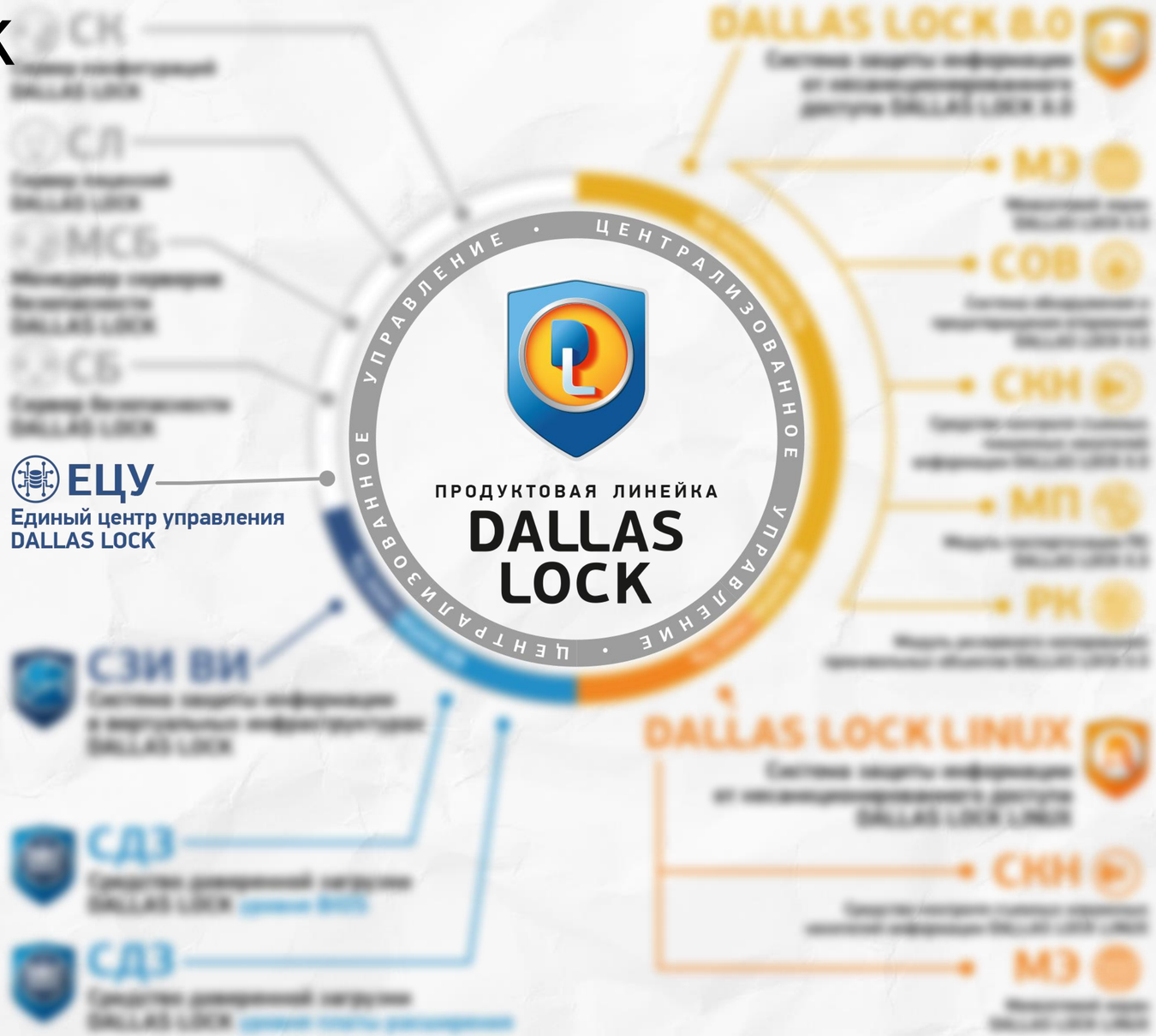
КОНФИДЕНТ®
ГРУППА КОМПАНИЙ

Dallas Lock

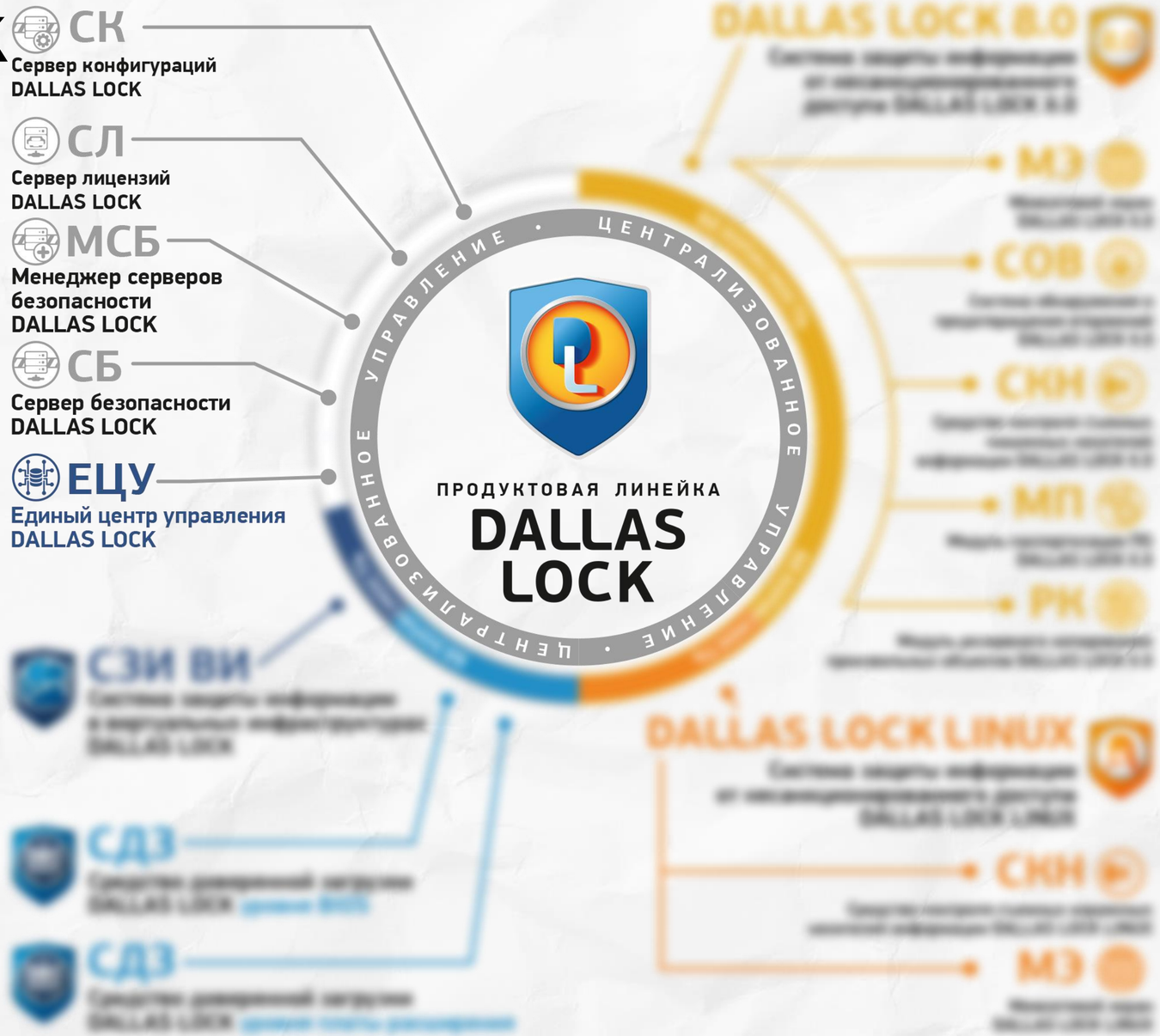


КОНФИДЕНТ®
ГРУППА КОМПАНИЙ

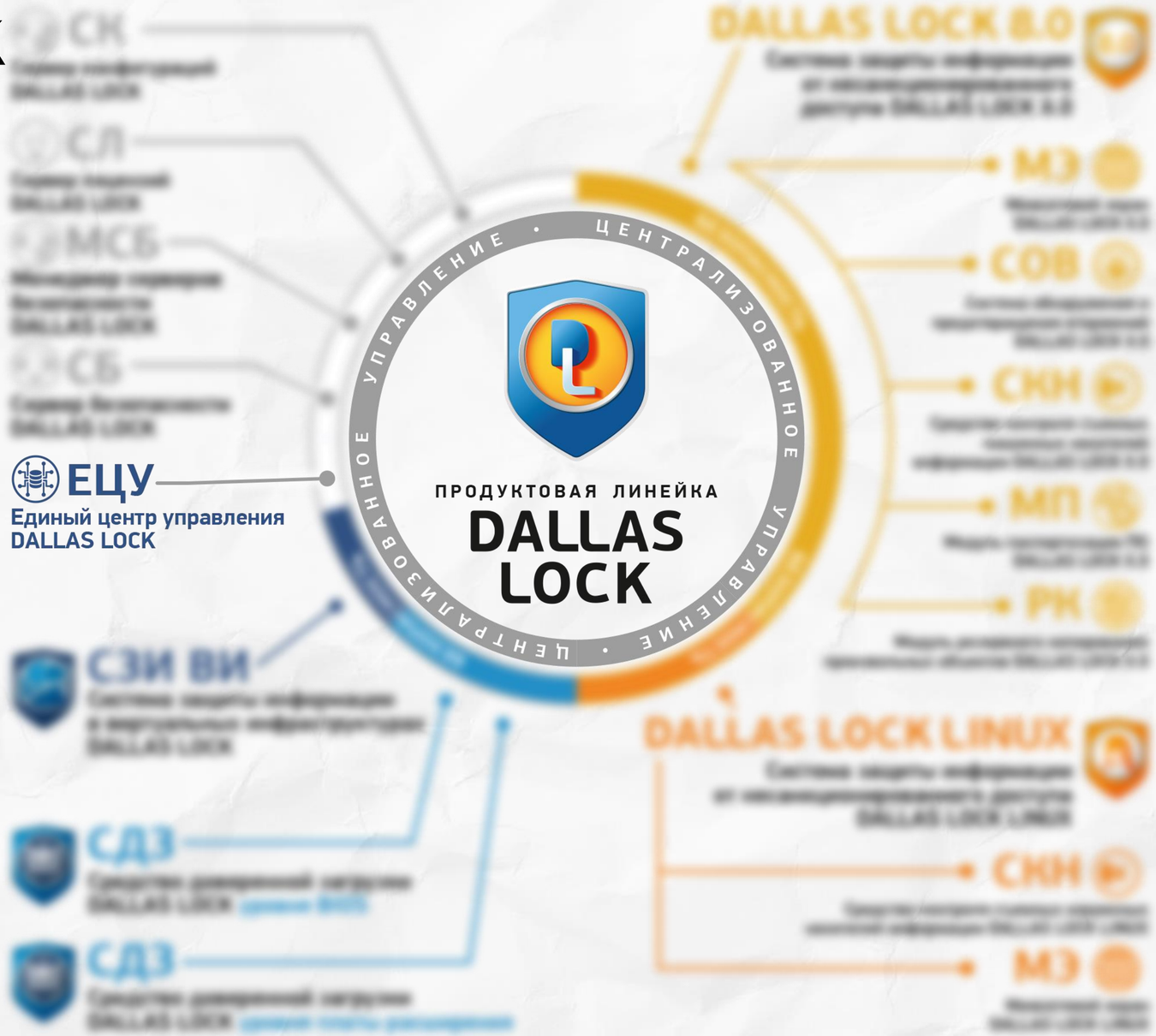
Dallas Lock


ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ
ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ
ПРОДУКТОВАЯ ЛИНЕЙКА
DALLAS LOCK
ЕЦУ
Единый центр управления DALLAS LOCK
DALLAS LOCK 8.0
DALLAS LOCK LINUX

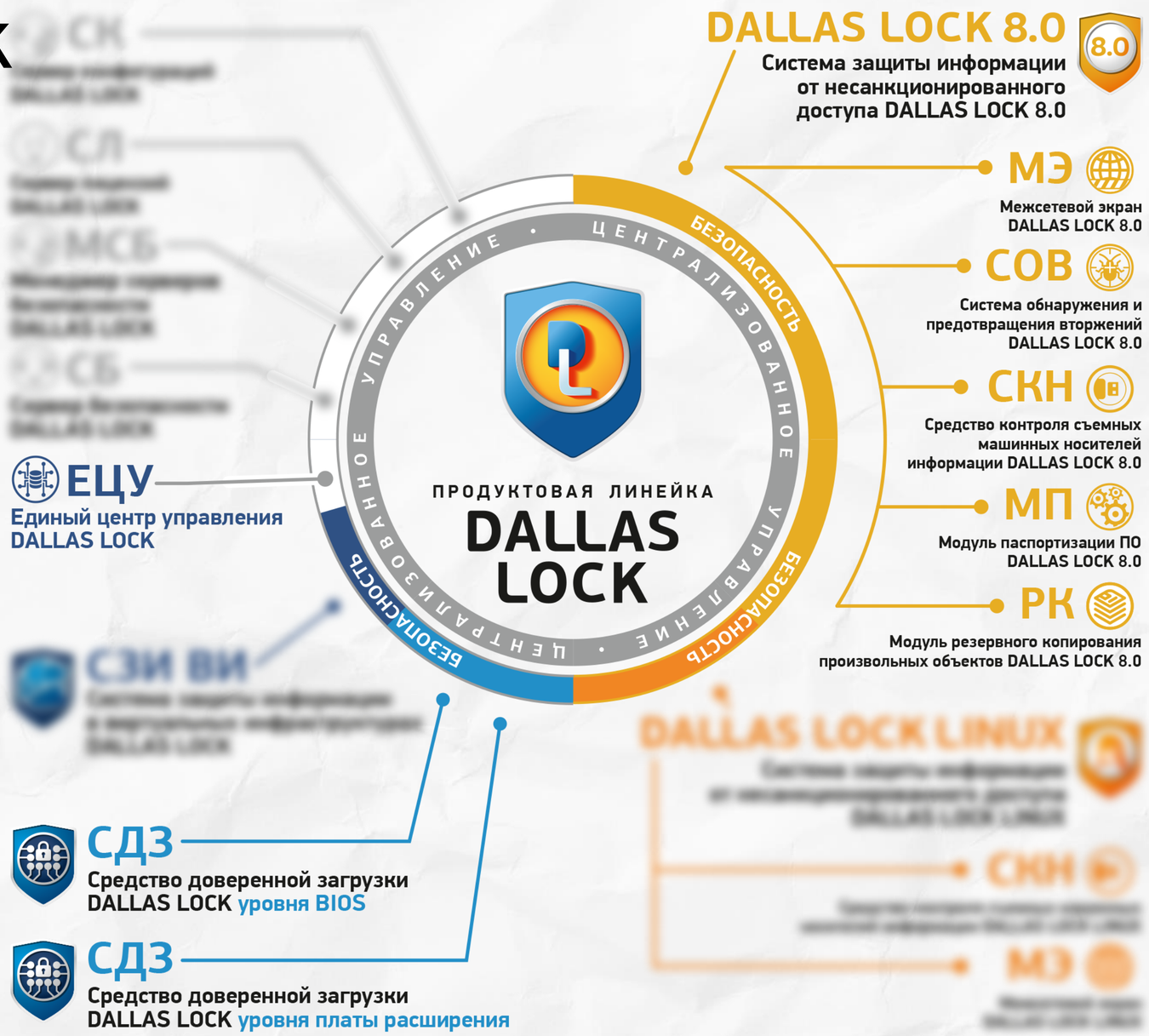
Dallas Lock


СК
Сервер конфигураций
DALLAS LOCK
СЛ
Сервер лицензий
DALLAS LOCK
МСБ
Менеджер серверов
безопасности
DALLAS LOCK
СБ
Сервер безопасности
DALLAS LOCK
ЕЦУ
Единый центр управления
DALLAS LOCK
ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ
ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ
ПРОДУКТОВАЯ ЛИНЕЙКА
DALLAS LOCK
DALLAS LOCK 8.0
СЗИ ВИ
СДЗ
СДЗ
DALLAS LOCK LINUX

Dallas Lock


ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ
ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ
ПРОДУКТОВАЯ ЛИНЕЙКА
DALLAS LOCK
ЕЦУ
Единый центр управления DALLAS LOCK
DALLAS LOCK 8.0
DALLAS LOCK LINUX

Dallas Lock



КОНФИДЕНТ®
ГРУППА КОМПАНИЙ

Единый центр управления Dallas Lock

ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ DALLAS LOCK

Сертификаты ЕЦУ

ФСТЭК России № 2720 от 25.09.2012 (в составе объекта СЗИ НСД Dallas Lock 8.0-К)

МО России № 5695 от 31.03.2022 (в составе объекта СДЗ, ГТ)

Реестр ПО

Приказ Минцифры России № 768 от 27.07.2021 (запись в реестре № 11185 от 29.07.2021 г.)

Минцифры России

Единый центр управления Dallas Lock

ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ DALLAS LOCK

Сертификация ЕЦУ в процессе

Май 2023

ФСТЭК России № 2945 от 16.08.2013

в составе СЗИ НСД Dallas Lock 8.0-C, ГТ, поддержка Guardant 2.0, среда эмуляции, резервное копирование

Июнь 2023

ФСТЭК России № 3594 от 04.07.2016

в составе объекта СЗИ НСД Dallas Lock Linux

Июль 2023

ФСТЭК России № 3666 от 25.11.2016

в составе СДЗ, ГТ, поддержка Guardant 2.0

Ноябрь 2023

ФСТЭК России

в составе СДЗ Dallas Lock уровня BIOS, ГТ

Единый центр управления Dallas Lock

ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ DALLAS LOCK

Совместимость

Astra Linux Common Edition (Орел) 2.12;
Astra Linux Special Edition (Смоленск) 1.6;
Astra Linux Special Edition 1.7;
Альт Рабочая Станция 9.x;
Альт Рабочая Станция 10.0, 10.1;
Альт Рабочая Станция K 10.0, 10.1;
Альт Сервер 9.x;
Альт Сервер 10.0, 10.1;
РЕД ОС 7.3 Муром;
Windows 8.1 (Core, Pro, Enterprise);
Windows 10/11 (Enterprise, Education, Pro, Home);
Windows Server 2012 / 2012 R2 (Foundation, Essentials, Standard, Datacenter);
Windows Server 2016 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server);
Windows Server 2019 (Essentials, Standard, Datacenter);
Windows Server 2022 (Standard, Datacenter);
Debian 10.x; Debian 11.x;
CentOS 7.x; Red Hat Enterprise Linux Server 7.x;
Ubuntu 18.04 LTS; Ubuntu 20.04 LTS.

КОНФИДЕНТ® ГРУППА КОМПАНИЙ

Единый центр управления Dallas Lock

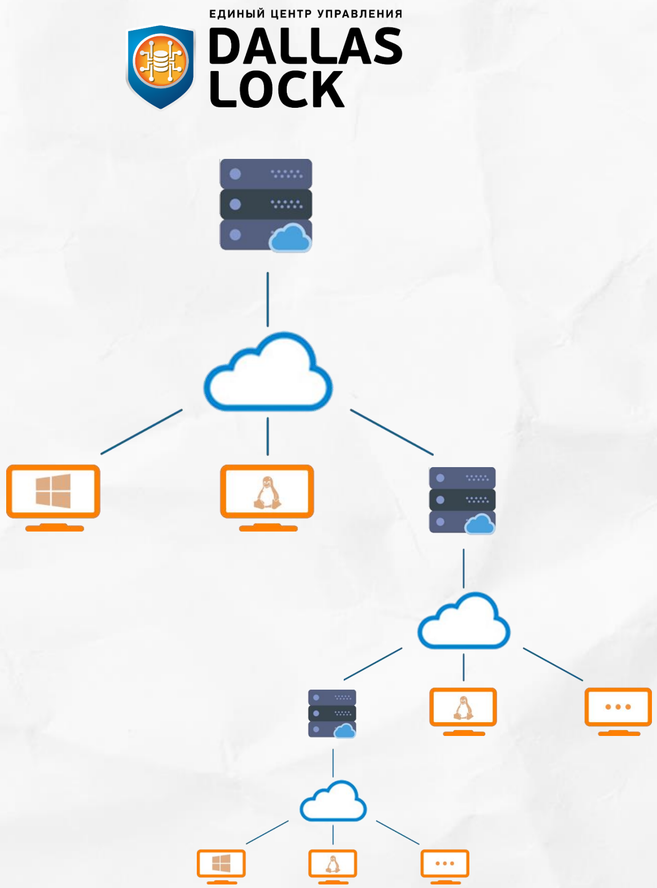
ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ
DALLAS LOCK

Централизованное управление – основные функции

- управление СЗИ Dallas Lock 8.0-K/8.0-C (Windows),
- управление СЗИ Dallas Lock Linux
- управление СДЗ Dallas Lock (уровня палаты и уровня BIOS)
- управление ТС с СЗИ, расположенными за NAT
- иерархия ДБ с наследованием
- кластеризация ДБ
- управление пользователями (группами пользователей) на ТС с СЗИ
- интеграция учетных записей (групп) с LDAP;
- централизованный сбор журналов
- графическое представление информации об инцидентах на разных уровнях иерархии домена
- …

КОНФИДЕНТ®
ГРУППА КОМПАНИЙ

Единый центр управления Dallas Lock



Централизованное управление – основные функции

- экспорт инцидентов в SIEM-систему
- контроль целостности программно-аппаратной среды, файловой системы, системного реестра
- управление аппаратными идентификаторами
- сканирование сети – поиск ТС с СЗИ по IP-адресу
- удаленная установка/обновление/удаление СЗИ в составе ДБ
- возможность переносить клиентов и их настройки из других средств централизованного управления
- объединение нескольких ДБ в единую логическую единицу, имеющую структуру вложенности со связями типа «родитель-потомок»
- …

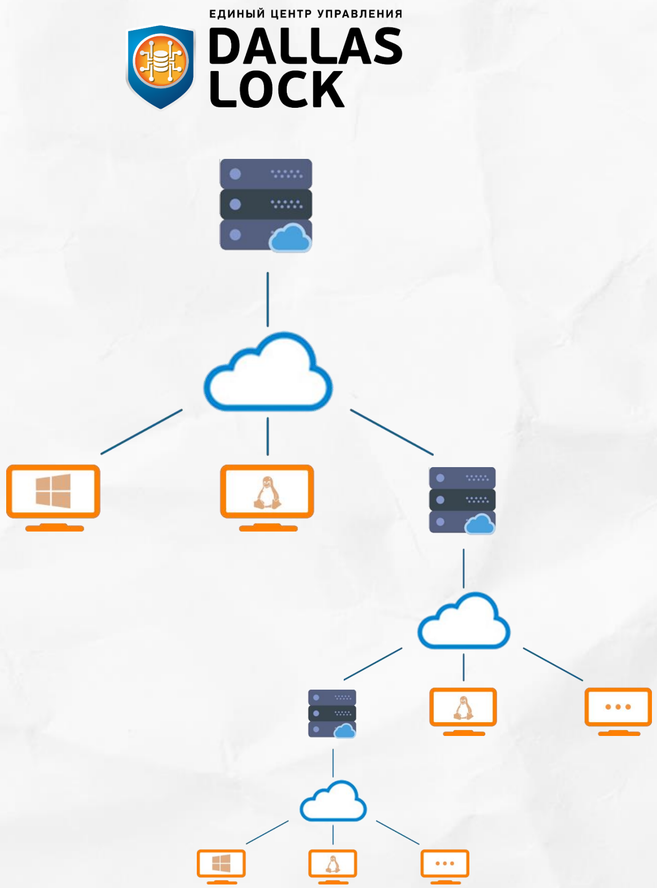
Единый центр управления Dallas Lock

ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ
DALLAS LOCK

Контроль и управление сетевым оборудованием

- сканирование сети обнаружения оборудования (SNMP и SSH)
- ввод/вывод сетевого оборудования в/из домена безопасности
- удаленное включение сетевого оборудования
- настройка параметров, берущихся под контроль
- получение отчета о конфигурации сетевого оборудования
- применение конфигураций
- контроль изменений конфигурации сетевого оборудования
- прием сообщений по протоколу Syslog
- сигнализация о нарушении целостности

Единый центр управления Dallas Lock

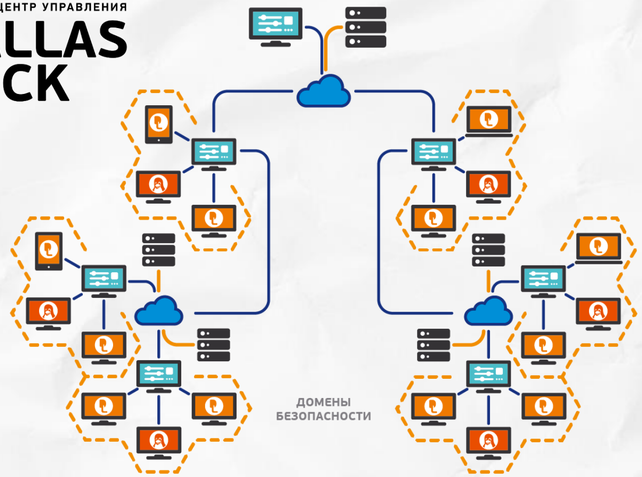


Удаленное управление без установленных СЗИ Dallas Lock

- удаленное подключение к ТС с доступом к рабочему столу пользователя (VNC) с возможностью управления настройками удаленного подключения
- удаленная перезагрузка/выключение ТС
- сбор журналов с ТС с возможностью настройки типов собираемых событий
- сбор отчетов об аппаратном и программном обеспечении с ТС
- сравнение отчетов с эталоном и сигнализация

ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ
DALLAS LOCK

Единый центр управления Dallas Lock



Сценарий 1: Инвентаризация активов

Сценарий 2: Оповещение об инцидентах ИБ (консоль, email)

Сценарий 3: Управление пользователями/группами на СЗИ Dallas Lock

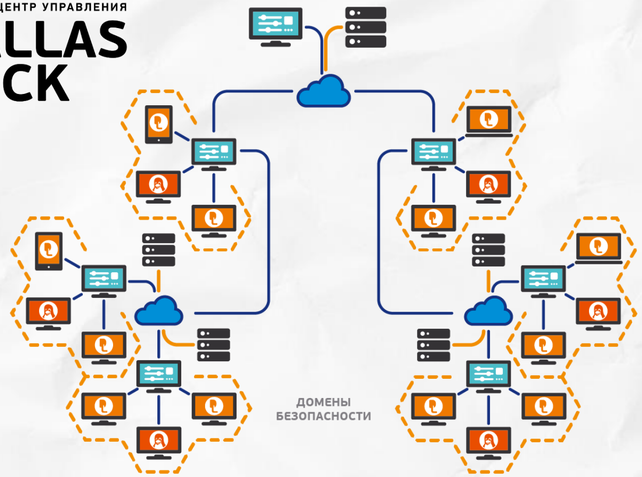
Сценарий 4: Удаленное выключение/перезагрузка ТС (агент ЕЦУ / клиент СЗИ Dallas Lock)

Сценарий 5: Удаленное управление ТС (агент ЕЦУ / клиент СЗИ Dallas Lock)

Сценарий 6: Контроль сетевого оборудования (без агентов/клиентов СЗИ Dallas Lock)

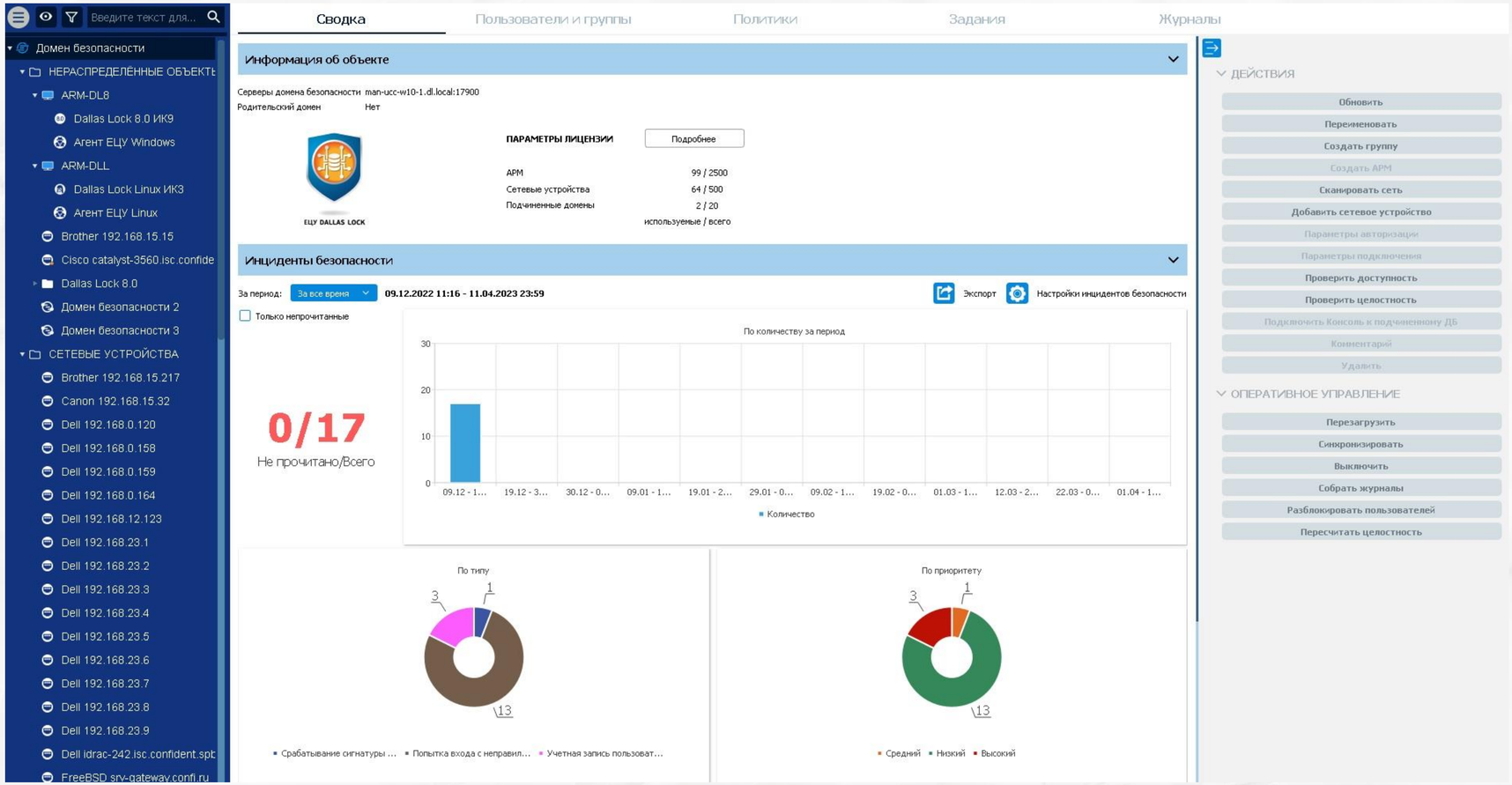
КОНФИДЕНТ®
ГРУППА КОМПАНИЙ

Единый центр управления Dallas Lock

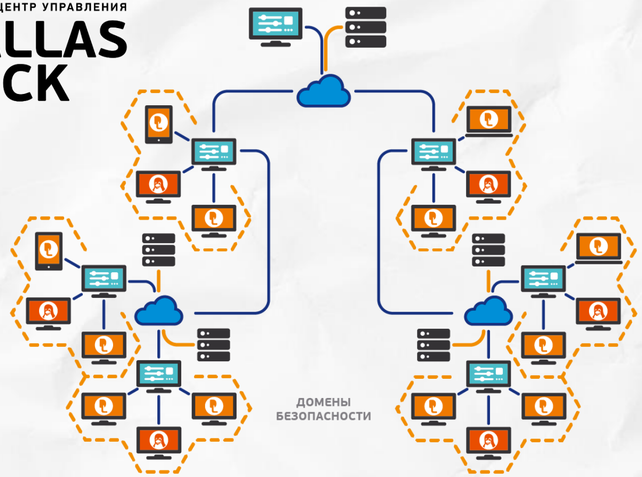


Сценарий 1:

Инвентаризация активов

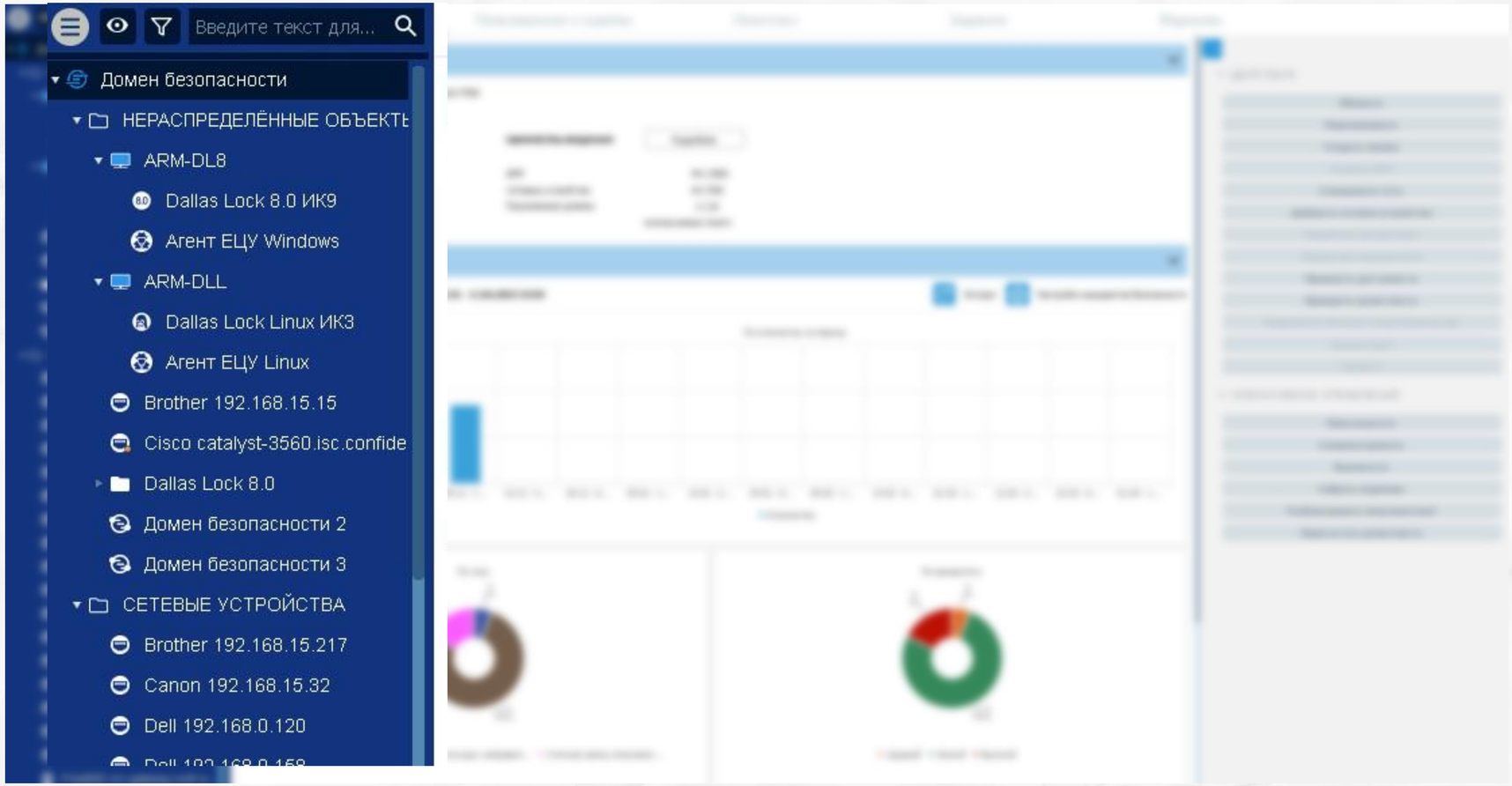


Единый центр управления Dallas Lock



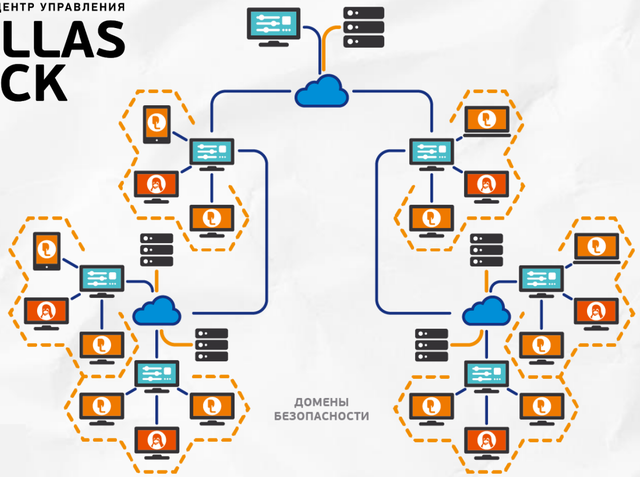
Сценарий 1:

Инвентаризация активов



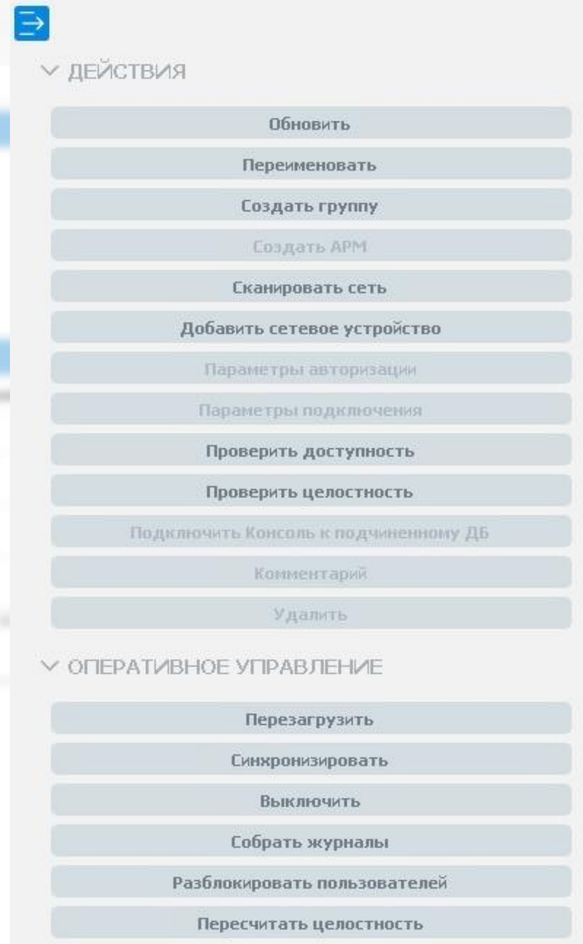
ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ
DALLAS LOCK

Единый центр управления Dallas Lock



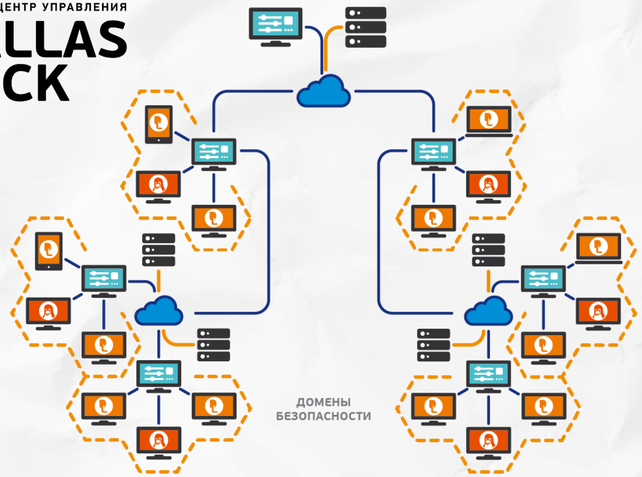
Сценарий 1:

Инвентаризация активов



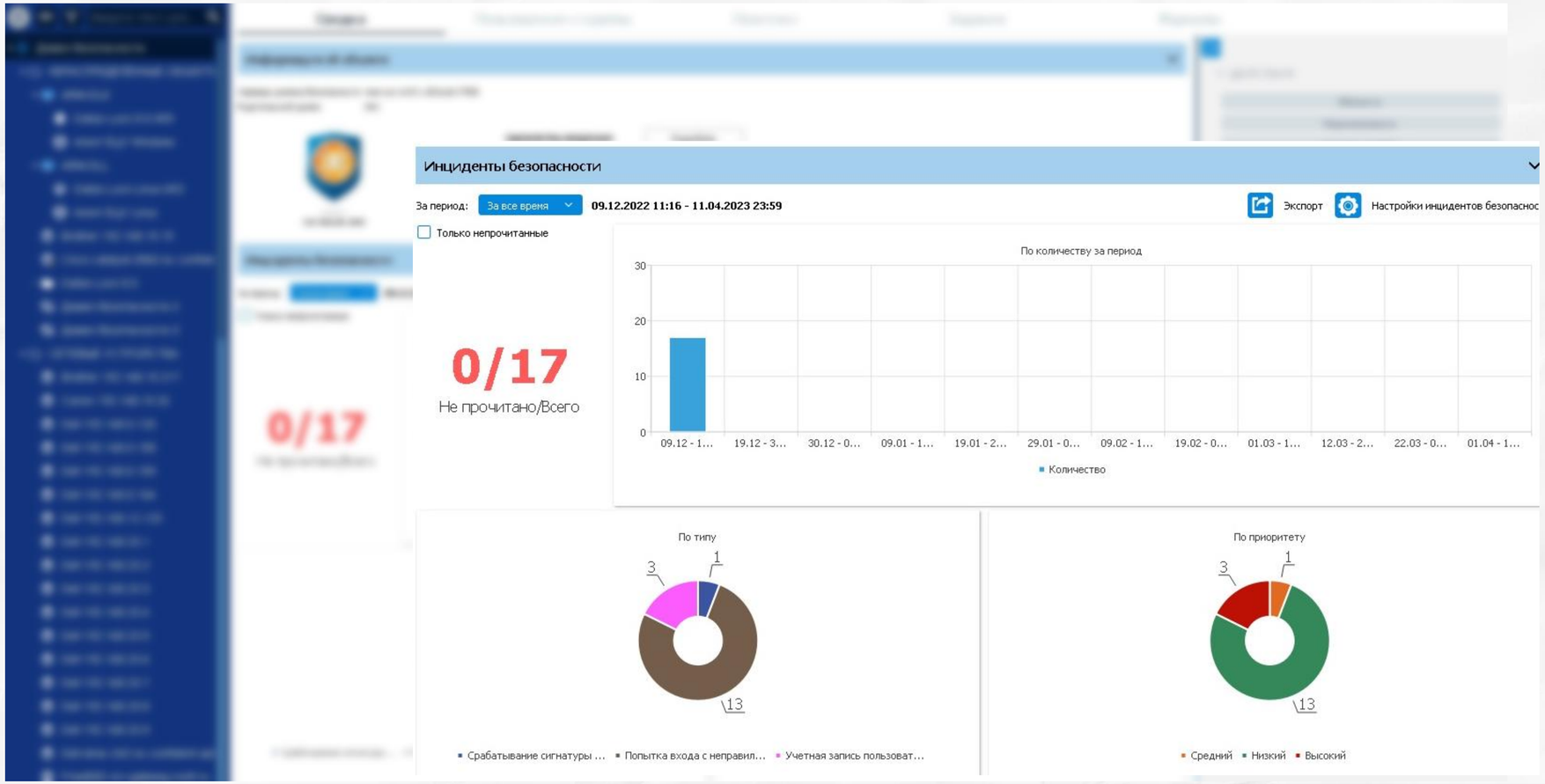
КОНФИДЕНТ®
ГРУППА КОМПАНИЙ

Единый центр управления Dallas Lock

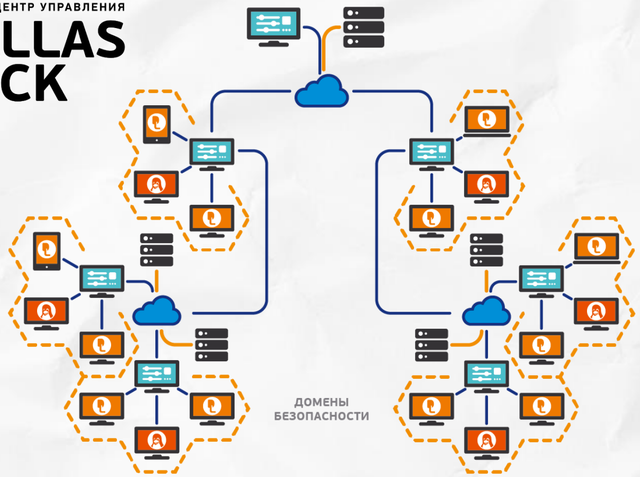


Сценарий 2:

Оповещение об инцидентах ИБ (консоль, email)

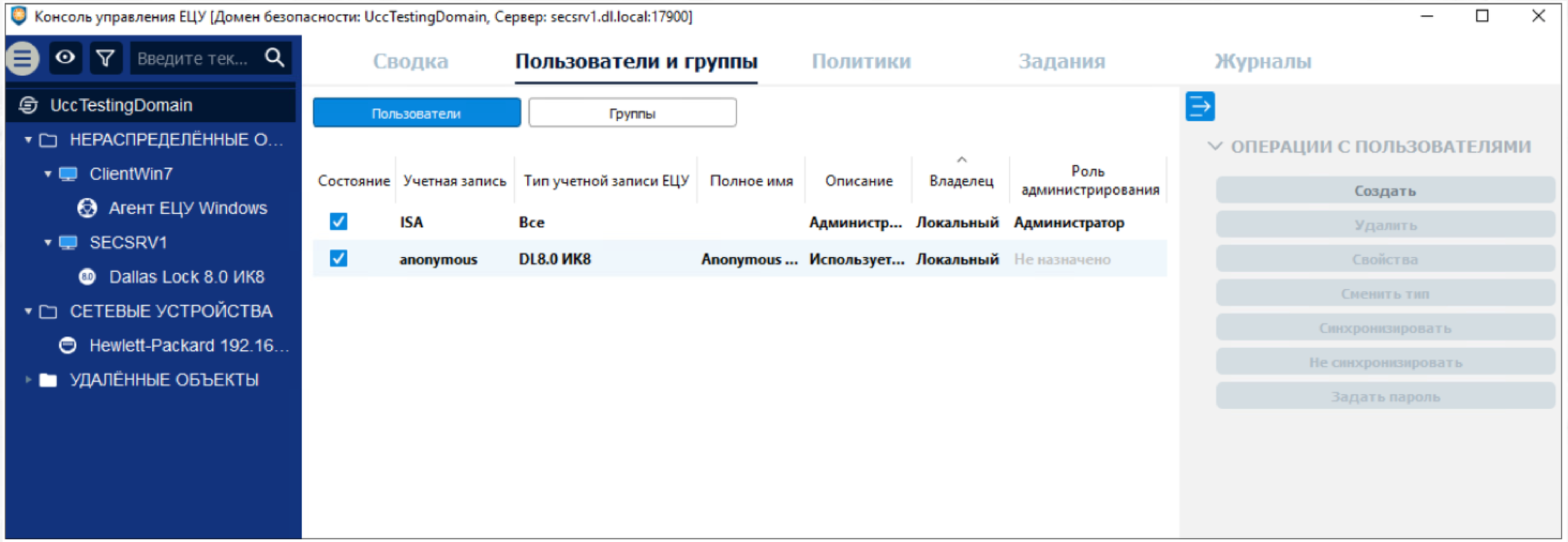


Единый центр управления Dallas Lock

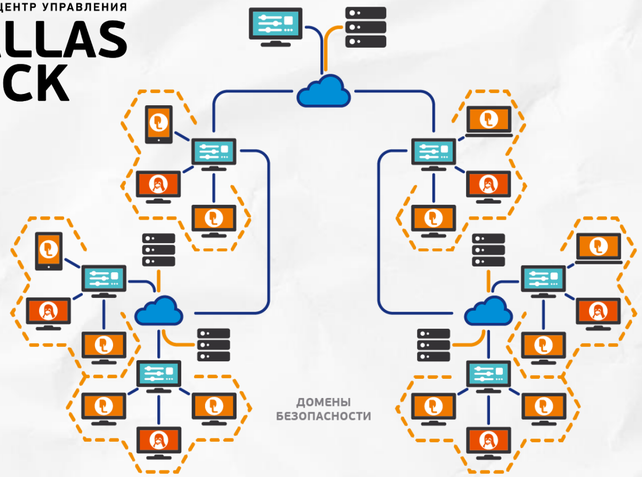


Сценарий 3:

Управление пользователями/группами на СЗИ Dallas Lock

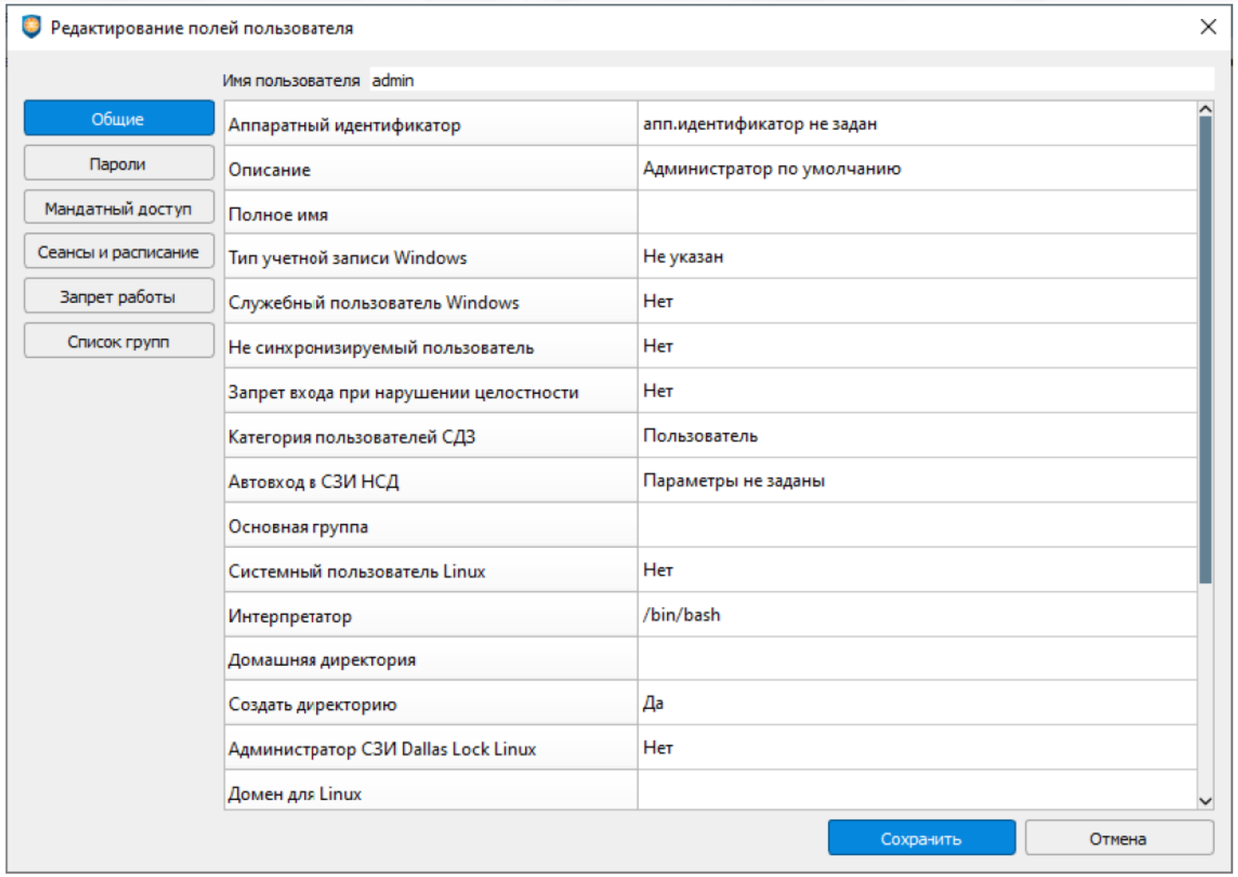


Единый центр управления Dallas Lock

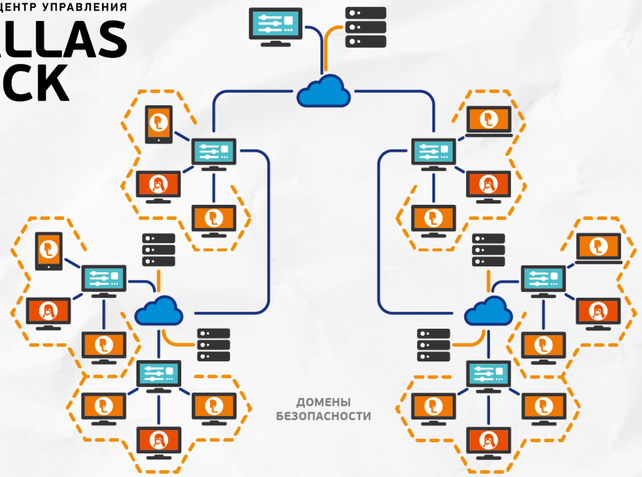


Сценарий 3:

Управление пользователями/группами на СЗИ Dallas Lock

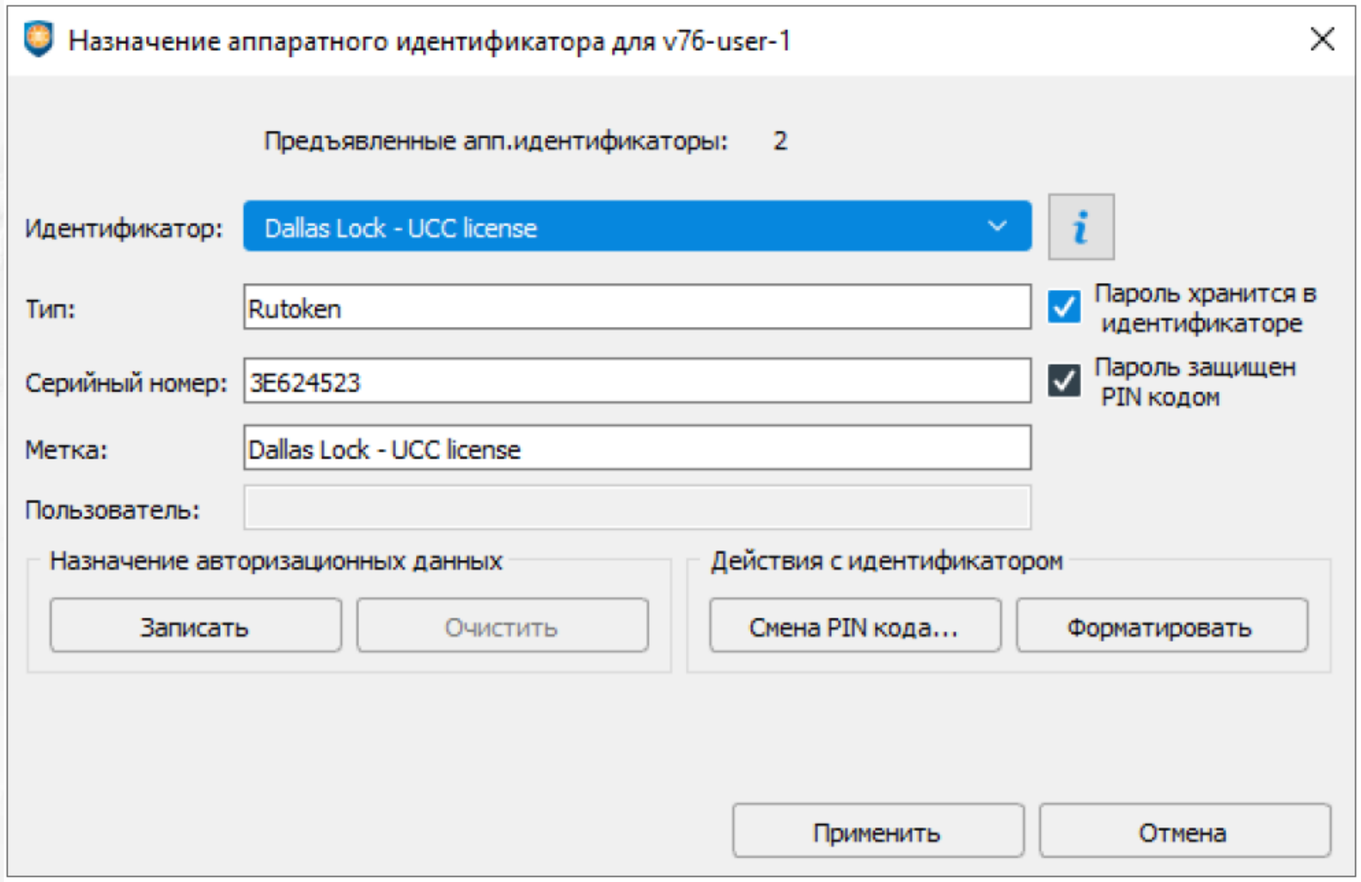


Единый центр управления Dallas Lock



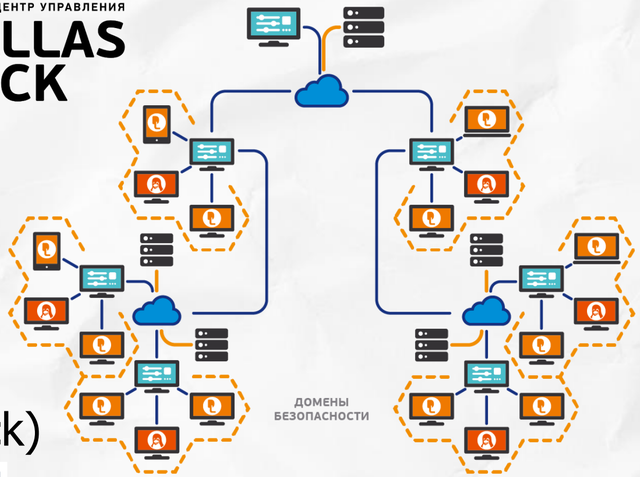
Сценарий 3:

Управление пользователями/группами на СЗИ Dallas Lock



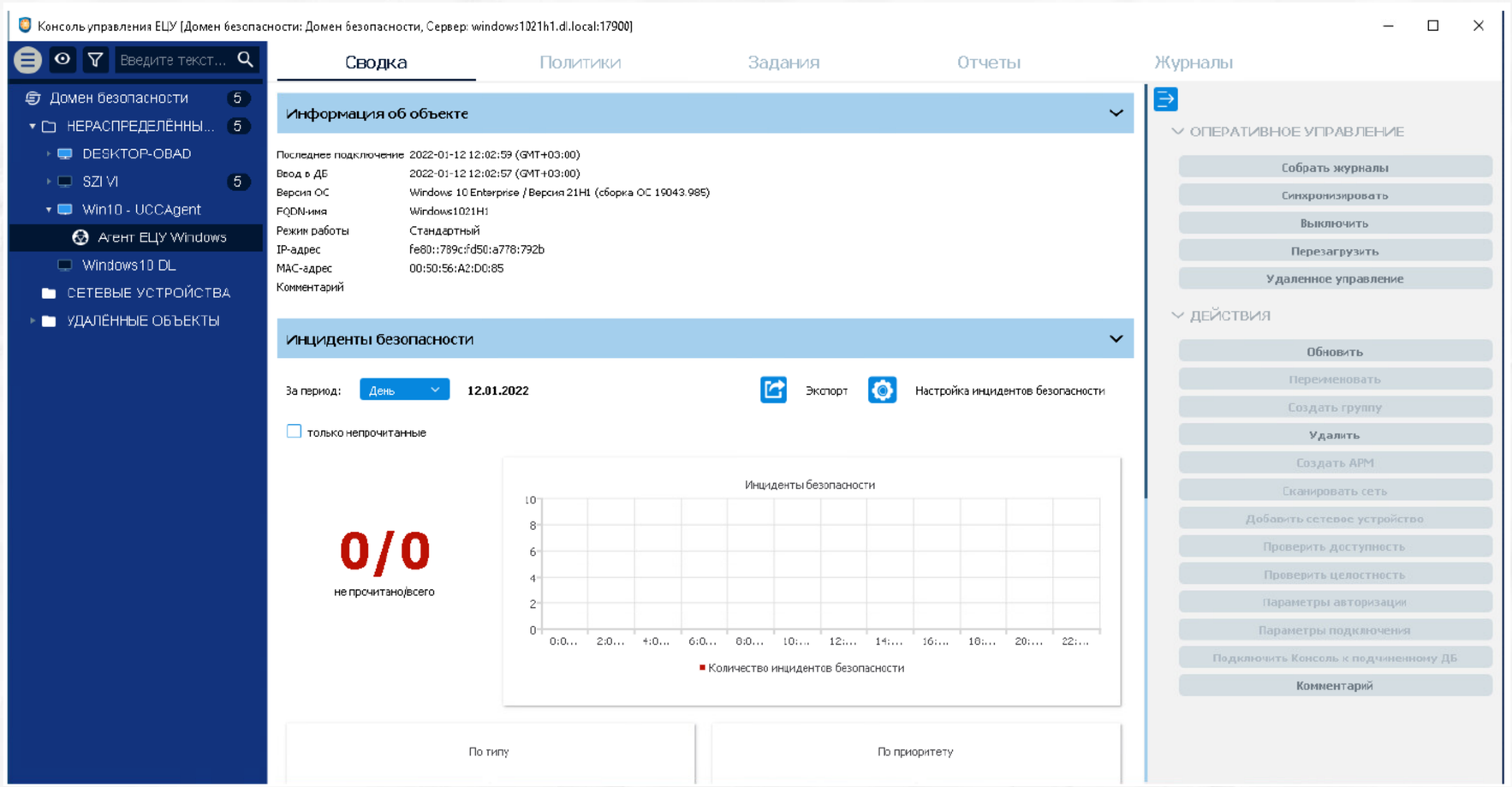
ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ
DALLAS LOCK

Единый центр управления Dallas Lock



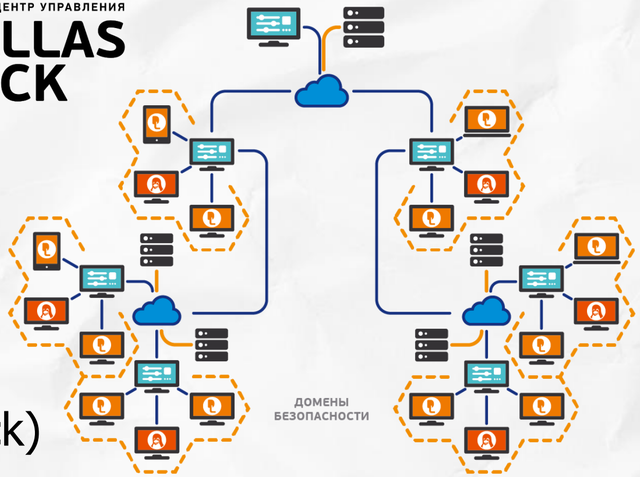
Сценарий 4:

Удаленное выключение/перезагрузка ТС (агент ЕЦУ / клиент СЗИ Dallas Lock)



КОНФИДЕНТ®
ГРУППА КОМПАНИЙ

Единый центр управления Dallas Lock



Сценарий 4:

Удаленное выключение/перезагрузка ТС (агент ЕЦУ / клиент СЗИ Dallas Lock)

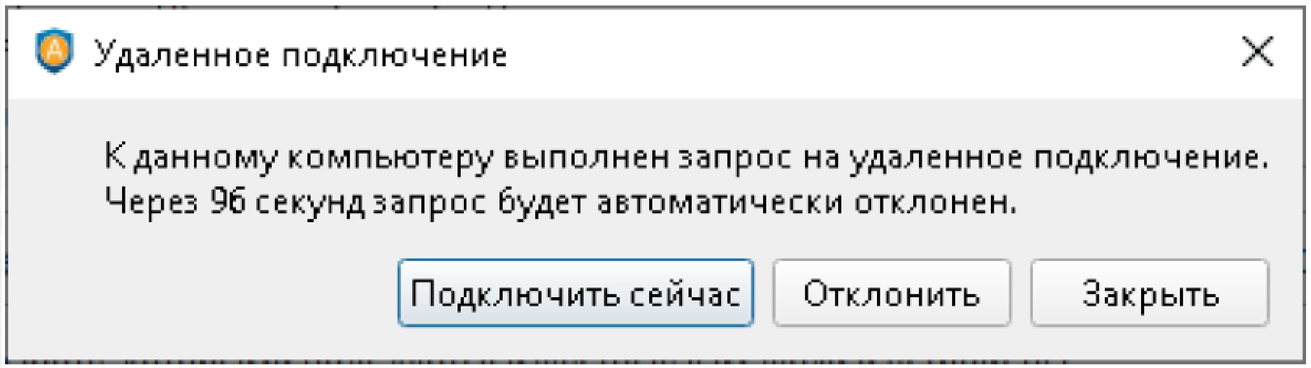


Рис. 205. Окно удаленного подключения на стороне АРМ с Агентом ЕЦУ

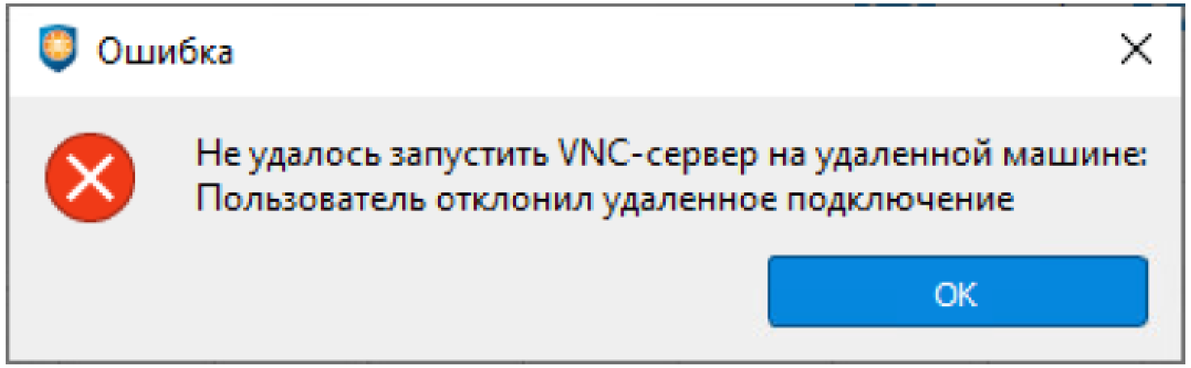
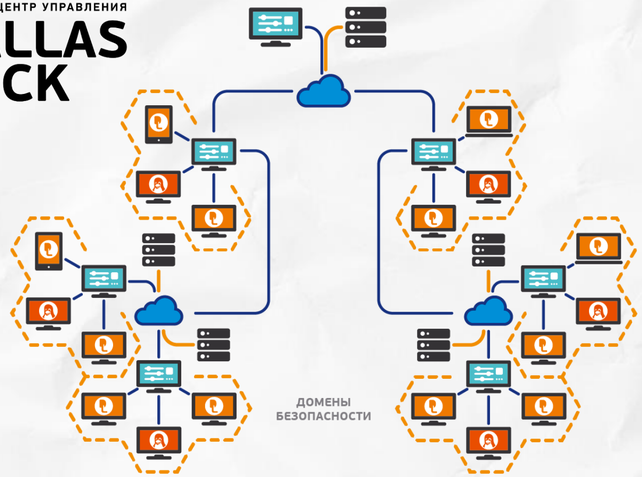


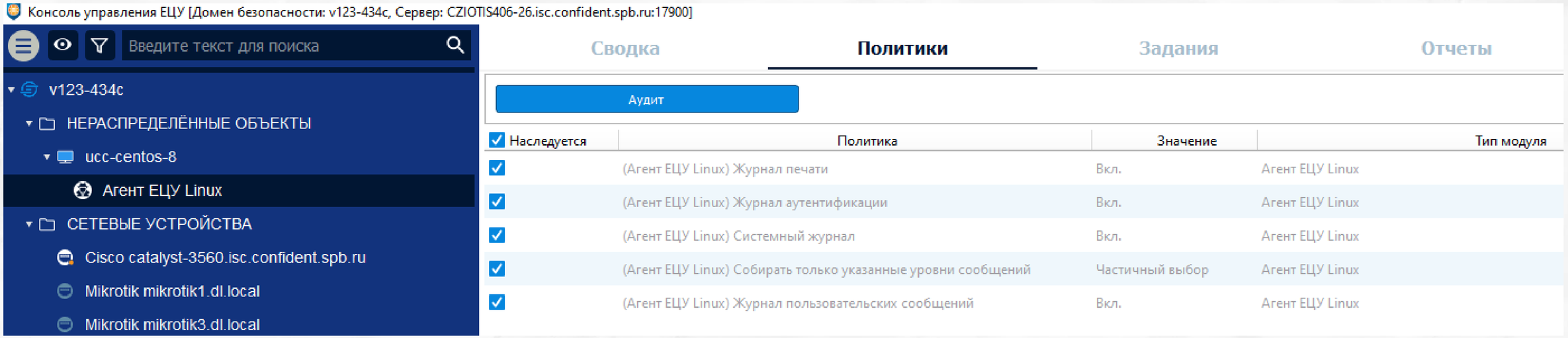
Рис. 206. Ошибка удаленного подключения

Единый центр управления Dallas Lock

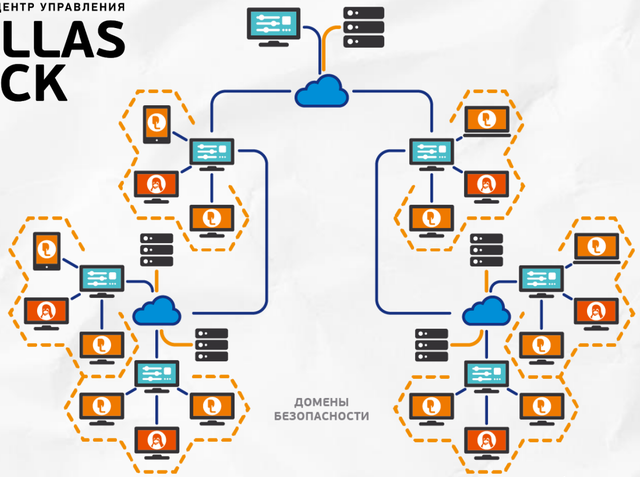


Сценарий 5:

Удаленное управление ТС (агент ЕЦУ / клиент СЗИ Dallas Lock)

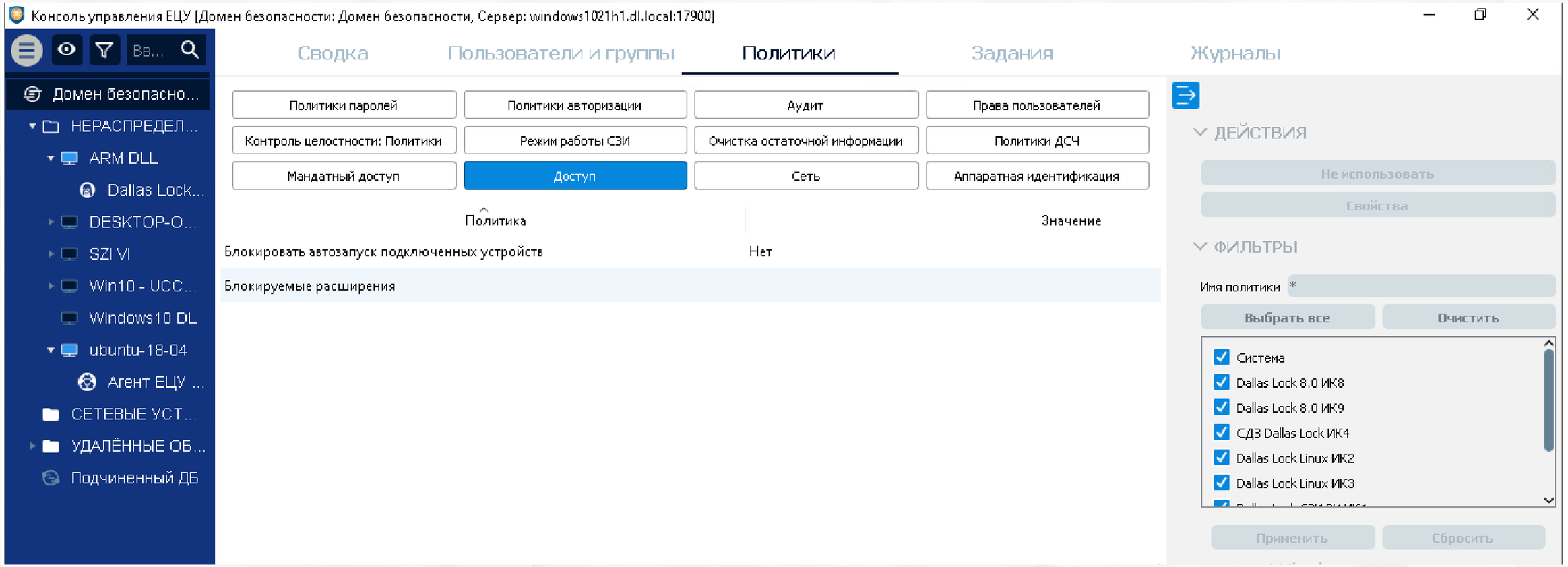


Единый центр управления Dallas Lock

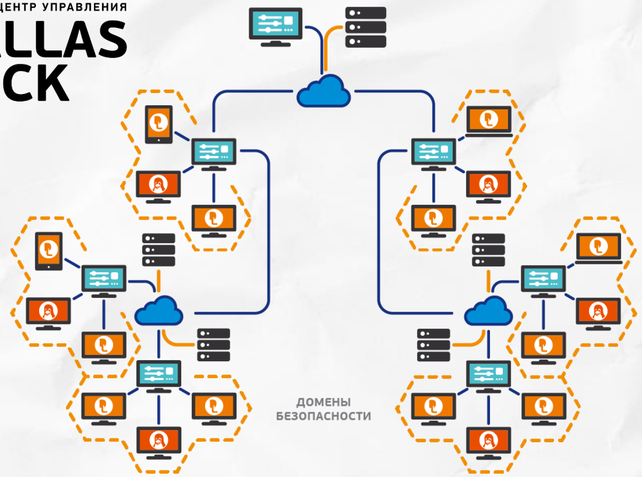


Сценарий 5:

Удаленное управление ТС (агент ЕЦУ / клиент СЗИ Dallas Lock)

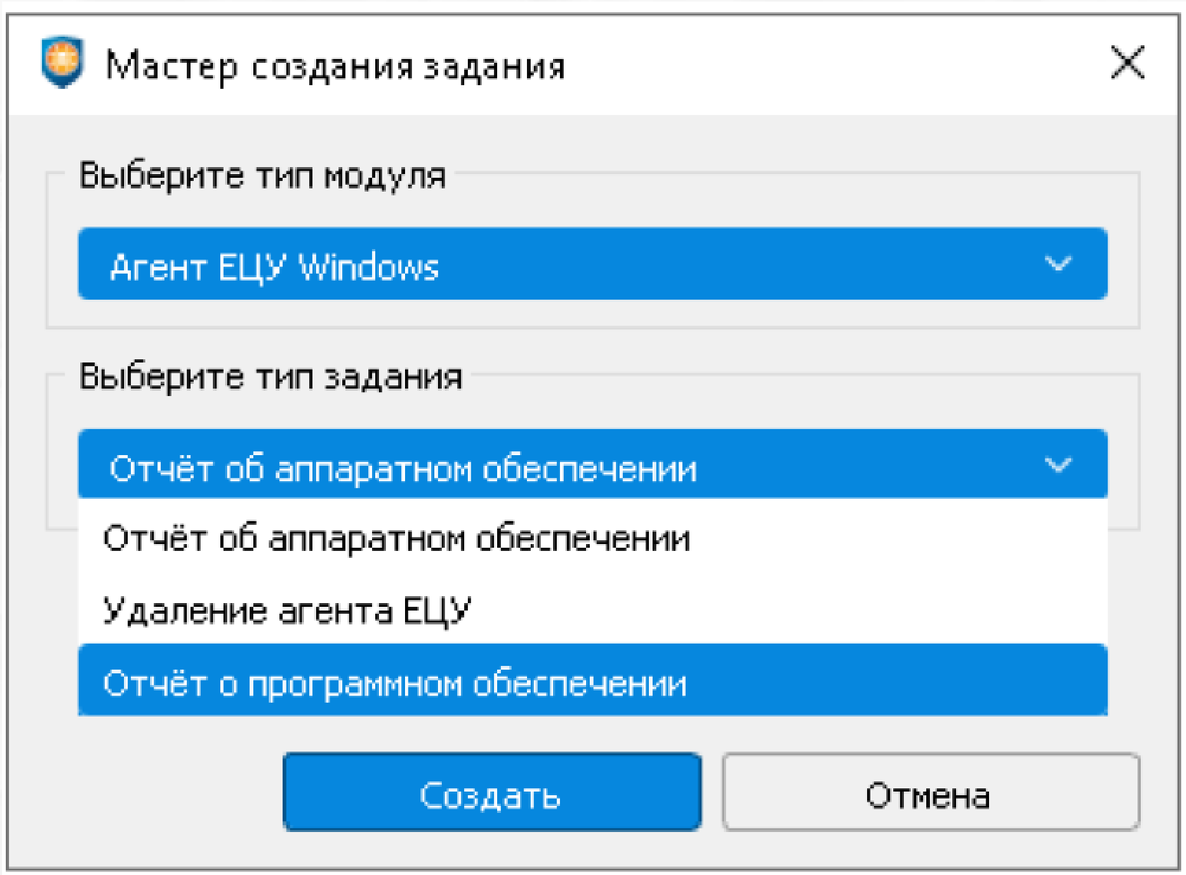


Единый центр управления Dallas Lock

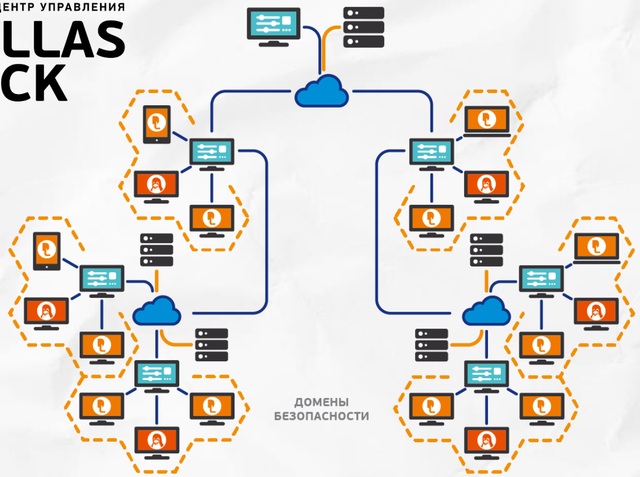


Сценарий 5:

Удаленное управление ТС (агент ЕЦУ / клиент СЗИ Dallas Lock)



Единый центр управления Dallas Lock



Сценарий 5:

Удаленное управление ТС (агент ЕЦУ / клиент СЗИ Dallas Lock)

Консоль управления ЕЦУ [Домен безопасности: Домен безопасности, Сервер: windows1021h1.dl.local:17900]

Сводка | Политики | Задания | Отчеты | Журналы

- Домен безопасно...
- НЕРАСПРЕДЕЛ...
  - ARM DLL
  - DESKTOP-O...
  - SZI VI
  - Win10 - UCC...
  - Windows10 DL
  - ubuntu-18-04
    - Агент ЕЦУ ...
- СЕТЕВЫЕ УСТ...
- УДАЛЁННЫЕ ОБ...
- Подчиненный ДБ

Отчёт об аппаратном обеспечении | Отчёт о программном обеспечении

ДЕЙСТВИЯ

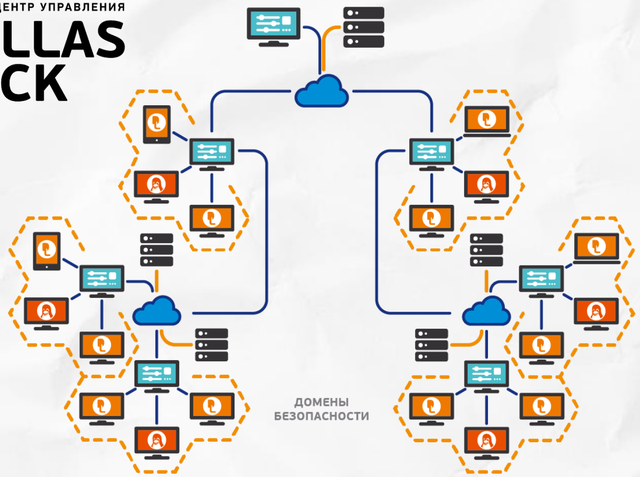
Применить изменения

Обновить

Сохранить в файл

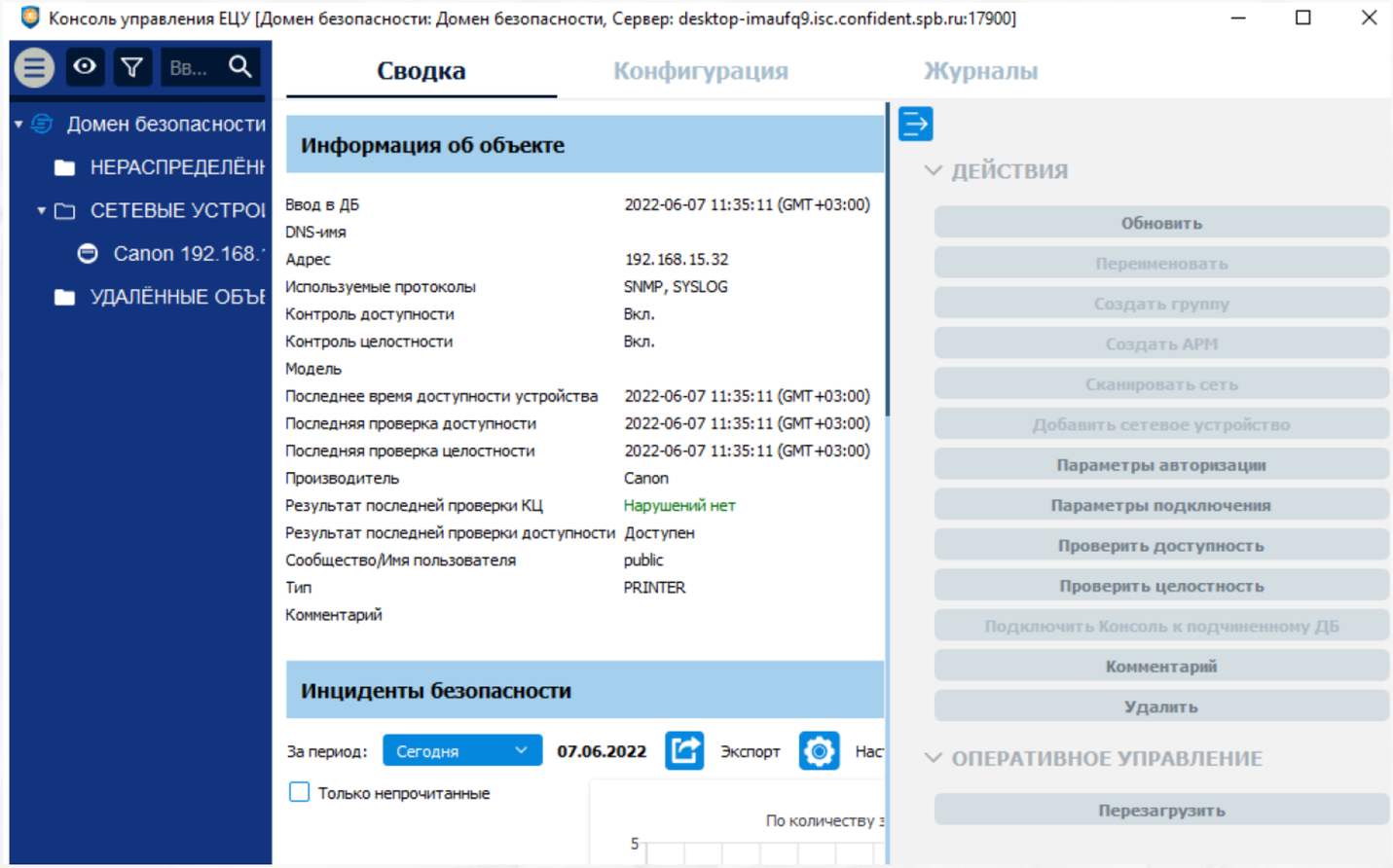
Эталонный отчет (2022-01-17 12:20:22 (GMT+03:00))	Текущий отчет (2022-01-17 12:20:22 (GMT+03:00))
Название пакета : accountsservice	Название пакета : accountsservice
Версия пакета : 0.6.45-lubuntu1.3	Версия пакета : 0.6.45-lubuntu1.3
Объем : 440 кБ	Объем : 440 кБ
Название пакета : acl	Название пакета : acl
Версия пакета : 2.2.52-3buildl	Версия пакета : 2.2.52-3buildl
Объем : 200 кБ	Объем : 200 кБ
Название пакета : acpi-support	Название пакета : acpi-support
Версия пакета : 0.142	Версия пакета : 0.142
Объем : 92 кБ	Объем : 92 кБ
Название пакета : acpid	Название пакета : acpid
Версия пакета : 1:2.0.28-lubuntul	Версия пакета : 1:2.0.28-lubuntul
Объем : 139 кБ	Объем : 139 кБ

Единый центр управления Dallas Lock

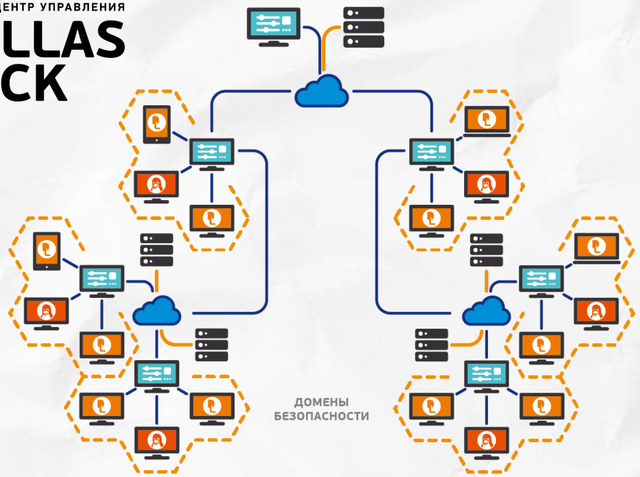


Сценарий 6:

Контроль сетевого оборудования (без агентов/клиентов СЗИ Dallas Lock)



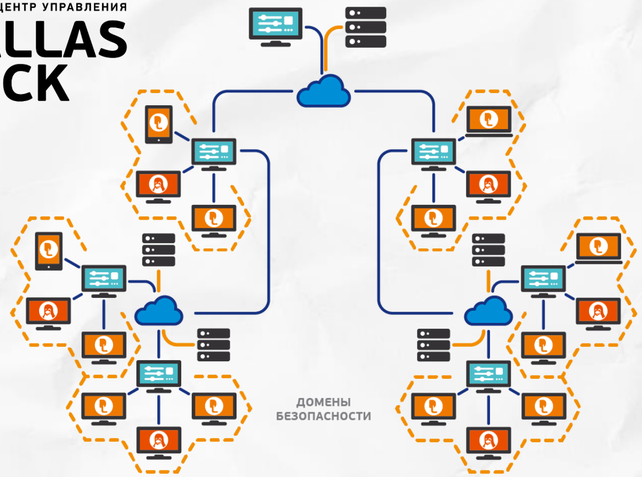
Единый центр управления Dallas Lock



Сценарий 6:

Контроль сетевого оборудования (без агентов/клиентов СЗИ Dallas Lock)

Единый центр управления Dallas Lock



Сценарий 6:

Контроль сетевого оборудования (без агентов/клиентов СЗИ Dallas Lock)

- сканирование сети обнаружения оборудования (SNMP и SSH)
- ввод/вывод сетевого оборудования в/из домена безопасности
- удаленное включение сетевого оборудования
- настройка параметров, берущихся под контроль
- получение отчета о конфигурации сетевого оборудования
- применение конфигураций
- контроль изменений конфигурации сетевого оборудования
- прием сообщений по протоколу Syslog
- сигнализация о нарушении целостности

Единый центр управления Dallas Lock

Центр управления

Современные требования к Центру управления информационной безопасностью

- поддержка сертифицированных отечественных ОС
- управление клиентскими частями под Windows и Linux, СДЗ, поддержка российских ОС, а также возможность удалённого подключения к ним
- возможность получать журналы с незащищённых АРМ
- наличие встроенного VNC-клиента
- работа за NAT (Network Address Translation)
- бесперебойная работа в больших инфраструктурах и при «слабом» сетевом соединении

Готов ответить
на ваши вопросы

E-mail: isc@confident.ru

www.dallaslock.ru

КОНФИДЕНТ®
ГРУППА КОМПАНИЙ