

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.

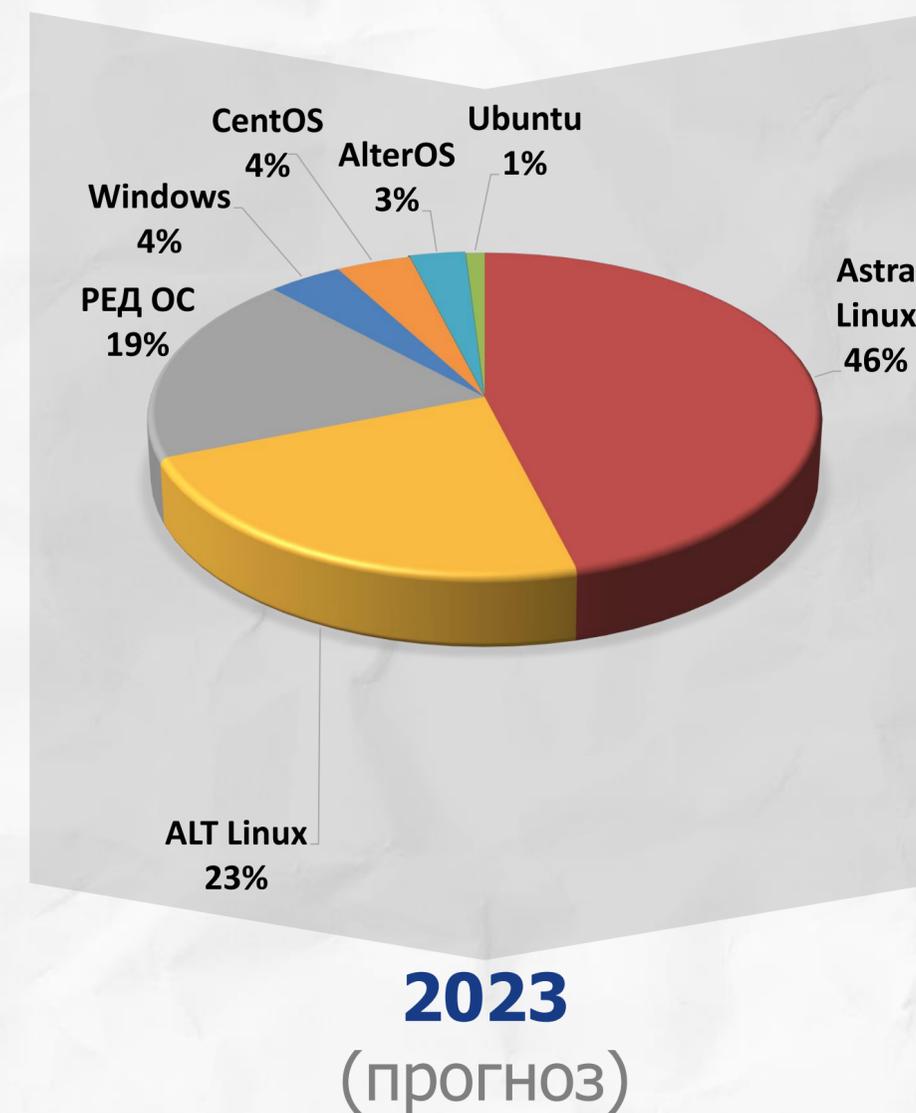
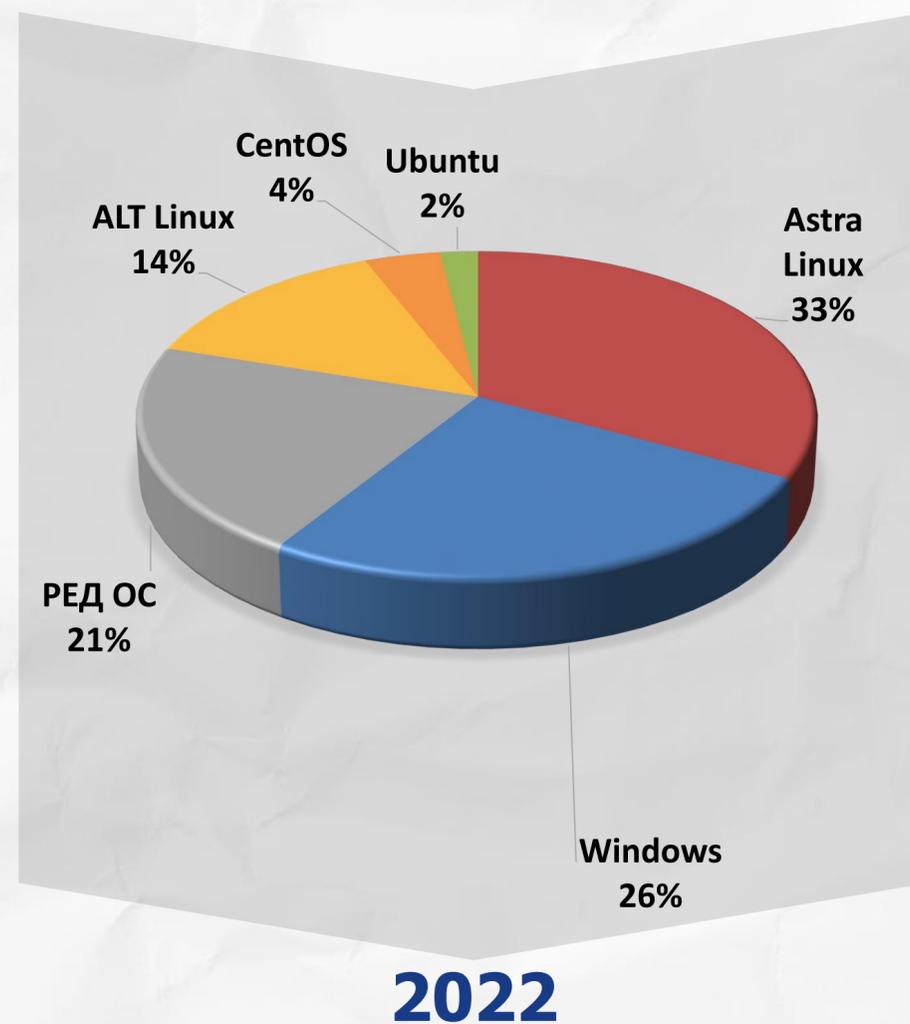
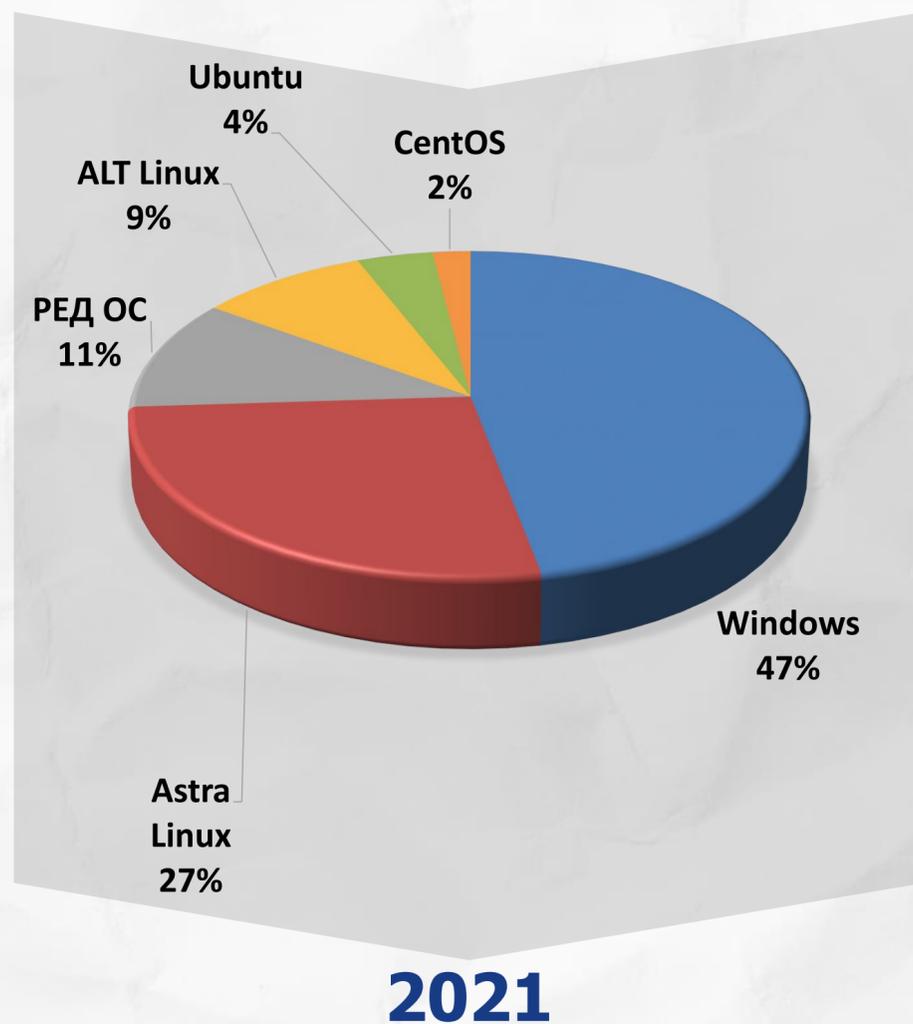
Награды

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

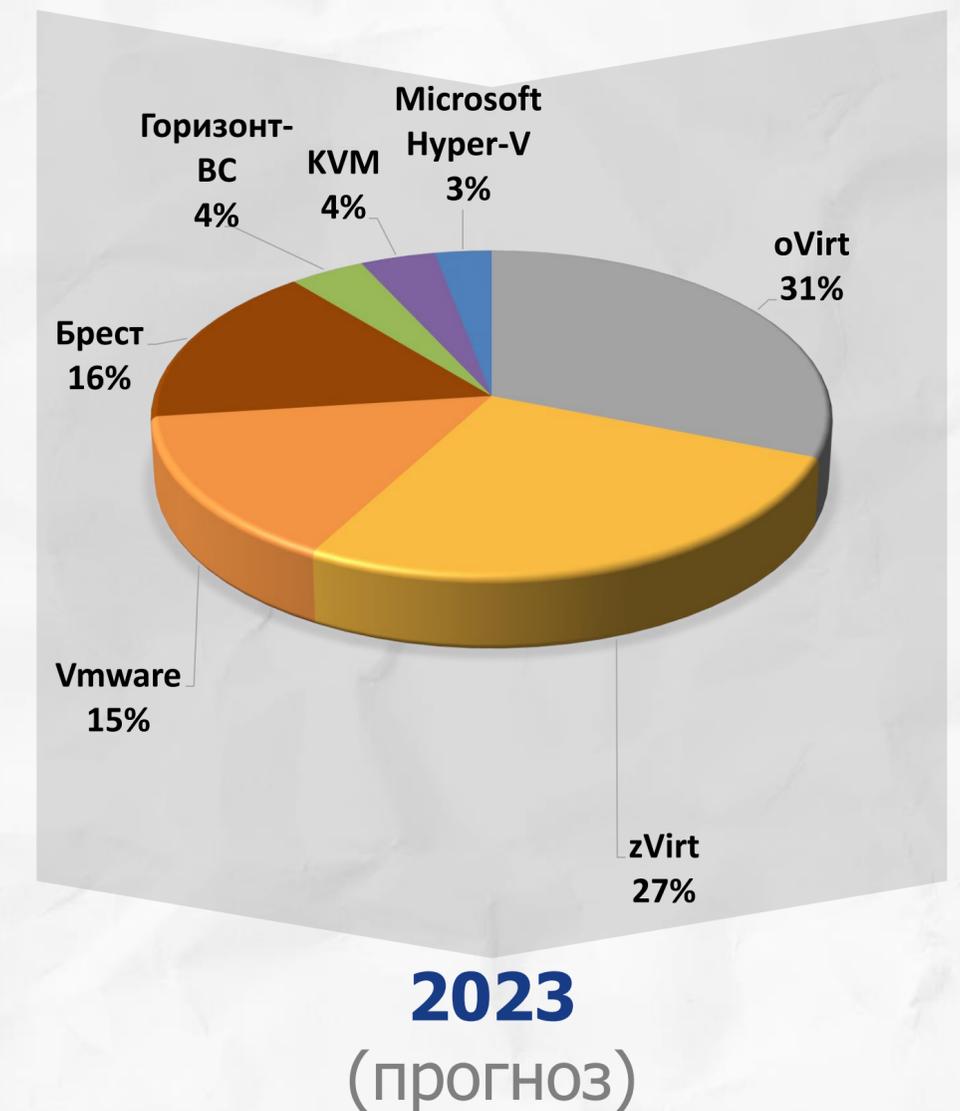
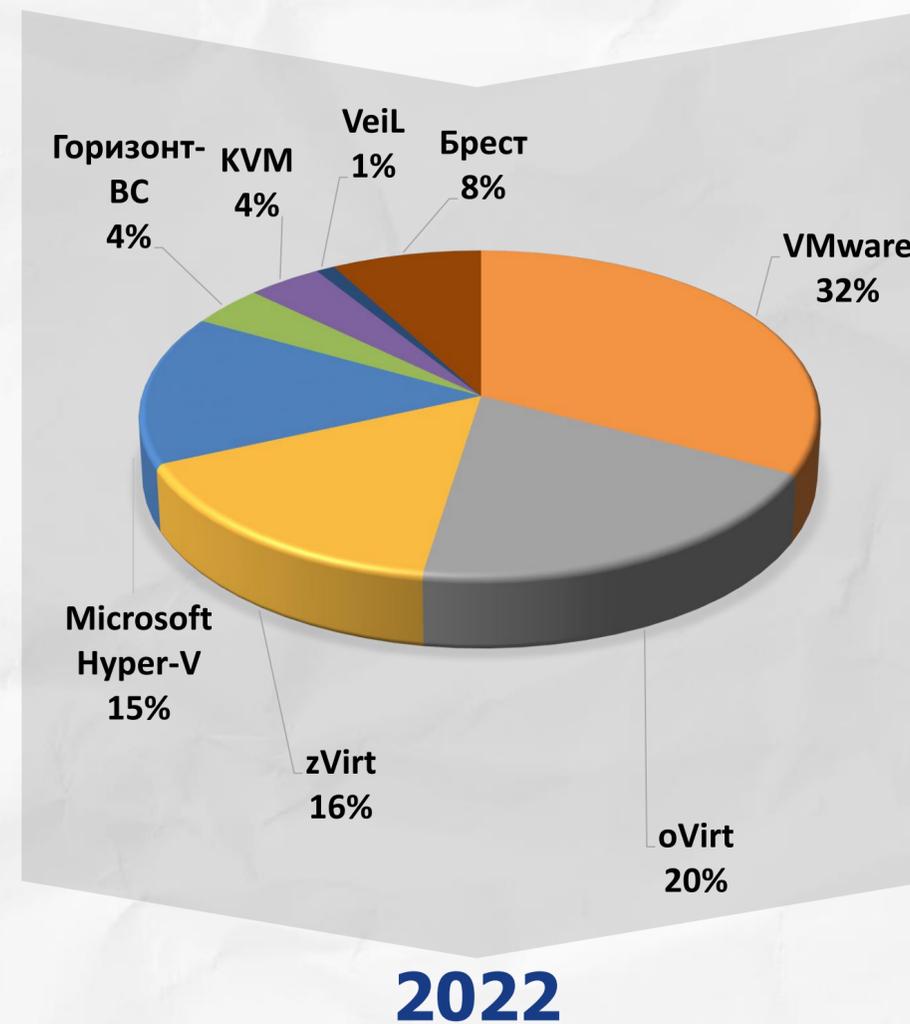
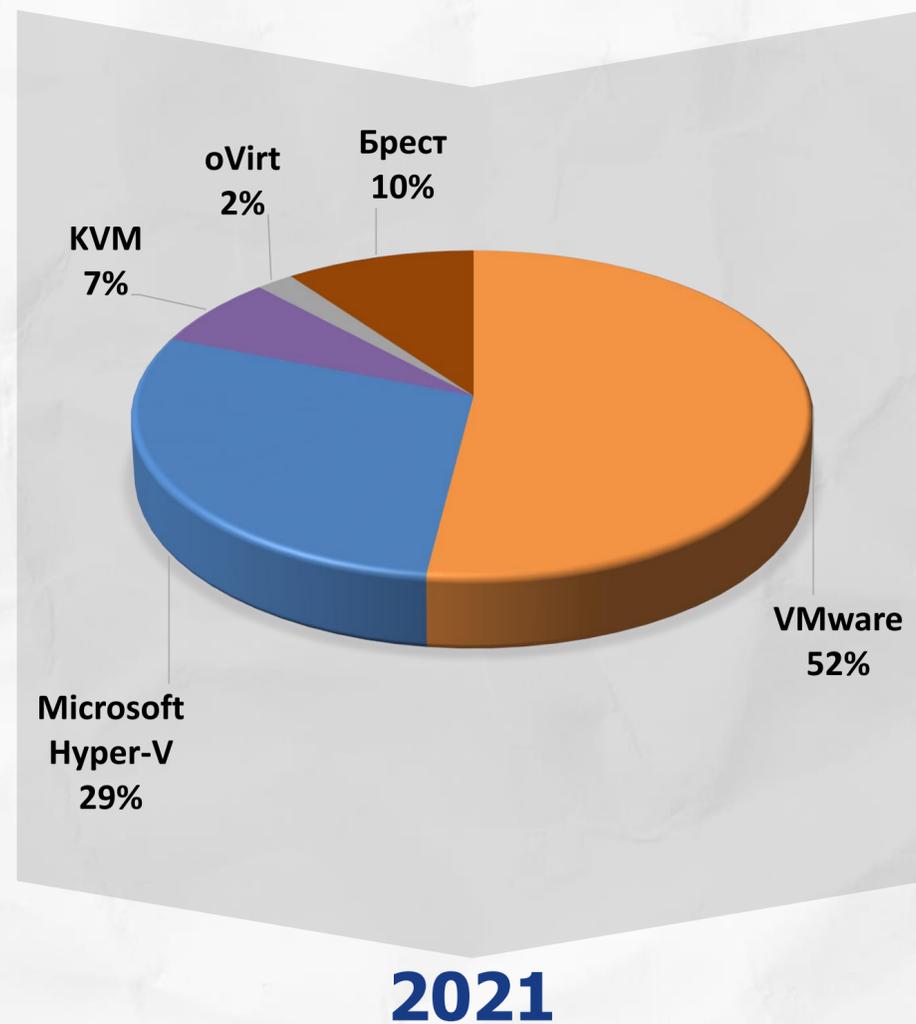


Актуальные вопросы защиты
информации с использованием
СЗИ Dallas Lock

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



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



Тренды импортозамещения

Защита рабочих станций и серверов

Windows



Linux



Отечественные
операционные
системы

Защита среды
виртуализации

VMware,
Hyper-V



KVM,
oVirt



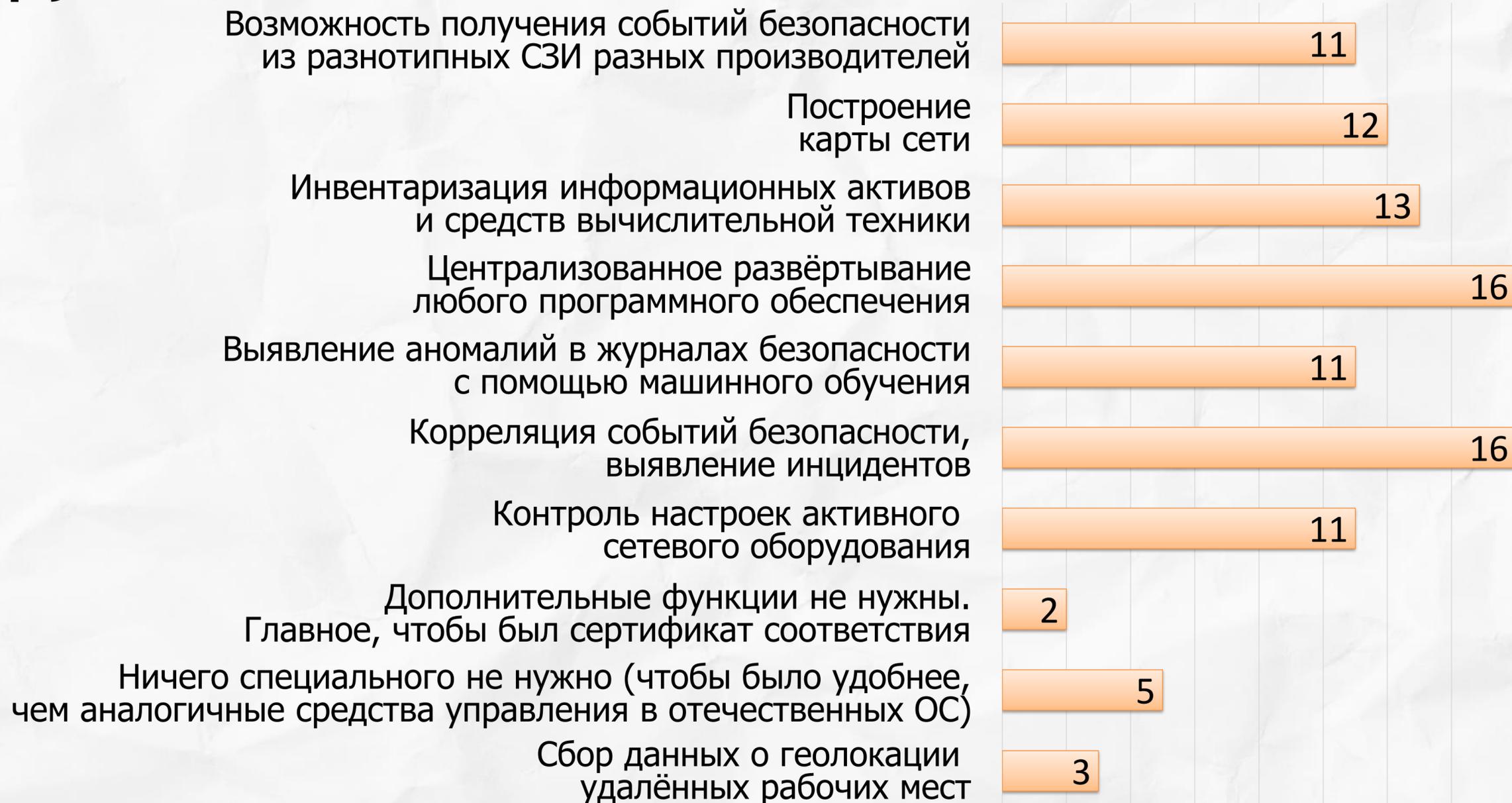
Отечественные
платформы
виртуализации



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



Востребованные у заказчиков дополнительные функции СЗИ

Возможность получения событий безопасности из разнотипных СЗИ разных производителей

Построение карты сети

Инвентаризация информационных активов и средств вычислительной техники

Централизованное развёртывание любого программного обеспечения

Выявление аномалий в журналах безопасности с помощью машинного обучения

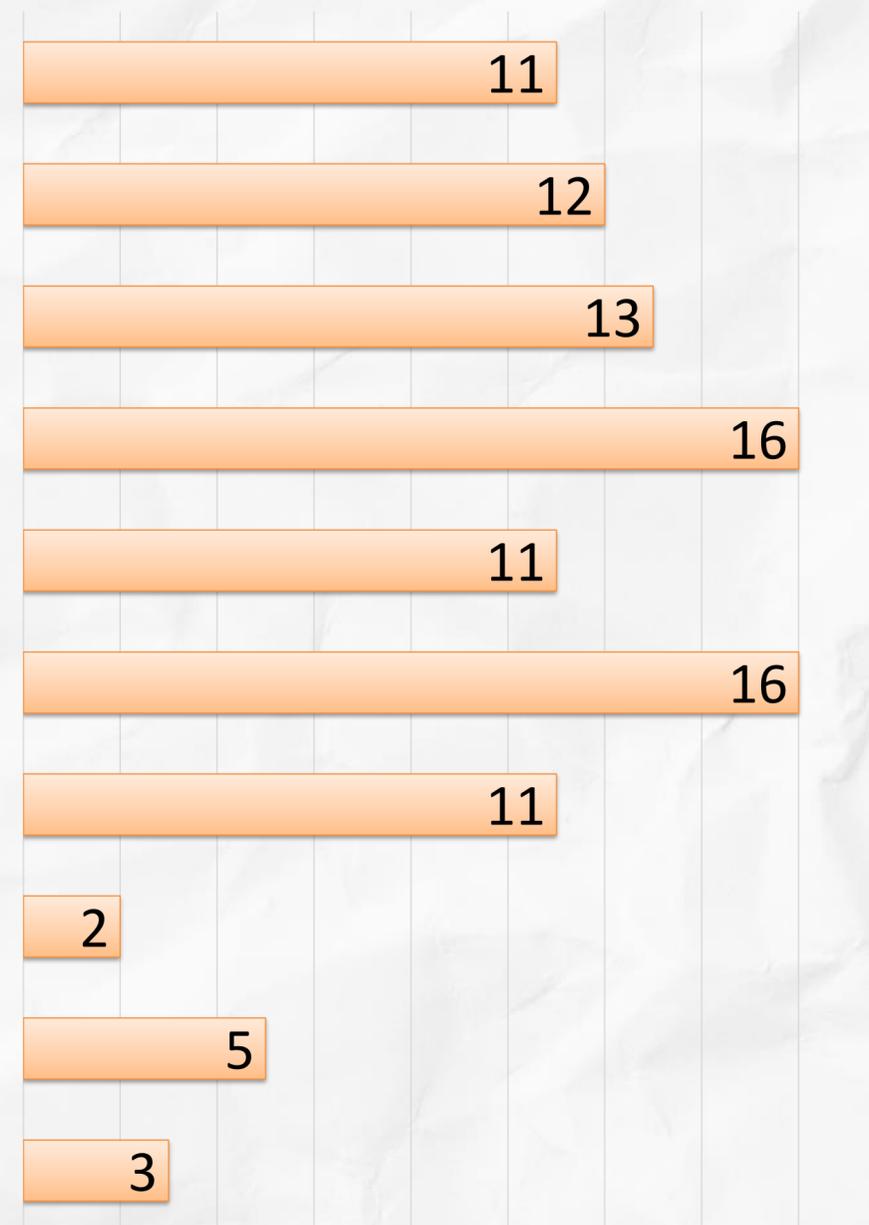
Корреляция событий безопасности, выявление инцидентов

Контроль настроек активного сетевого оборудования

Дополнительные функции не нужны. Главное, чтобы был сертификат соответствия

Ничего специального не нужно (чтобы было удобнее, чем аналогичные средства управления в отечественных ОС)

Сбор данных о геолокации удалённых рабочих мест





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

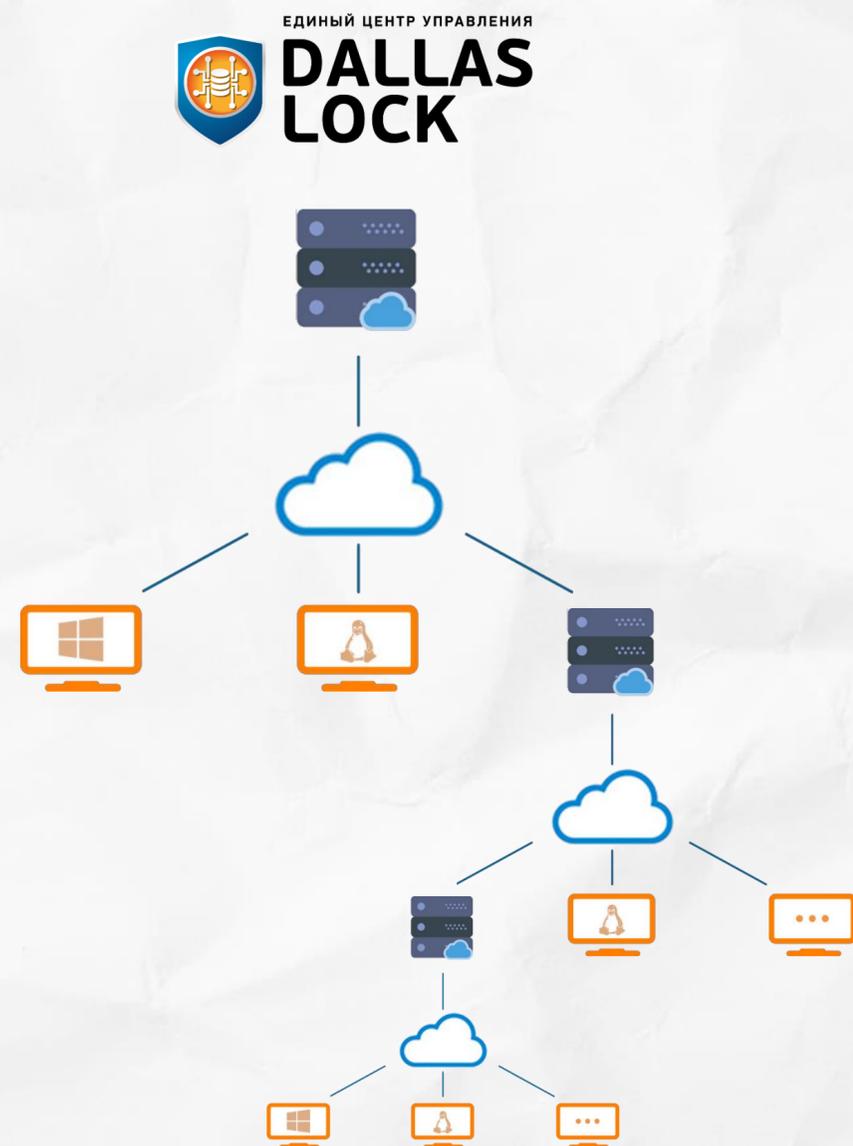
Центр управления



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



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

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

СЗИ ВИ
Система защиты информации
в виртуальных инфраструктурах
DALLAS LOCK

СДЗ
Средство доверенной загрузки
DALLAS LOCK

DALLAS LOCK 8.0
Система защиты информации
от несанкционированного
доступа DALLAS LOCK 8.0

МЭ
Межсетевой экран
DALLAS LOCK 8.0

СОВ
Система обнаружения и
предотвращения вторжений
DALLAS LOCK 8.0

СКН
Средство контроля съемных
машинных носителей
информации DALLAS LOCK 8.0

МП
Модуль паспортизации ПО
DALLAS LOCK 8.0

РК
Модуль резервного копирования
произвольных объектов DALLAS LOCK 8.0

DALLAS LOCK LINUX
Система защиты информации
от несанкционированного доступа
DALLAS LOCK LINUX

СКН
Средство контроля съемных машинных носителей информации
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



СЗИ ВИ

Система защиты информации
в виртуальных инфраструктурах
DALLAS LOCK



СДЗ

Средство доверенной загрузки
DALLAS LOCK **уровня BIOS**



СДЗ

Средство доверенной загрузки
DALLAS LOCK **уровня платы расширения**



DALLAS LOCK 8.0



Система защиты информации
от несанкционированного
доступа DALLAS LOCK 8.0

МЭ



Межсетевой экран
DALLAS LOCK 8.0

СОВ



Система обнаружения и
предотвращения вторжений
DALLAS LOCK 8.0

СКН



Средство контроля съемных
машинных носителей
информации DALLAS LOCK 8.0

МП



Модуль паспортизации ПО
DALLAS LOCK 8.0

РК



Модуль резервного копирования
произвольных объектов DALLAS LOCK 8.0

DALLAS LOCK LINUX



Система защиты информации
от несанкционированного доступа
DALLAS LOCK LINUX

СКН



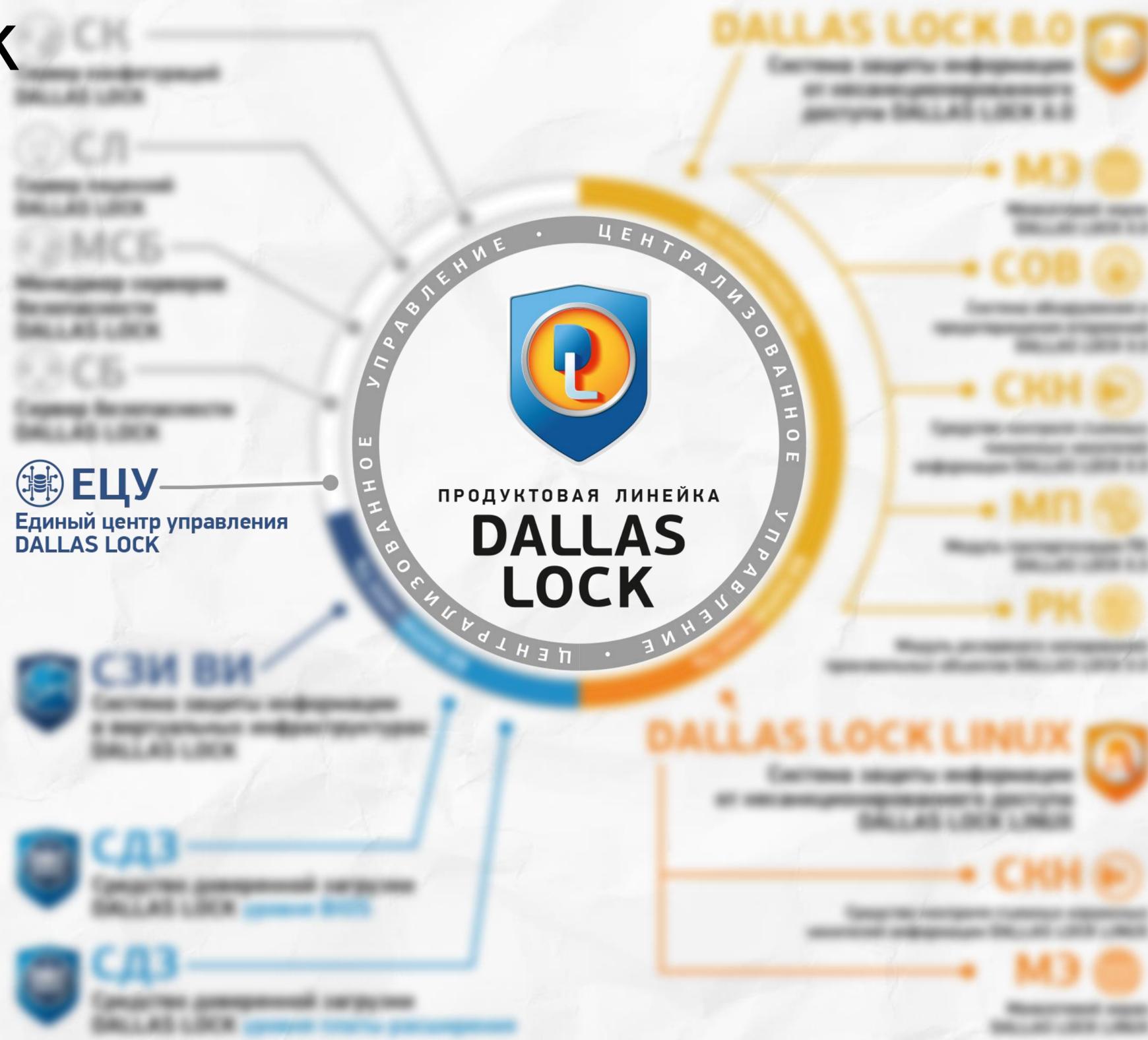
Средство контроля съемных машинных
носителей информации DALLAS LOCK LINUX

МЭ



Межсетевой экран
DALLAS LOCK LINUX

Dallas Lock



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

СЗИ ВИ
Система защиты информации
и идентификации информации
DALLAS LOCK

САД
Система автоматизированного
управления доступом
DALLAS LOCK

САД
Система автоматизированного
управления доступом
DALLAS LOCK



DALLAS LOCK 8.0
Система защиты информации
и идентификации информации
DALLAS LOCK 8.0

МД
Менеджер
DALLAS LOCK 8.0

СОБ
Система
DALLAS LOCK 8.0

СНН
Система
DALLAS LOCK 8.0

МП
Менеджер
DALLAS LOCK 8.0

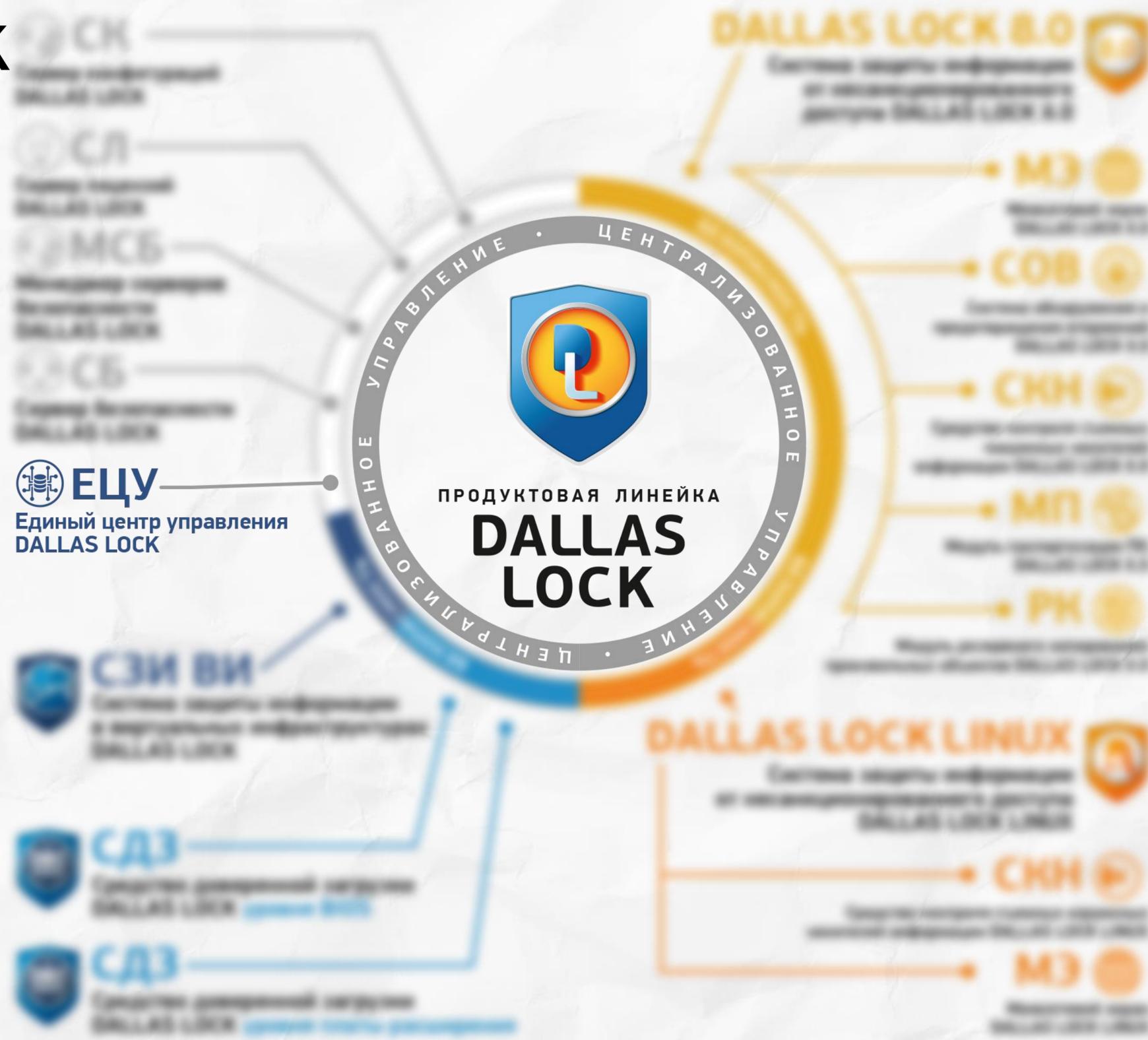
ПК
Система
DALLAS LOCK 8.0

DALLAS LOCK LINUX
Система защиты информации
и идентификации информации
DALLAS LOCK LINUX

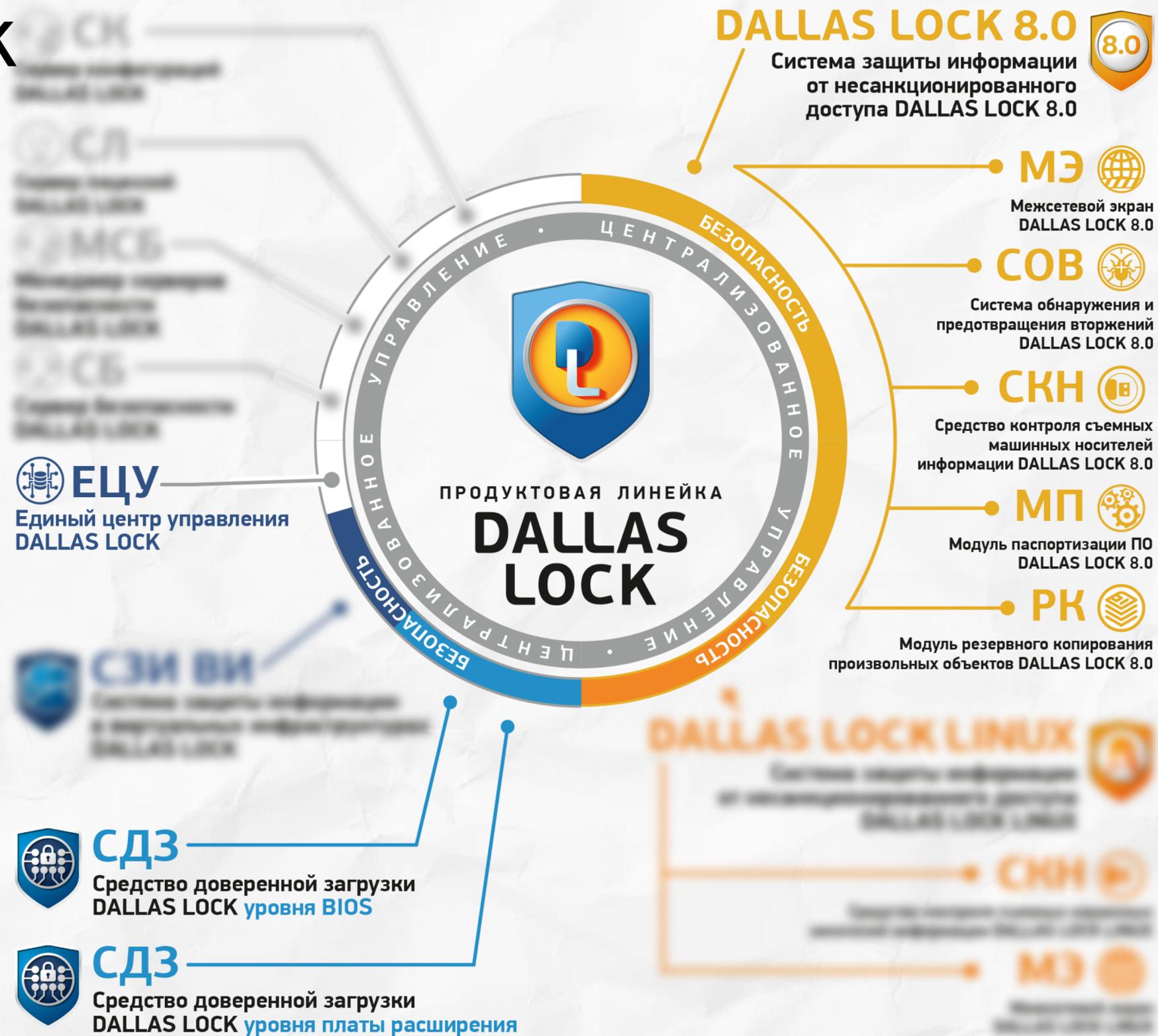
СНН
Система
DALLAS LOCK LINUX

МД
Менеджер
DALLAS LOCK LINUX

Dallas Lock



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.)



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-С, 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



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 К 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);

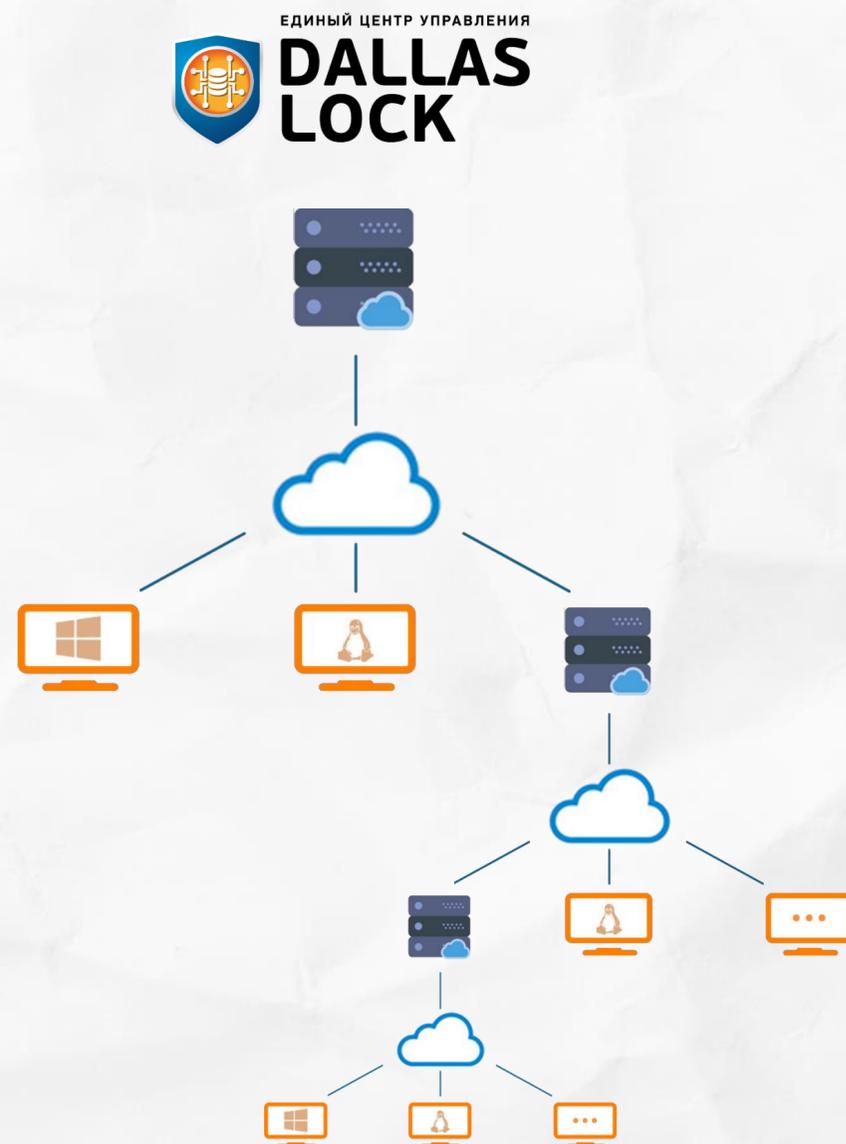
Windows Server 2022 (Standard, Datacenter);

Debian 10.x; Debian 11.x;

CentOS 7.x; Red Hat Enterprise Linux Server 7.x;

Ubuntu 18.04 LTS; Ubuntu 20.04 LTS.

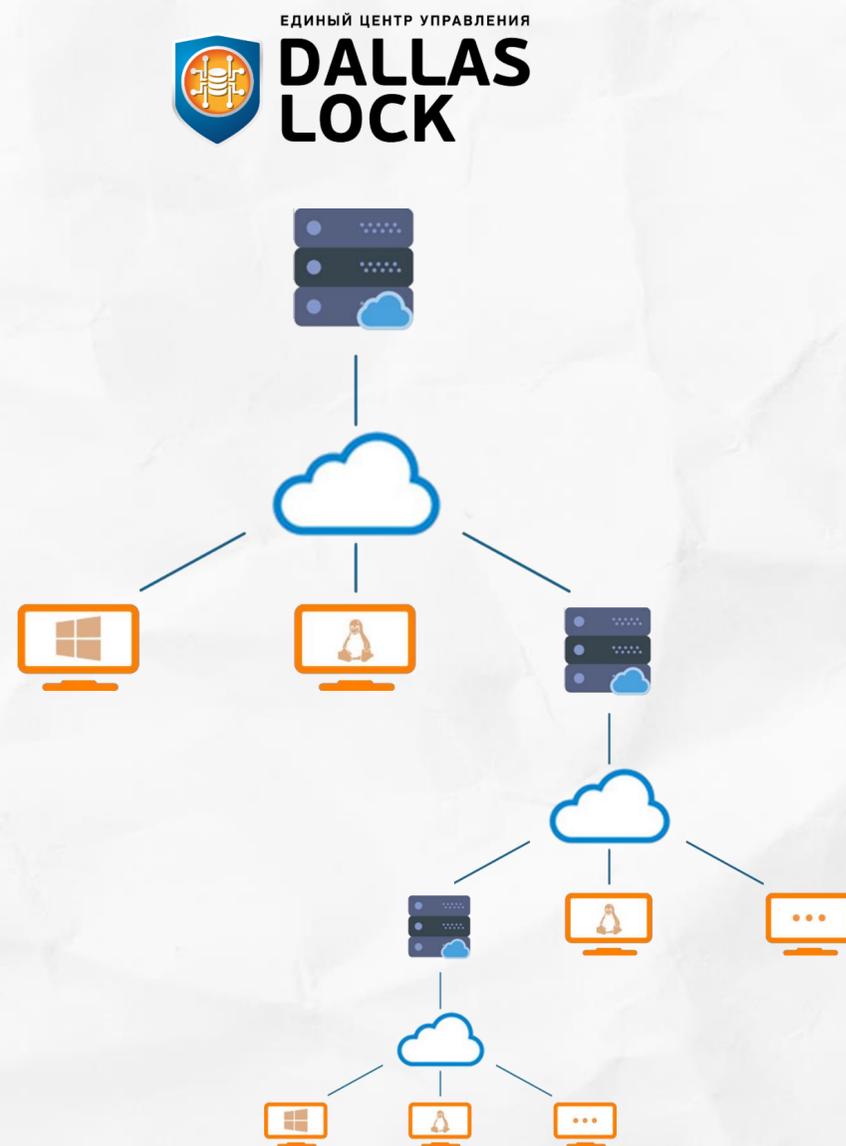
Единый центр управления Dallas Lock



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
- ...

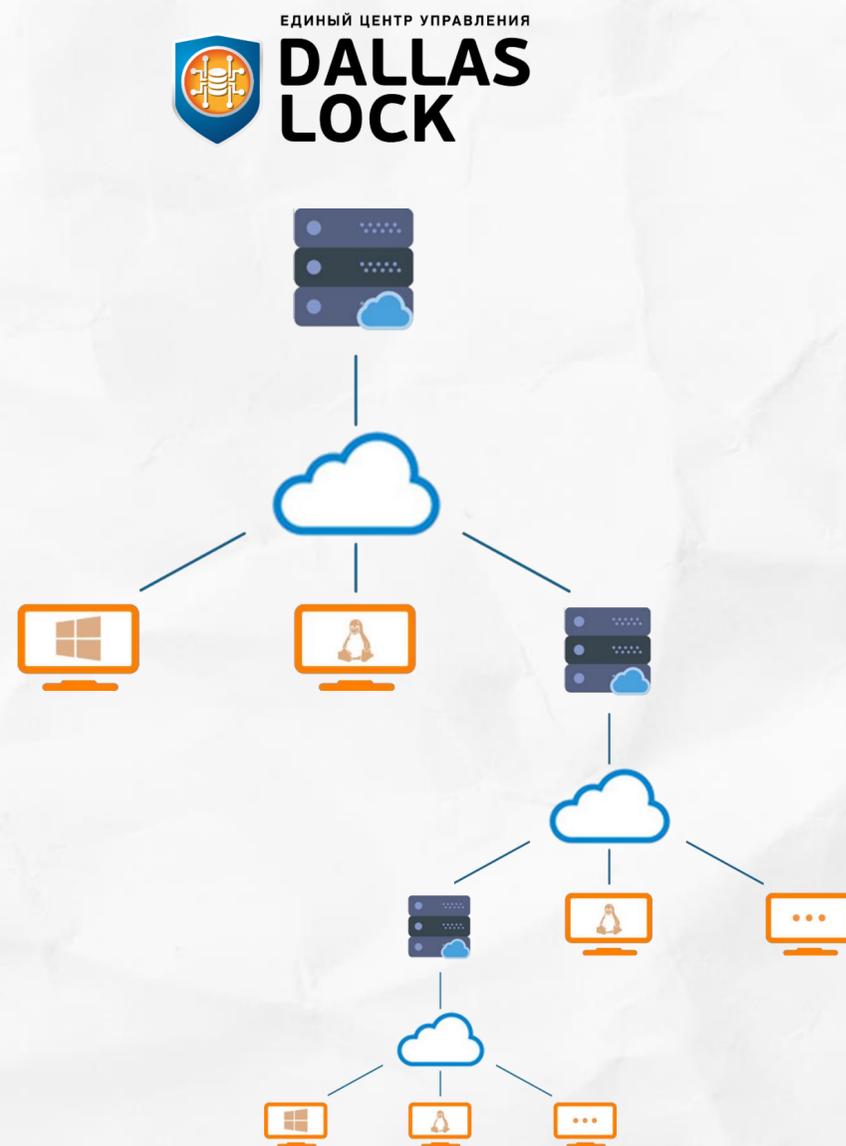
Единый центр управления Dallas Lock



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»
- ...

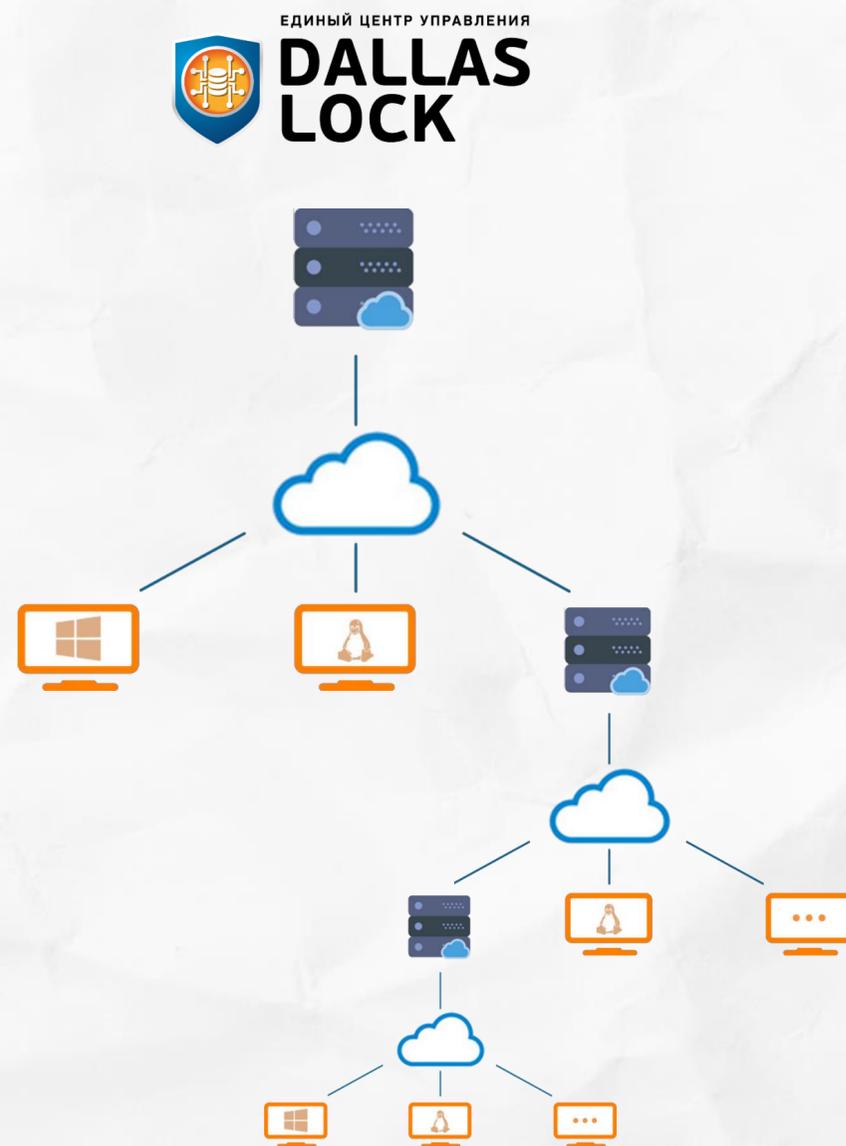
Единый центр управления Dallas Lock



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

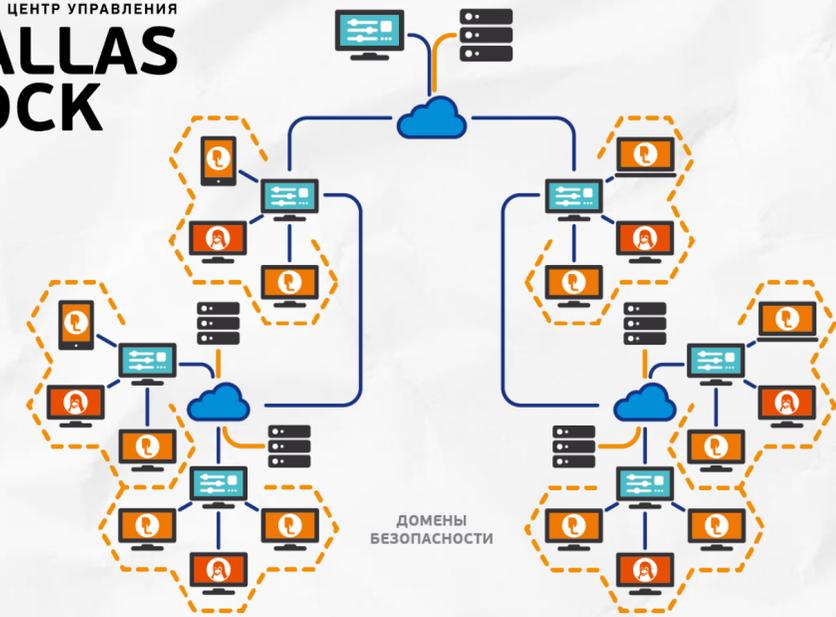
Единый центр управления Dallas Lock



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



Сценарий 1: Инвентаризация активов

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

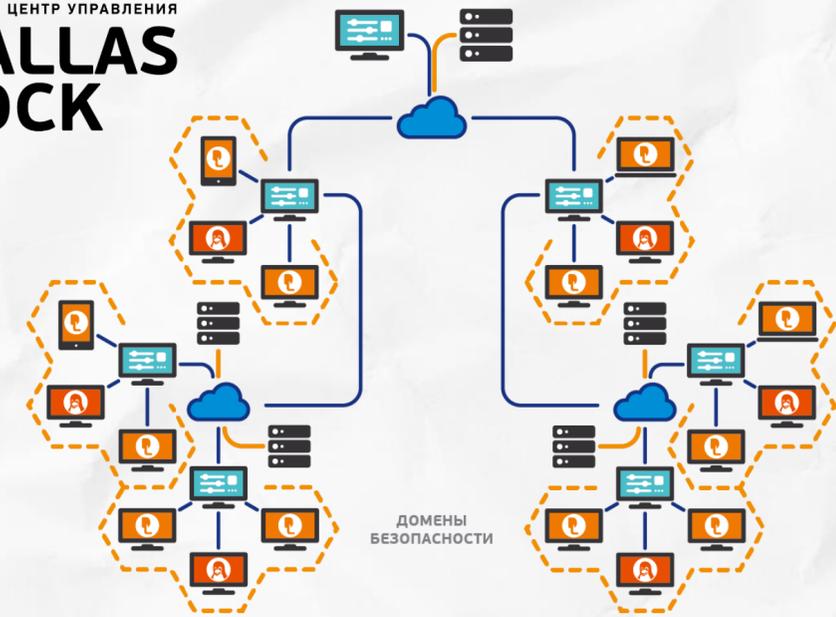
Сценарий 3: Управление пользователями/группами на СЗИ Dallas Lock

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)

Единый центр управления Dallas Lock



Сценарий 1: Инвентаризация активов

Введите текст для...

Домен безопасности

- НЕРАСПРЕДЕЛЁННЫЕ ОБЪЕКТЫ
- ARM-DL8
 - Dallas Lock 8.0 ИК9
 - Агент ЕЦУ Windows
- ARM-DLL
 - Dallas Lock Linux ИК3
 - Агент ЕЦУ Linux
- Brother 192.168.15.15
- Cisco catalyst-3560.isc.confide
- Dallas Lock 8.0
 - Домен безопасности 2
 - Домен безопасности 3
- СЕТЕВЫЕ УСТРОЙСТВА
 - Brother 192.168.15.217
 - Canon 192.168.15.32
 - Dell 192.168.0.120
 - Dell 192.168.0.158
 - Dell 192.168.0.159
 - Dell 192.168.0.164
 - Dell 192.168.12.123
 - Dell 192.168.23.1
 - Dell 192.168.23.2
 - Dell 192.168.23.3
 - Dell 192.168.23.4
 - Dell 192.168.23.5
 - Dell 192.168.23.6
 - Dell 192.168.23.7
 - Dell 192.168.23.8
 - Dell 192.168.23.9
 - Dell idrac-242.isc.confident.spt
 - FreeBSD.srv-gateway.confli.ru

Сводка
Пользователи и группы
Политики
Задания
Журналы

Информация об объекте

Серверы домена безопасности: map-ucc-w10-1.dl.local:17900
Родительский домен: Нет

ПАРАМЕТРЫ ЛИЦЕНЗИИ Подробнее

АРМ	99 / 2500
Сетевые устройства	64 / 500
Подчиненные домены	2 / 20 используемые / всего

Инциденты безопасности

За период: За все время 09.12.2022 11:16 - 11.04.2023 23:59 Экспорт Настройки инцидентов безопасности

Только непрочитанные

0/17

Не прочитано/Всего

По количеству за период

■ Количество

По типу

■ Срабатывание сигнатуры... ■ Попытка входа с неправл... ■ Учетная запись пользоват...

По приоритету

■ Средний ■ Низкий ■ Высокий

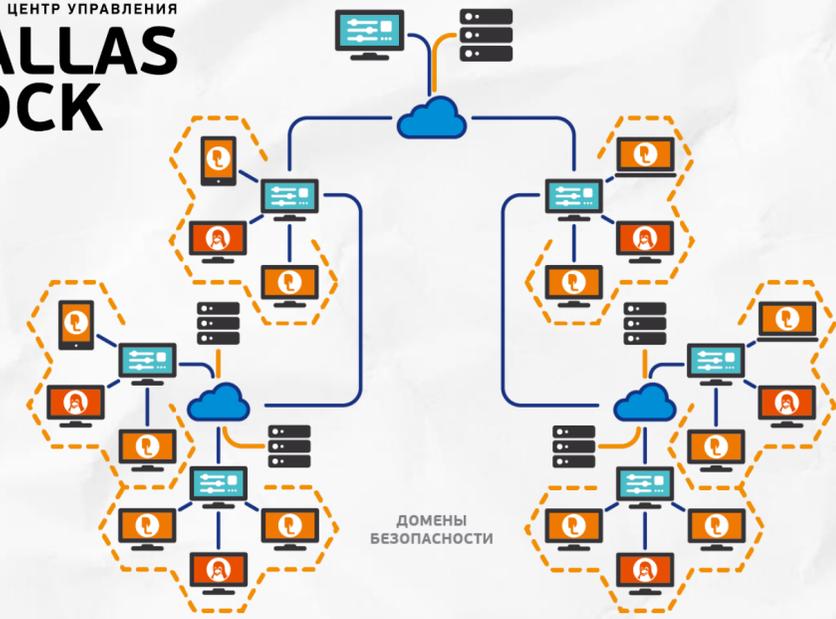
ДЕЙСТВИЯ

- Обновить
- Переименовать
- Создать группу
- Создать АРМ
- Сканировать сеть
- Добавить сетевое устройство
- Параметры авторизации
- Параметры подключения
- Проверить доступность
- Проверить целостность
- Подключить Консоль к подчиненному ДБ
- Комментарий
- Удалить

ОПЕРАТИВНОЕ УПРАВЛЕНИЕ

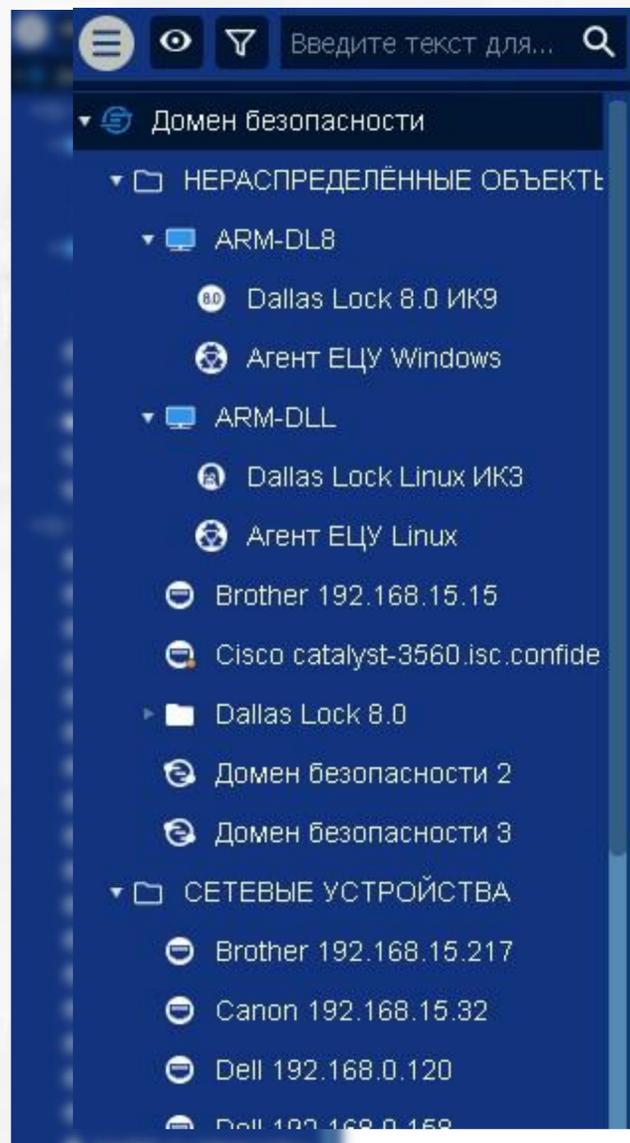
- Перезагрузить
- Синхронизировать
- Выключить
- Собрать журналы
- Разблокировать пользователей
- Пересчитать целостность

Единый центр управления Dallas Lock

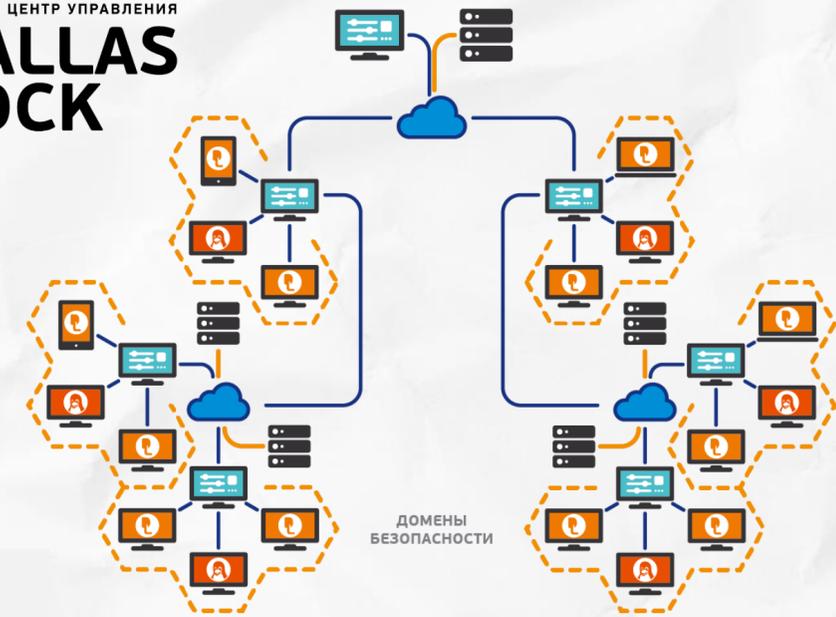


Сценарий 1:

Инвентаризация активов

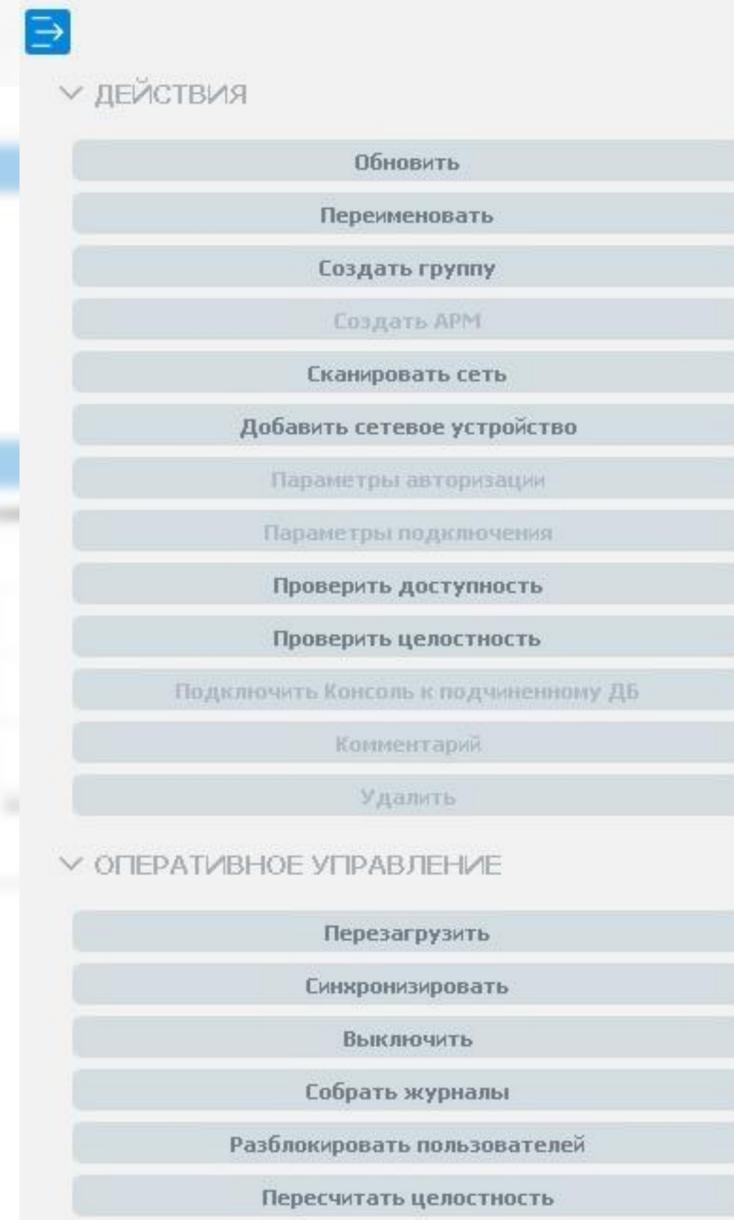


Единый центр управления Dallas Lock

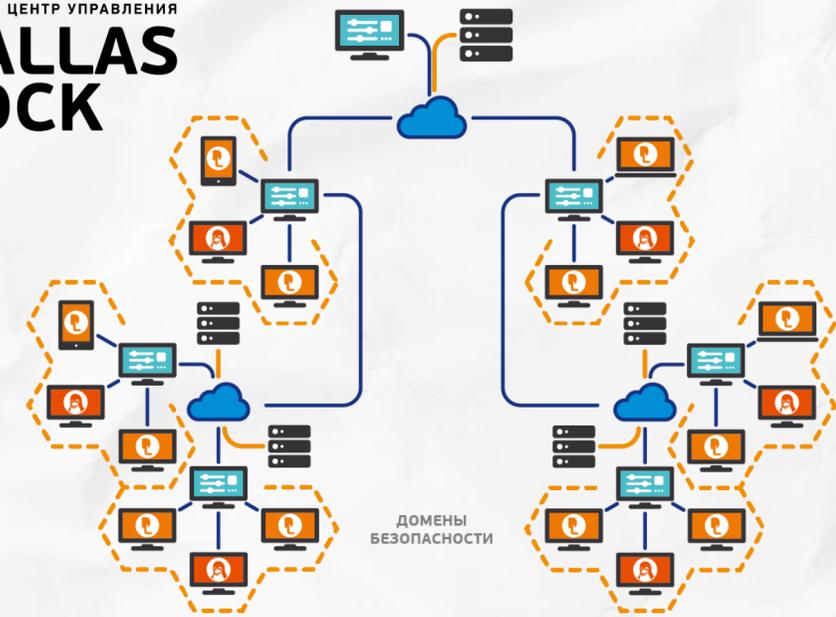


Сценарий 1:

Инвентаризация активов

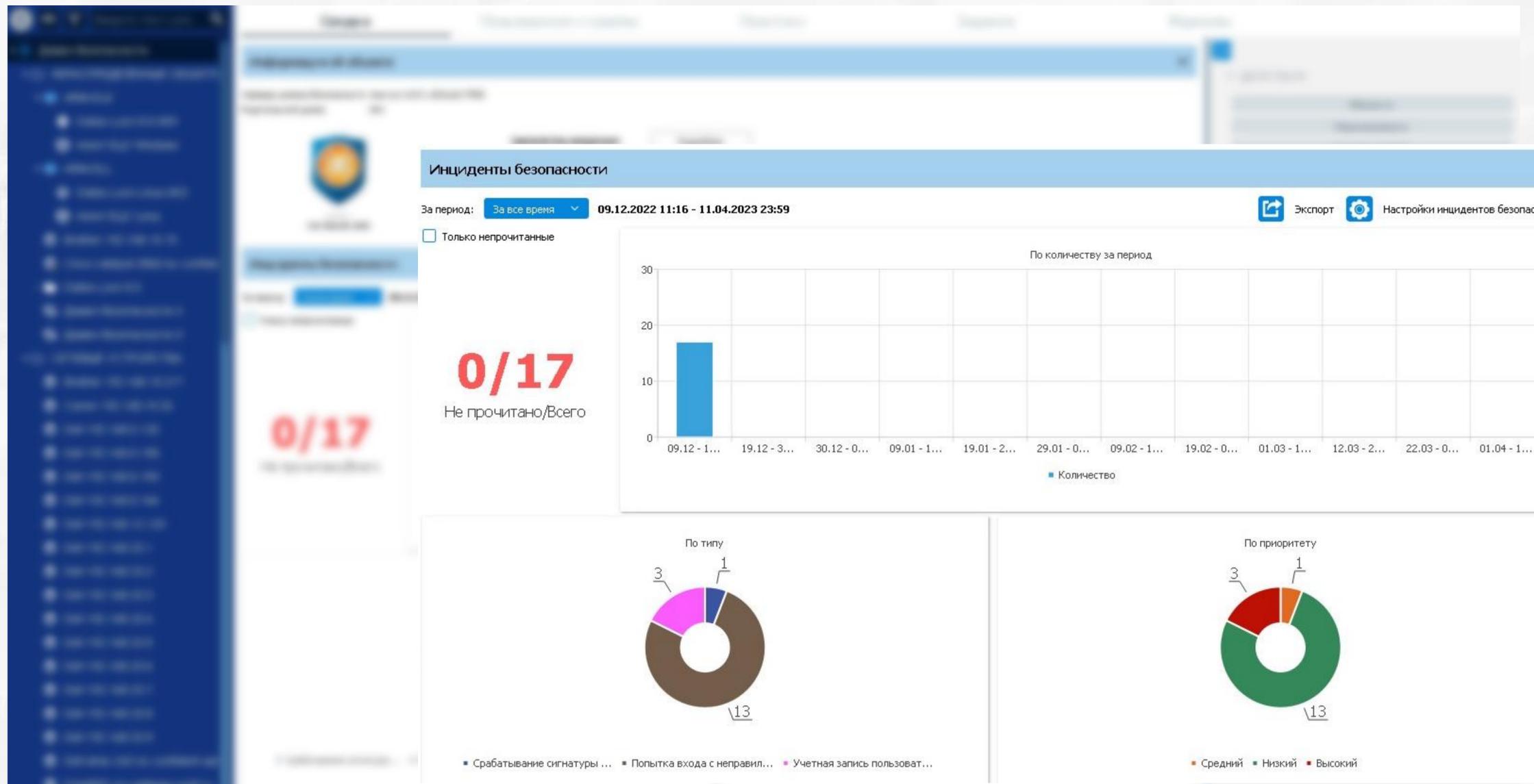


Единый центр управления Dallas Lock

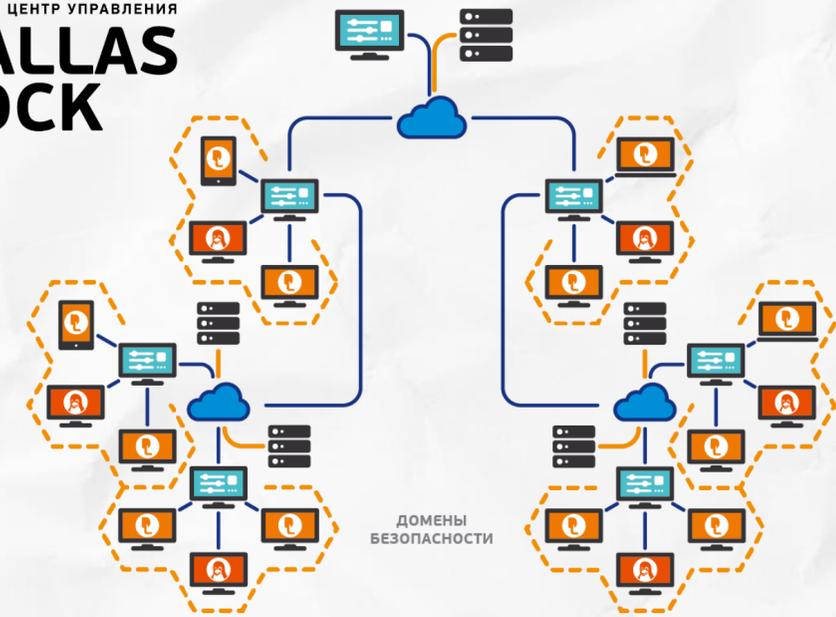


Сценарий 2:

Оповещение об инцидентах ИБ (консоль, email)



Единый центр управления Dallas Lock



Сценарий 3:

Управление пользователями/группами на СЗИ Dallas Lock

Консоль управления ЕЦУ [Домен безопасности: UccTestingDomain, Сервер: secsrv1.dl.local:17900]

Сводка **Пользователи и группы** Политики Задания Журналы

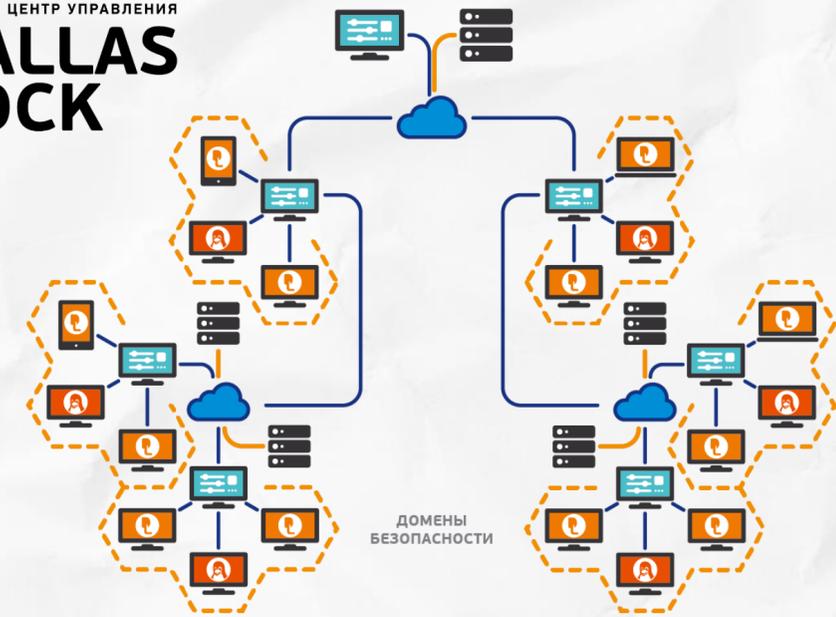
Пользователи Группы

Состояние	Учетная запись	Тип учетной записи ЕЦУ	Полное имя	Описание	Владелец	Роль администрирования
<input checked="" type="checkbox"/>	ISA	Все		Администр...	Локальный	Администратор
<input checked="" type="checkbox"/>	anonymous	DL8.0 ИК8	Анонимous ...	Использует...	Локальный	Не назначено

ОПЕРАЦИИ С ПОЛЬЗОВАТЕЛЯМИ

- Создать
- Удалить
- Свойства
- Сменить тип
- Синхронизировать
- Не синхронизировать
- Задать пароль

Единьй центр управления Dallas Lock



Сценарий 3:

Управление пользователями/группами на СЗИ Dallas Lock

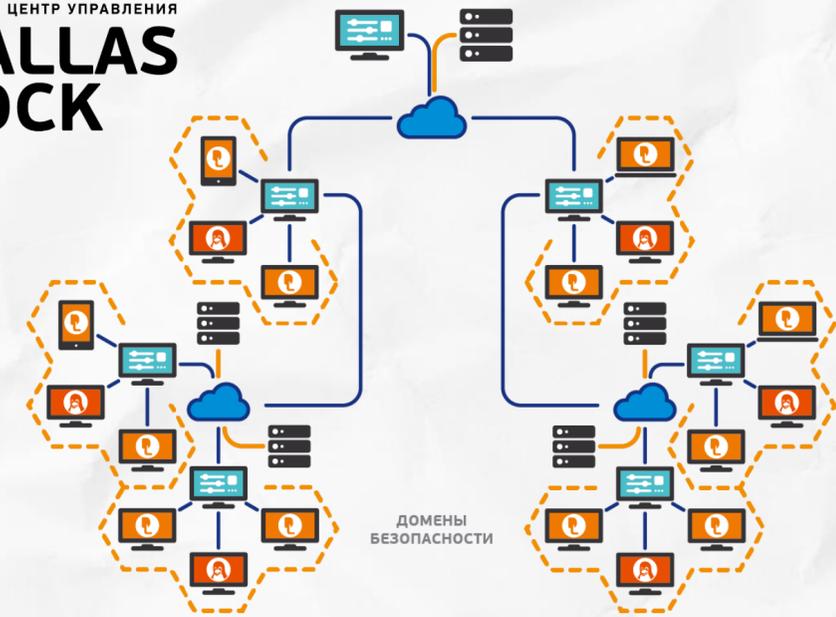
Редактирование полей пользователя

Имя пользователя: admin

Общие	Аппаратный идентификатор	апп.идентификатор не задан
Пароли	Описание	Администратор по умолчанию
Мандатный доступ	Полное имя	
Сеансы и расписание	Тип учетной записи Windows	Не указан
Запрет работы	Служебный пользователь Windows	Нет
Список групп	Не синхронизируемый пользователь	Нет
	Запрет входа при нарушении целостности	Нет
	Категория пользователей СДЗ	Пользователь
	Автовход в СЗИ НСД	Параметры не заданы
	Основная группа	
	Системный пользователь Linux	Нет
	Интерпретатор	/bin/bash
	Домашняя директория	
	Создать директорию	Да
	Администратор СЗИ Dallas Lock Linux	Нет
	Домен для Linux	

Сохранить Отмена

Единый центр управления Dallas Lock



Сценарий 3:

Управление пользователями/группами на СЗИ Dallas Lock

Назначение аппаратного идентификатора для v76-user-1

Предъявленные апп.идентификаторы: 2

Идентификатор: Dallas Lock - UCC license

Тип: Rutoken

Серийный номер: 3E624523

Метка: Dallas Lock - UCC license

Пользователь:

Пароль хранится в идентификаторе

Пароль защищен PIN кодом

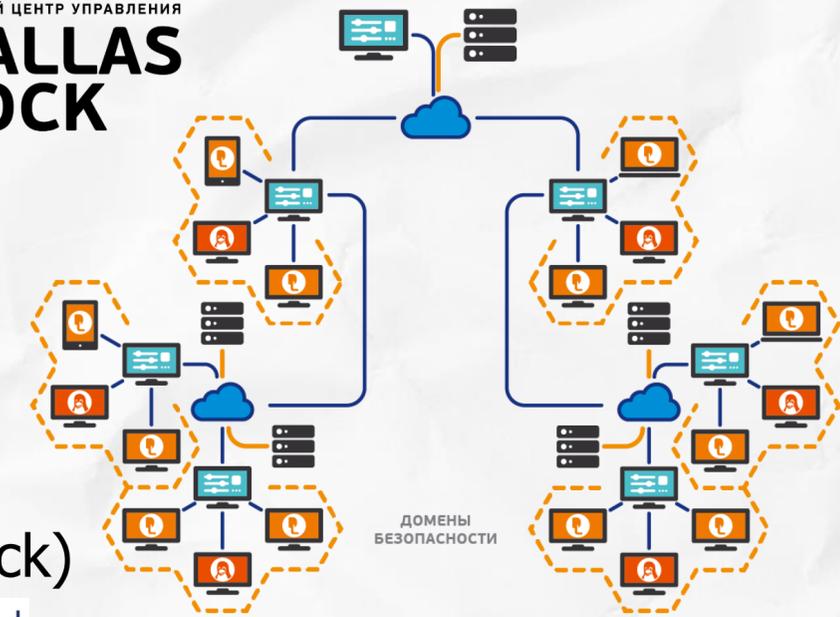
Назначение авторизационных данных

Действия с идентификатором

Записать Очистить Смена PIN кода... Форматировать

Применить Отмена

Единый центр управления Dallas Lock



Сценарий 4:

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

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

Сводка | Политики | Задания | Отчеты | Журналы

Информация об объекте

Последнее подключение	2022-01-12 12:02:59 (GMT+03:00)
Ввод в ДБ	2022-01-12 12:02:57 (GMT+03:00)
Версия ОС	Windows 10 Enterprise / Версия 21H1 (сборка ОС 19043.985)
FQDN-имя	Windows1021H1
Режим работы	Стандартный
IP-адрес	fe80::789c:fd50:a778:792b
MAC-адрес	00:50:56:A2:D0:85
Комментарий	

Инциденты безопасности

За период: **День** 12.01.2022

только непрочитанные

0/0 не прочитано/всего

Инциденты безопасности

■ Количество инцидентов безопасности

По типу | По приоритету

Журналы

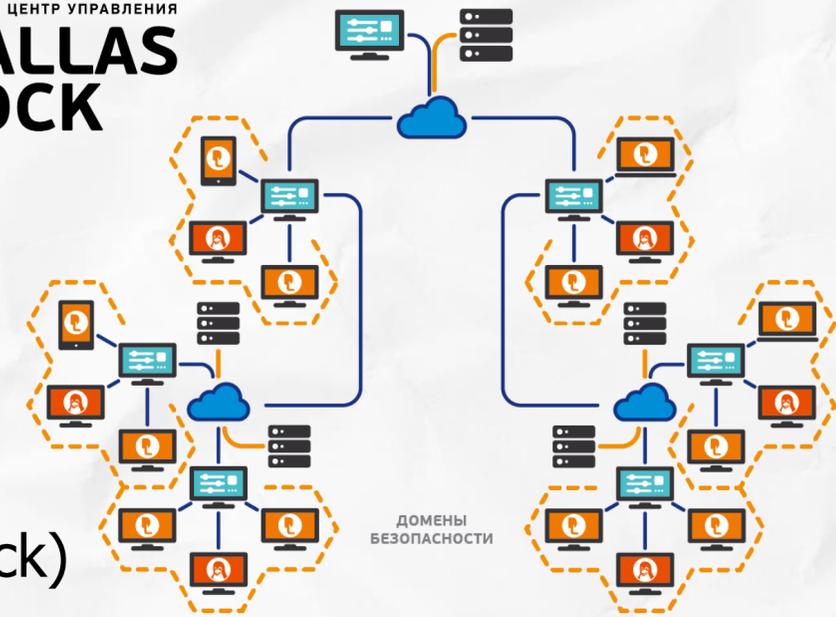
ОПЕРАТИВНОЕ УПРАВЛЕНИЕ

- Собрать журналы
- Синхронизировать
- Выключить
- Перезагрузить
- Удаленное управление

ДЕЙСТВИЯ

- Обновить
- Переименовать
- Создать группу
- Удалить
- Создать АРМ
- Сканировать сеть
- Добавить сетевое устройство
- Проверить доступность
- Проверить целостность
- Параметры авторизации
- Параметры подключения
- Подключить Консоль к подчиненному ДБ
- Комментарий

Единый центр управления Dallas Lock



Сценарий 4:

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

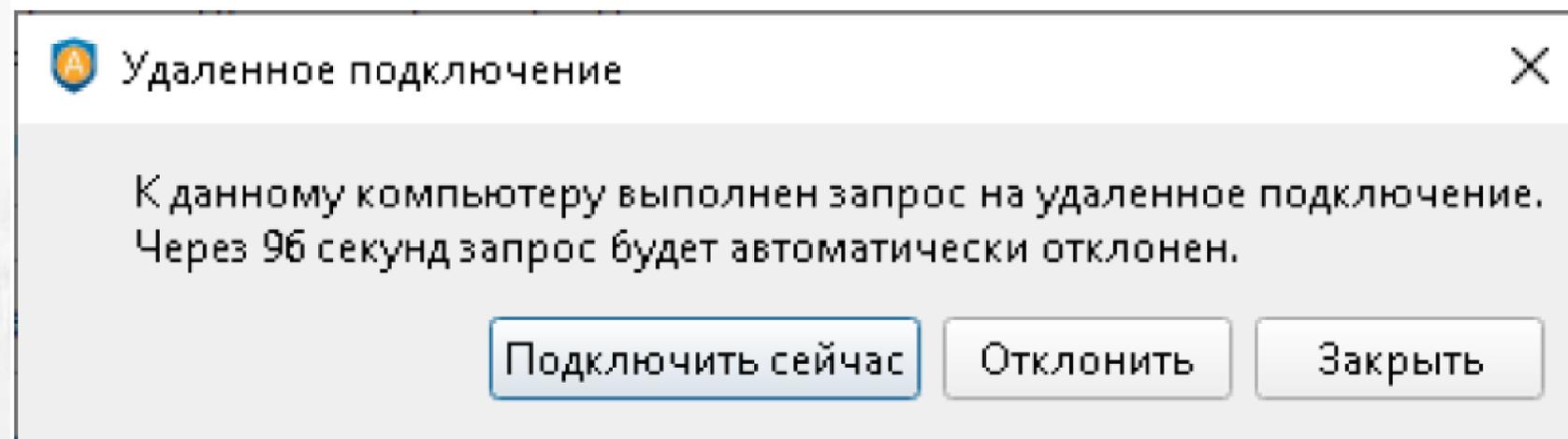


Рис. 205. Окно удаленного подключения на стороне АРМ с Агентом ЕЦУ

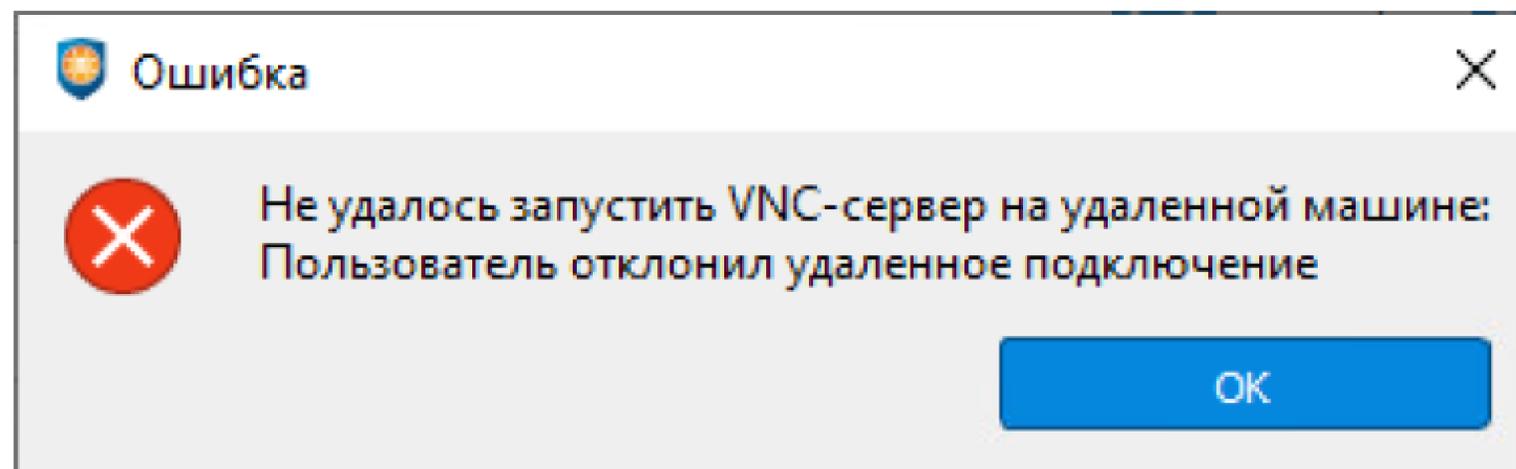
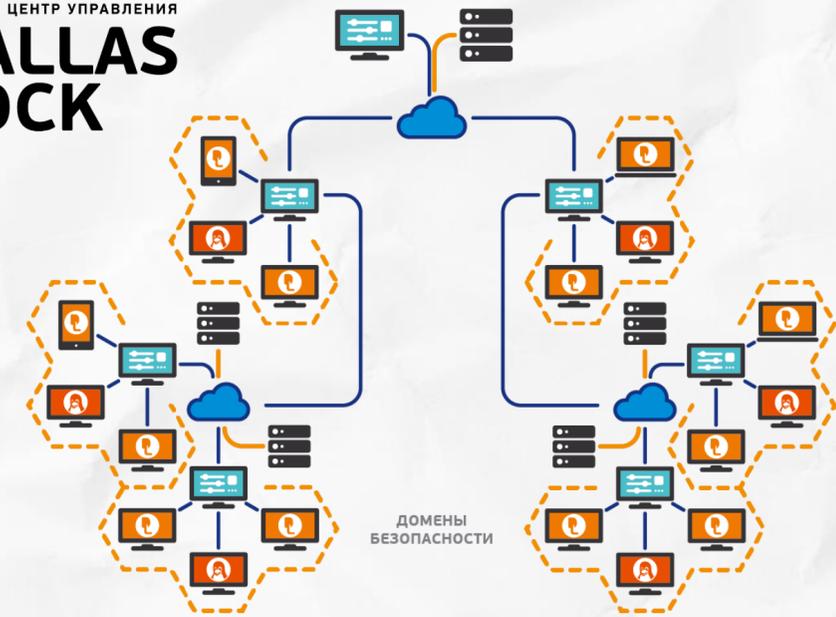


Рис. 206. Ошибка удаленного подключения

Единьй центр управления Dallas Lock



Сценарий 5:

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

Консоль управления ЕЦУ [Домен безопасности: v123-434c, Сервер: CZIOTIS406-26.isc.confident.spb.ru:17900]

Введите текст для поиска

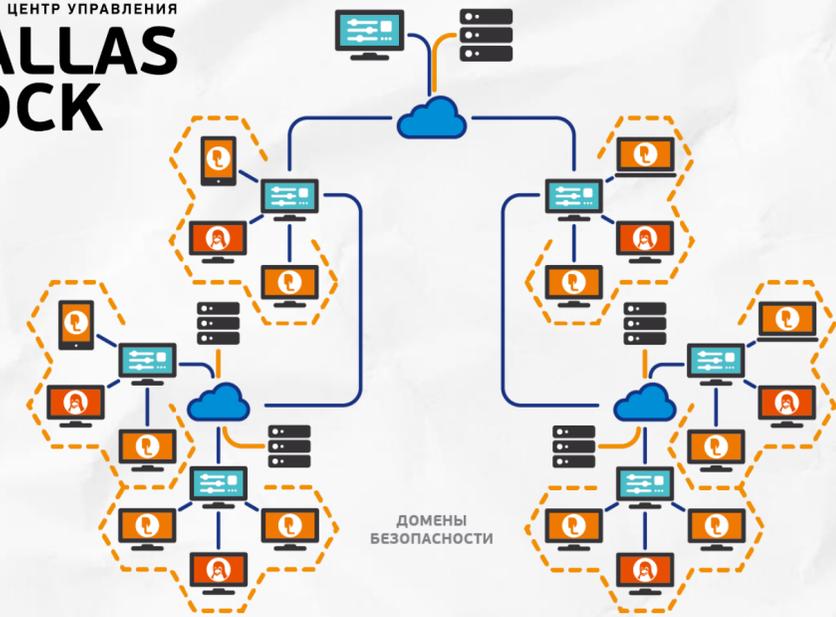
- ▼ v123-434c
 - ▼ НЕРАСПРЕДЕЛЁННЫЕ ОБЪЕКТЫ
 - ▼ ucc-centos-8
 - 🌐 Агент ЕЦУ Linux
 - ▼ СЕТЕВЫЕ УСТРОЙСТВА
 - 🌐 Cisco catalyst-3560.isc.confident.spb.ru
 - 🌐 Mikrotik mikrotik1.dl.local
 - 🌐 Mikrotik mikrotik3.dl.local

Сводка
Политики
Задания
Отчеты

Аудит

	Политика	Значение	Тип модуля
<input checked="" type="checkbox"/>	Наследуется		
<input checked="" type="checkbox"/>	(Агент ЕЦУ Linux) Журнал печати	Вкл.	Агент ЕЦУ Linux
<input checked="" type="checkbox"/>	(Агент ЕЦУ Linux) Журнал аутентификации	Вкл.	Агент ЕЦУ Linux
<input checked="" type="checkbox"/>	(Агент ЕЦУ Linux) Системный журнал	Вкл.	Агент ЕЦУ Linux
<input checked="" type="checkbox"/>	(Агент ЕЦУ Linux) Собирать только указанные уровни сообщений	Частичный выбор	Агент ЕЦУ Linux
<input checked="" type="checkbox"/>	(Агент ЕЦУ Linux) Журнал пользовательских сообщений	Вкл.	Агент ЕЦУ Linux

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 Пользователи и группы **Политики** Задания Журналы

Политики паролей	Политики авторизации	Аудит	Права пользователей
Контроль целостности: Политики	Режим работы СЗИ	Очистка остаточной информации	Политики ДСЧ
Мандатный доступ	Доступ	Сеть	Аппаратная идентификация

Политика | Значение

Блокировать автозапуск подключенных устройств | Нет

Блокируемые расширения

ДЕЙСТВИЯ

Не использовать

Свойства

ФИЛЬТРЫ

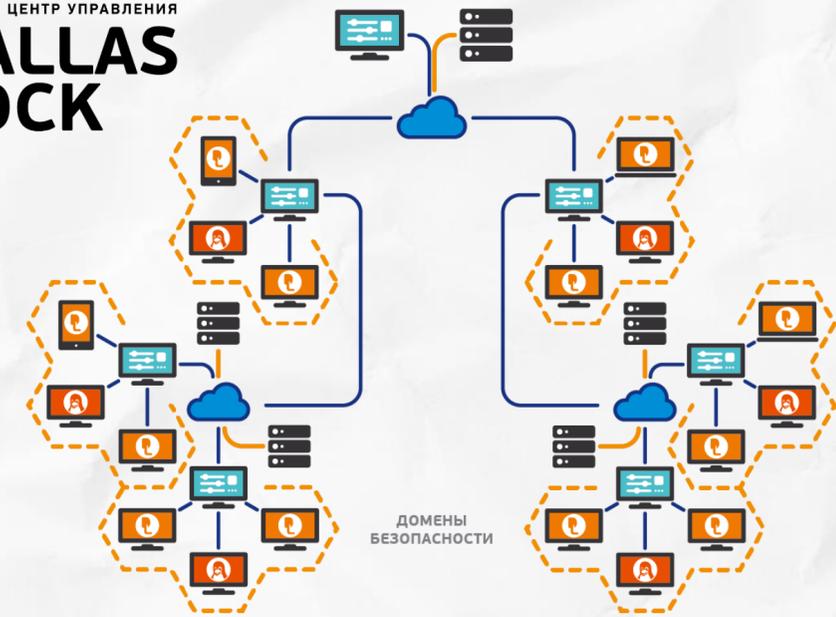
Имя политики *

Выбрать все | Очистить

- Система
- Dallas Lock 8.0 ИК8
- Dallas Lock 8.0 ИК9
- СДЗ Dallas Lock ИК4
- Dallas Lock Linux ИК2
- Dallas Lock Linux ИК3

Применить | Сбросить

Единый центр управления Dallas Lock



Сценарий 5:

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

Мастер создания задания

Выберите тип модуля

Агент ЕЦУ Windows

Выберите тип задания

Отчёт об аппаратном обеспечении

Отчёт об аппаратном обеспечении

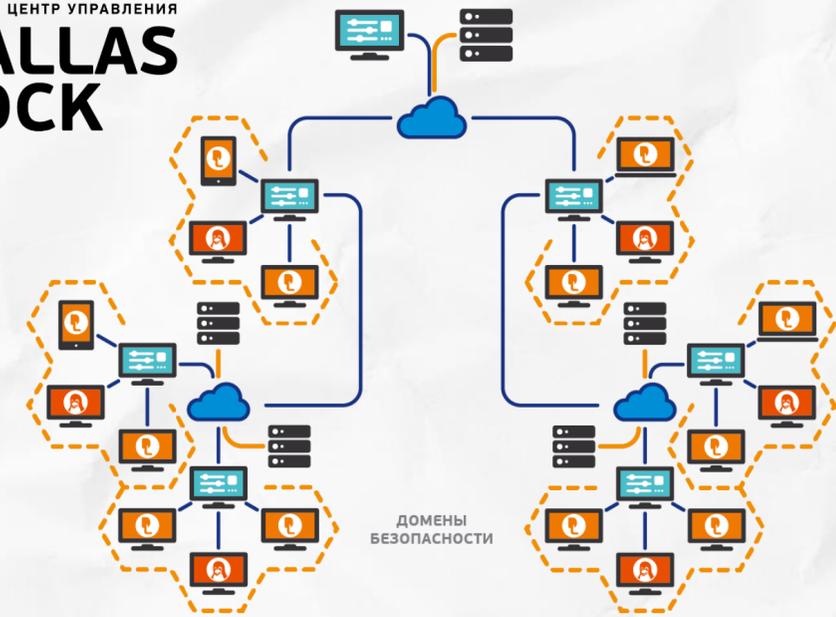
Удаление агента ЕЦУ

Отчёт о программном обеспечении

Создать

Отмена

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

Отчёт об аппаратном обеспечении **Отчёт о программном обеспечении**

Эталонный отчет (2022-01-17 12:20:22 (GMT+03:00)) Текущий отчет (2022-01-17 12:20:22 (GMT+03:00))

Эталонный отчет (2022-01-17 12:20:22 (GMT+03:00))	Текущий отчет (2022-01-17 12:20:22 (GMT+03:00))
1 Название пакета : accountsservice	1 Название пакета : accountsservice
2 Версия пакета : 0.6.45-lubuntu1.3	2 Версия пакета : 0.6.45-lubuntu1.3
3 Объем : 440 кБ	3 Объем : 440 кБ
4	4
5 Название пакета : acl	5 Название пакета : acl
6 Версия пакета : 2.2.52-3build1	6 Версия пакета : 2.2.52-3build1
7 Объем : 200 кБ	7 Объем : 200 кБ
8	8
9 Название пакета : aspi-support	9 Название пакета : aspi-support
10 Версия пакета : 0.142	10 Версия пакета : 0.142
11 Объем : 92 кБ	11 Объем : 92 кБ
12	12
13 Название пакета : aspid	13 Название пакета : aspid
14 Версия пакета : 1:2.0.28-lubuntu1	14 Версия пакета : 1:2.0.28-lubuntu1
15 Объем : 139 кБ	15 Объем : 139 кБ

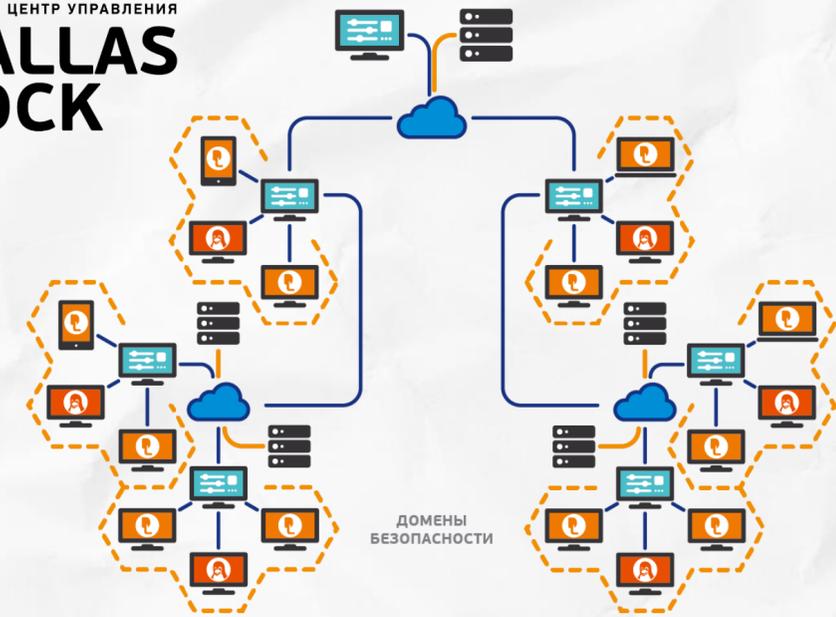
ДЕЙСТВИЯ

Применить изменения

Обновить

Сохранить в файл

Единый центр управления Dallas Lock



Сценарий 6:

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

Консоль управления ЕЦУ [Домен безопасности: Домен безопасности, Сервер: desktop-imaufq9.isc.confident.spb.ru:17900]

Сводка
Конфигурация
Журналы

Информация об объекте

Ввод в ДБ	2022-06-07 11:35:11 (GMT+03:00)
DNS-имя	
Адрес	192.168.15.32
Используемые протоколы	SNMP, SYSLOG
Контроль доступности	Вкл.
Контроль целостности	Вкл.
Модель	
Последнее время доступности устройства	2022-06-07 11:35:11 (GMT+03:00)
Последняя проверка доступности	2022-06-07 11:35:11 (GMT+03:00)
Последняя проверка целостности	2022-06-07 11:35:11 (GMT+03:00)
Производитель	Canon
Результат последней проверки КЦ	Нарушений нет
Результат последней проверки доступности	Доступен
Сообщество/Имя пользователя	public
Тип	PRINTER
Комментарий	

Инциденты безопасности

За период: Сегодня 07.06.2022 Экспорт Настройка

Только непрочитанные

По количеству: 5

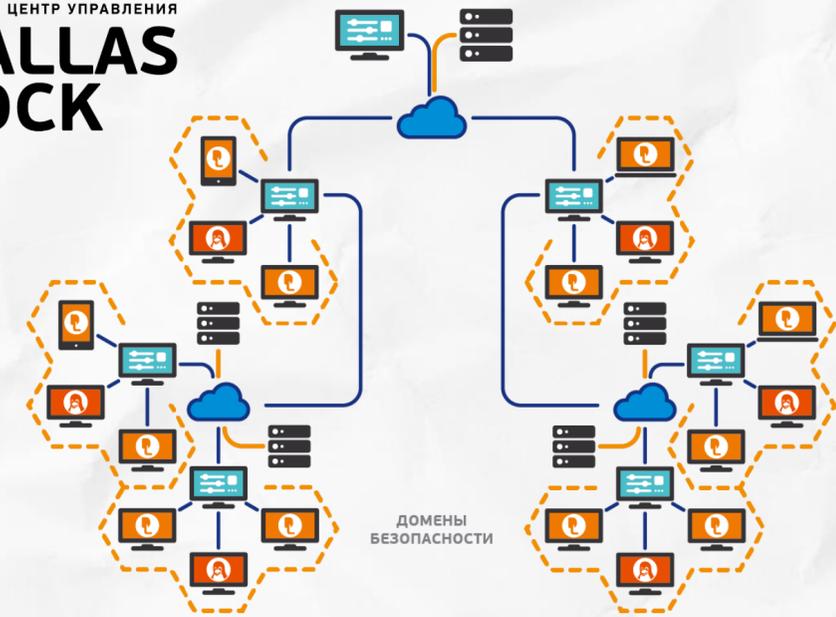
ДЕЙСТВИЯ

- Обновить
- Переименовать
- Создать группу
- Создать АРМ
- Сканировать сеть
- Добавить сетевое устройство
- Параметры авторизации
- Параметры подключения
- Проверить доступность
- Проверить целостность
- Подключить Консоль к подчиненному ДБ
- Комментарий
- Удалить

ОПЕРАТИВНОЕ УПРАВЛЕНИЕ

- Перезагрузить

Единый центр управления Dallas Lock



Сценарий 6:

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

Сводка
Конфигурация
Журналы

Введите текст для...

Домен безопасности

- НЕРАСПРЕДЕЛЁННЫЕ ОБЪЕКТЫ
- ▾ СЕТЕВЫЕ УСТРОЙСТВА
- Hewlett-Packard czipr308-130112
- УДАЛЁННЫЕ ОБЪЕКТЫ

SNMP

Показать только отличия

№	✓ гог	Параметр	Эталонное значение	Последнее значение
1	✓	Описание	HP ETHERNET MULTI-ENVIRONMENT,SN:CNB6GCVF...	HP ETHERNET MULTI-ENVIRONMENT,SN:CNB6GCVFQ...
2	✓	Идентификатор вендора	1.3.6.1.4.1.11.2.3.9.1	1.3.6.1.4.1.11.2.3.9.1
3	✓	Контакты	∅	∅
4	✓	Имя узла	CZIPR308-130112	CZIPR308-130112
5	✓	Расположение	∅	∅
6	✓	Сетевой уровень сервиса	72	72
7	✓	Количество сетевых интерфейсов	2	2

ДЕЙСТВИЯ

Применить изменения

Обновить

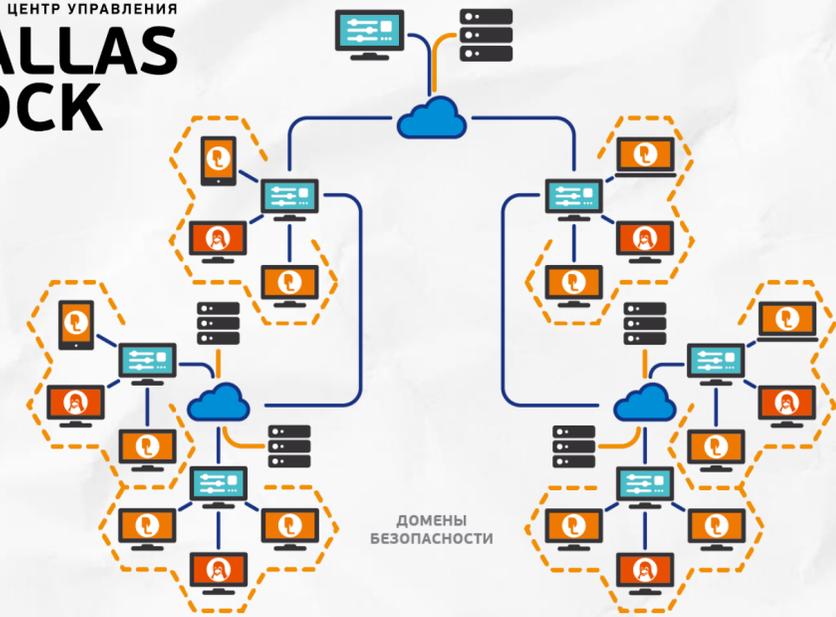
Сохранить в файл

Выключить контроль доступности

Добавить параметр

Удалить выделенные параметры

Единьй 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

