ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ
DALLAS LOCK

ЕДИНЫЙ **ЦЕНТР УПРАВЛЕНИЯ DALLAS LOCK**

ОБЗОР

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ

DALLAS LOCK

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Для оптимизации процесса настройки СЗИ, аудита и расследования инцидентов информационной безопасности в корпоративной сети с несколькими филиалами администратор информационной безопасности должен обладать инструментом, который позволил бы осуществить все это посредством одного интерфейса, единого центра управления (ЕЦУ).

ЕЦУ Dallas Lock – это средство централизованного управления, предназначенное для решения гораздо большего круга задач по сравнению с хорошо зарекомендовавшим себя Сервером безопасности Dallas Lock:

1. Централизованное управление решениями продуктовой линейки Dallas Lock:
- СЗИ НСД Dallas Lock 8.0 редакции «К» и «С»;
- СЗИ НСД Dallas Lock Linux;
- СЗИ ВИ Dallas Lock редакции «Стандартная» и «Расширенная»;
- СДЗ Dallas Lock уровня платы расширения;
- СДЗ Dallas Lock уровня базовой системы ввода-вывода;
- WAF Dallas Lock;
- и перспективные продукты компании.

2. Удаленная настройка, а также сбор журналов и отчетов с рабочих станций и серверов при помощи модуля Агент ЕЦУ.

3. Контроль целостности настроек сетевого оборудования по протоколам SNMP и SSH и сбор событий по Syslog.

4. Интеграция со сторонними продуктами:
- Антивирус Kaspersky;
- SIEM-системы;
- Active Directory.

Компания «Конфидент» выражает стремление создать продукт, который бы позволял контролировать безопасность всей ИТ-инфраструктуры организации вне зависимости от ее структуры и масштабов.

ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ

DALLAS LOCK

ЕДИНЫЙ
ЦЕНТР УПРАВЛЕНИЯ

ПРЕДПОСЫЛКИ СОЗДАНИЯ ЕЦУ DALLAS LOCK

Ранее централизованное управление несколькими компьютерами в ЛВС, защищенными изделиями продуктовой линейки Dallas Lock, осуществлялось только с помощью Сервера безопасности (СБ) Dallas Lock.

СБ Dallas Lock позволяет создавать отказоустойчивые домены безопасности и предоставляет следующие основные возможности:

- централизованное управление пользователями и группами пользователей на клиентских АРМ;
- централизованное управление политиками безопасности клиентских АРМ;
- централизованный сбор журналов;
- централизованное управление доступом к ресурсам файловой системы и к устройствам;
- контроль целостности объектов в рамках всего домена безопасности;
- просмотр состояния отдельных клиентских АРМ и удаленное управление ими;
- объединение клиентов в группы.

Вместе с тем СБ Dallas Lock обладает следующими архитектурными ограничениями:

- агентская схема защиты конечных точек не позволяет контролировать другие элементы ИТ-инфраструктуры (например, активное сетевое оборудование);
- допускается только «плоская» структура доменов безопасности (невозможно строить иерархию доменов), ограниченная функциональностью Менеджера серверов безопасности (МСБ) Dallas Lock;
- функционирование СБ Dallas Lock и МСБ Dallas Lock возможно только под управлением ОС Windows;
- в ИТ-инфраструктурах, в которых количество АРМ превышает несколько десятков тысяч, требуется создавать несколько доменов безопасности для безотказной работы системы защиты информации*.

ДОМЕНЫ БЕЗОПАСНОСТИ

МЕНЕДЖЕР СЕРВЕРОВ БЕЗОПАСНОСТИ

СЕРВЕР БЕЗОПАСНОСТИ

РЕШЕНИЯ ДЛЯ ЗАЩИТЫ АРМ С ОС WINDOWS:
СДЗ DALLAS LOCK +
DALLAS LOCK 8.0: СЗИ НСД, СКН-П, СКН-Н, МЭ, СОВ, РК

РЕШЕНИЯ ДЛЯ ЗАЩИТЫ АРМ С ОС LINUX:
СДЗ DALLAS LOCK +
DALLAS LOCK LINUX: СЗИ НСД, СКН-П, МЭ

* Сервер безопасности Dallas Lock не может управлять клиентскими АРМ, которые находятся за NAT (Network Address Translation).

МАСШТАБИРУЕМОСТЬ И ПРОИЗВОДИТЕЛЬНОСТЬ

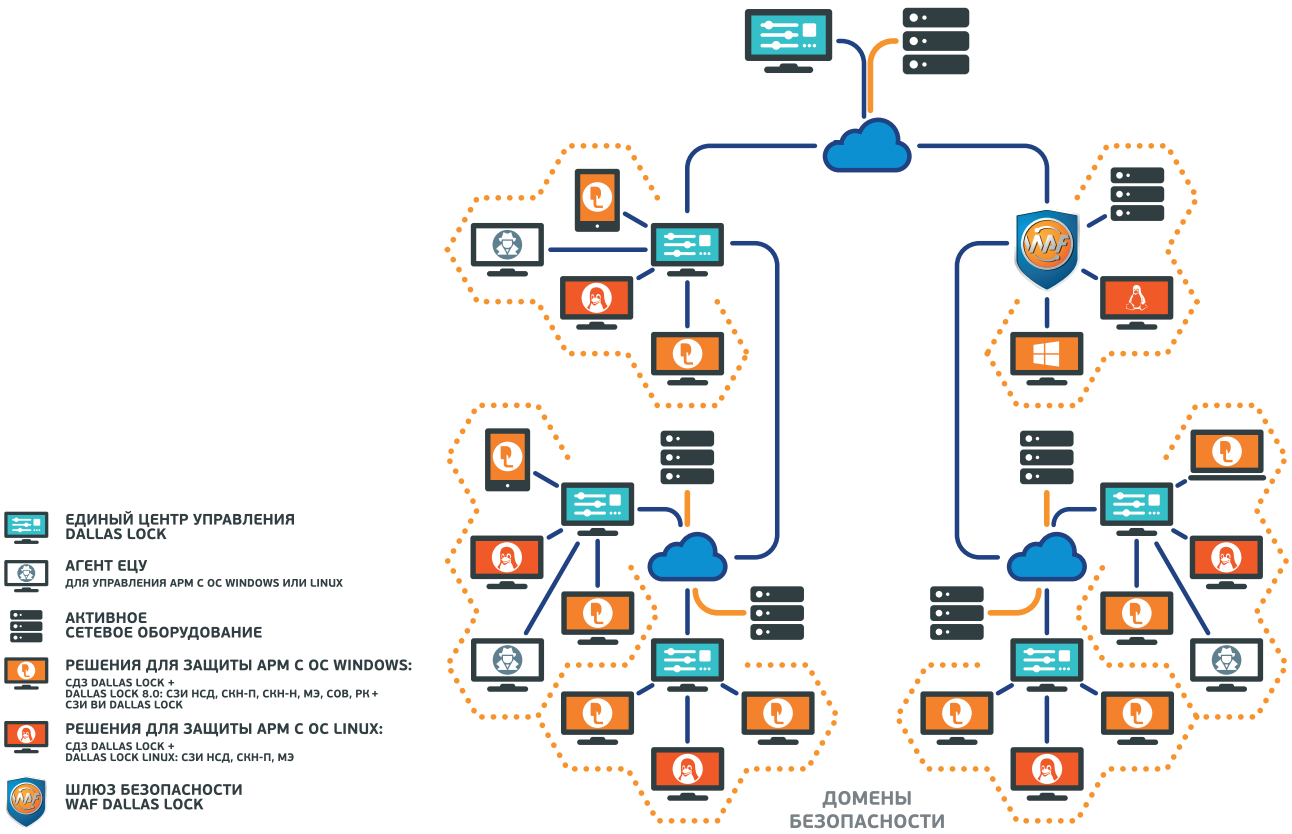
Для защиты гетерогенных систем (большое количество компьютеров, работающих на различных ОС, и сетевого оборудования) необходимо полноценное централизованное управление.

Когда количество компьютеров в инфраструктуре Заказчика составляет несколько десятков тысяч штук, то применение Сервера безопасности Dallas Lock подразумевает создание нескольких доменов безопасности, а также применение Менеджера серверов безопасности Dallas Lock и, как рекомендация, развертывание Сервера лицензий Dallas Lock.

ЕЦУ Dallas Lock фактически заменяет вышеперечисленные инструменты (Сервер безопасности, Менеджер серверов безопасности). Таким образом, обеспечиваются простота и удобство управления рабочими станциями на очень крупных внедрениях.

ЕЦУ Dallas Lock рекомендуется применять даже в небольших инфраструктурах, а при количестве защищаемых объектов (рабочие станции, серверы, сетевое оборудование) более 100 шт. использование ЕЦУ Dallas Lock строго обязательно.

За счет возможности построения отказоустойчивых кластеров из отдельных приложений ЕЦУ Dallas Lock возможно управление сложными гетерогенными инфраструктурами с количеством защищаемых объектов более 50 000 шт.



В таблице 1 представлены рекомендации по применению существующих инструментов централизованного управления ЕЦУ Dallas Lock в зависимости от количества клиентских рабочих станций.

Таблица 1. Рекомендации по применению инструментов централизованного управления ЕЦУ Dallas Lock в зависимости от количества рабочих станций

Количество клиентских АРМ	Сервер ЕЦУ	Кластер серверов ЕЦУ	Подчиненные ДБ	СУБД для хранения журналов ЕЦУ	Выгрузка событий в SIEM-систему
< 10	○				
10 – 5 000	●			○	
5 000 - 10 000	●	○	○	○	○
10 000 – 50 000+	●	●	●	●	●

○ – опционально, ● – рекомендуется применять.

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА ЕЦУ DALLAS LOCK

1. **Контроль состояния (целостности настроек) активного сетевого оборудования.** ЕЦУ Dallas Lock идентифицирует сетевое оборудование как объекты домена безопасности, а также осуществляет получение отчета о конфигурациях и мониторинг их изменений по протоколам SNMP и SSH для таких объектов.

Особенности:

- поддержка разных версий протокола SNMP (SNMPv1, SNMPv2, SNMPv3);
- сканирование сети для обнаружения SNMP- и SSH-клиентов;
- контроль целостности конфигурации активного сетевого оборудования, в том числе отдельных параметров OID;
- сигнализация о нарушении целостности;
- поддержка собственной расширяемой базы конфигурационных файлов.

2. **Возможность сохранения файла конфигурации ЕЦУ**, включающего в себя дерево домена безопасности, политики, учетные записи и группы для каждого узла дерева, с последующим применением сохраненного ранее файла конфигурации.

3. **Удаленная настройка**, а также сбор журналов и отчетов с рабочих станций и серверов без установленных средств и систем защиты информации с помощью отдельного кросс-платформенного модуля Агент ЕЦУ. Возможность удаленного подключения к клиентским машинам с помощью Агента ЕЦУ с доступом к рабочему столу пользователя.

4. **Контроль и управление Антивирусом Kaspersky**. А именно: получение журналов и информации об инцидентах и состоянии Антивируса Kaspersky, запуск принудительного сканирования и обновления антивирусных баз данных.

5. **Структурированное отображение объектов домена безопасности** в виде иерархии с наследованием значений параметров безопасности. Дерево доменов безопасности может быть сколько угодно большим и сложным. Переключение между настройками каждого домена безопасности происходит интуитивно понятно.

6. **Совместимость с ОС семейств Windows и Linux**. Работоспособность обеспечивается в том числе на российских дистрибутивах: Astra Linux Common Edition (релиз «Орел»), Astra Linux Special Edition (релиз «Смоленск»), Альт Рабочая станция (включая версию «СП»), Альт Сервер (включая версию «СП»), РЕД ОС 7.3 Муром, ROSA. Список поддерживаемых ОС постоянно пополняется.

7. **Управление СЗИ продуктовой линейки Dallas Lock на клиентских АРМ**, находящимися за NAT. Для корректного функционирования механизмов централизованного управления достаточно, чтобы клиентские АРМ «видели» ЕЦУ Dallas Lock. Новая технология сетевого взаимодействия СЗИ позволяет защищать информацию на удаленных компьютерах в сложных сетях.

8. **Управление шлюзом безопасности WAF Dallas Lock** с возможностью сбора журналов, просмотра подробной информации об объекте и списка инцидентов безопасности модуля с графической панелью. Кроме того, ЕЦУ Dallas Lock может создавать задания для создания/восстановления резервной копии, сбора журналов, сброса к заводским настройкам и обновления базы решающих правил.

9. **Гибкое управление настройками и правилами межсетевого экрана** для АРМ под управлением Dallas Lock 8.0, в том числе с возможностью создания новых правил МЭ с помощью простого и понятного пошагового мастера, а также дальнейшего их редактирования.

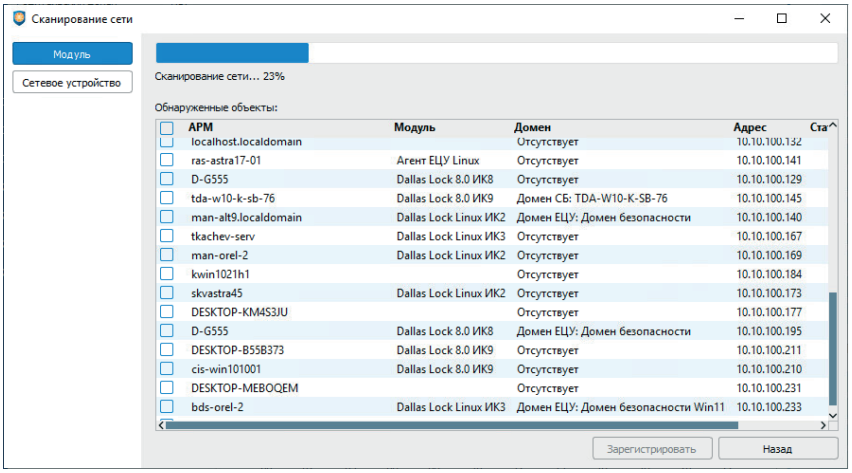
Помимо совершенно новых возможностей по контролю настроек активного сетевого оборудования, ЕЦУ Dallas Lock в том числе во многом повторяет функциональность СБ Dallas Lock, делая ее доступной на различных платформах под управлением ОС семейств Windows и Linux:

- репликация функциональности серверов;
- «бесшовная» интеграция с другими решениями продуктовой линейки Dallas Lock;
- настраиваемая система оповещений об инцидентах безопасности;
- использование единой системы управления учетными записями и параметрами безопасности объектов домена;
- управление доступом на основе ролей;
- отображение структуры домена в виде дерева;
- интеграция списка учетных записей и групп пользователей с Active Directory;
- объединение компьютеров в группы для удобства аудита и управления;
- централизованное отслеживание состояния целостности объектов домена безопасности;
- ведение централизованного аудита событий домена безопасности;
- удаленное развертывание средств защиты информации на АРМ;
- общая графическая панель мониторинга защищенности системы с отображением статистики;
- графическое представление информации об инцидентах на разных уровнях иерархии домена безопасности;
- управление широким перечнем аппаратных идентификаторов.

ЗАЯВКА НА ДЕМОВЕРСИЮ
ОТСКАНИРУЙТЕ QR-КОД

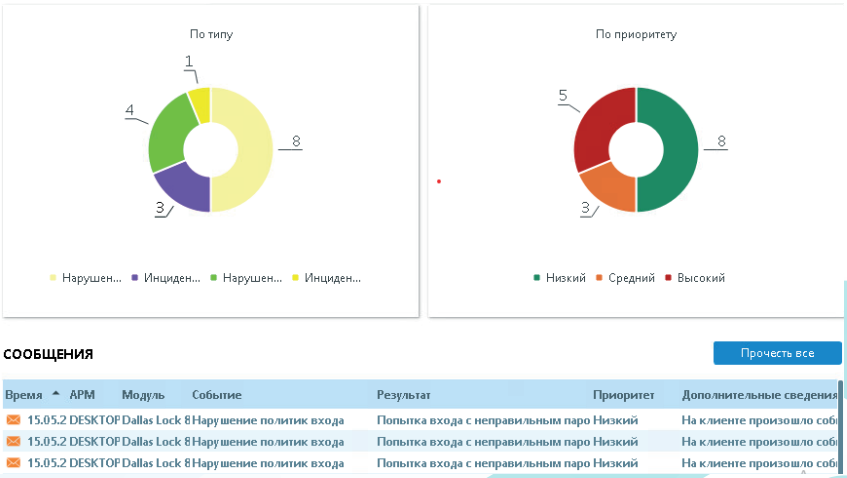
ОСНОВНЫЕ СЦЕНАРИИ ПРИМЕНЕНИЯ

1. Сканирование сети для обнаружения установленных средств защиты информации Dallas Lock, Агентов ЕЦУ и сетевого оборудования для последующего введения под управление ЕЦУ Dallas Lock.

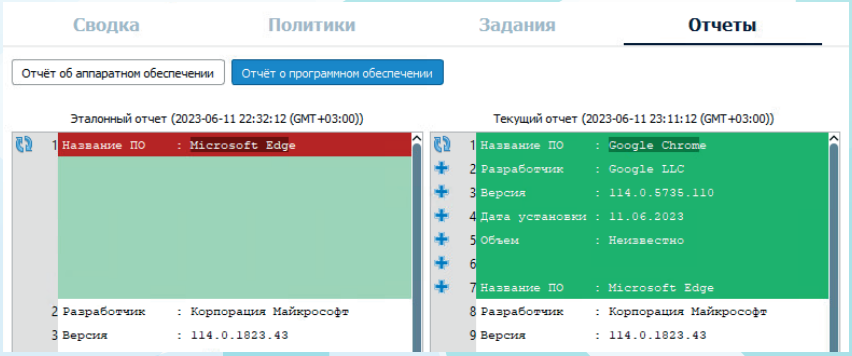


2. Централизованное управление учетными записями и политиками безопасности средств защиты информации Dallas Lock.

3. Мониторинг событий безопасности на разных уровнях иерархии и работа с подсистемой аудита.



4. Сбор отчетов об аппаратном и программном обеспечении с возможностью сравнения собранных отчетов с эталонным значением.



5. Удаленное управление рабочими станциями с доступом к рабочему столу пользователя без установленных СЗИ при помощи Агента ЕЦУ.

6. Централизованная инсталляция и деинсталляция средств защиты информации Dallas Lock на рабочие станции.

7. Управление конфигурацией активного сетевого оборудования с возможностью контроля за изменениями.

№	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	MikrotikVM	MikrotikVM
5	☑	Расположение	Main Office	Main Office
6	☑	Сетевой уровень сервиса	78	78
7	☑	Количество сетевых интерфейсов	1	1
8	☑	Имя интерфейса	ether1	ether-changed

8. Создание, настройка и управление правилами межсетевого экрана для АРМ под управлением Dallas Lock 8.0.

№	Имя правила	Направление передачи	Тип правила	Параметры протоколов
1	ICMPv6 по умолчанию (входящее)	Входящие пакеты	ICMPv6-правило	ICMP- сообщения: 3,133,135,129,136
2	ICMP по умолчанию (входящее)	Входящие пакеты	ICMP-правило	ICMP- сообщения: 3,8,10,11;
3	HTTP/ HTTPS клиент	Исходящие пакеты	TCP/UDP-правило	Локальные TCP-порты: Все; Внешн
4	IGMP	Любые пакеты	IGMP-правило	Все
5	ARP	Любые пакеты	ARP-правило	IP-адрес отправителя: Все; IP-адрес
6	Локальные сетевые папки	Любые пакеты	TCP/UDP-правило	Локальные TCP-порты: 139,445,135;
7	DNS клиент	Любые пакеты	TCP/UDP-правило	Локальные TCP-порты: Все; Внешн
8	DHCP клиент	Любые пакеты	TCP/UDP-правило	Локальные TCP-порты: Все; Внешн
9	Internet Explorer HTTP/ HTTPS	Любые пакеты	TCP/UDP-правило	Локальные TCP-порты: Все; Внешн
10	yandex.ru	Исходящие пакеты	IP-правило	Локальный IP-адрес: Все; Внешний
11	Внешние сетевые папки	Любые пакеты	TCP/UDP-правило	Локальные TCP-порты: Все; Внешн
12	DL СБ (входящее)	Входящие пакеты	TCP/UDP-правило	Локальные TCP-порты: 17490,17491
13	DL СБ (исходящее)	Исходящие пакеты	TCP/UDP-правило	Локальные TCP-порты: Все; Внешн
14	LDAP	Любые пакеты	TCP/UDP-правило	Локальные TCP-порты: 389; Внешн
По умолчан...	Действие с пакетами, не попавш...	Любые пакеты		

ПЕРЕХОД С СБ DALLAS LOCK НА ЕЦУ DALLAS LOCK

Разработан мастер миграции, который позволяет администратору безопасности без больших временных затрат и проведения повторной настройки реализовать переход с СБ Dallas Lock на ЕЦУ Dallas Lock.

Миграция позволяет осуществить перенос следующих параметров СБ:

- структура дерева ДБ;
- учетные записи;
- политики безопасности.

Мастер миграции позволяет переносить данные следующих продуктов: СЗИ НСД Dallas Lock 8.0-К/С, СЗИ НСД Dallas Lock Linux и СДЗ Dallas Lock.
В будущем появится возможность мигрировать настройки и политики МЭ и СКН с СБ Dallas Lock на ЕЦУ Dallas Lock.

РАЗВИТИЕ ПРОДУКТА

В следующих версиях ЕЦУ Dallas Lock планируется постепенная реализация следующих функциональных возможностей:

- расширение интеграции с решениями продуктовой линейки Dallas Lock в части централизованного управления компонентами МЭ, СОВ, СКН и РК;
- интеграция с доменными службами FreeIPA, Samba, а также с отечественными системами централизованного управления Astra Linux Directory и РЕД АДМ;
- расширение возможностей централизованного управления пользователями, группами и аппаратными идентификаторами;
- реализация предустановленных настроек политик безопасности (шаблонов) соответствующим стандартам;
- анализ уязвимостей и оценка защищенности сетевого оборудования с рекомендациями по настройке для администратора исходя из лучших практик;
- расширение возможностей удаленного управления рабочими станциями без установленных СЗИ;
- управление рисками информационной безопасности;
- оценка влияния инцидентов безопасности на ключевые показатели эффективности организации.

ЗАКЛЮЧЕНИЕ

Продукт ЕЦУ Dallas Lock совместно с Агентом ЕЦУ являются новым шагом в развитии инструментов централизованного управления продуктовой линейки Dallas Lock, появление которого было обусловлено необходимостью предоставить пользователям наиболее эффективный и унифицированный инструмент для развертывания и администрирования системы защиты.

ЕЦУ Dallas Lock — это кросс-платформенное решение, которое функционирует в том числе на сертифицированных российских ОС.

Благодаря широкому набору функциональных возможностей и сценариев применения, ЕЦУ Dallas Lock выгодно выделяется на фоне СБ Dallas Lock и рекомендован к использованию вместо него.

ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ
DALLAS LOCK

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

192029, г. Санкт-Петербург
пр. Обуховской Обороны, д. 51, лит. К
телефон/факс: (812) **325-1037**

http://www.**confident**.ru/
http://www.**dallaslock**.ru/
e-mail:
isc@confident.ru - коммерческие вопросы
helpdesk@confident.ru - техническая поддержка

Схема проезда: