КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Использование продуктов Dallas Lock для построения системы защиты информации

Иван Дятлов

ВЕДУЩИЙ МЕНЕДЖЕР ПО РАБОТЕ С ПАРТНЕРАМИ ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ ГК «КОНФИДЕНТ»

EMAIL: DIM@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU

Dallas Lock 8.0

Dallas Lock Linux

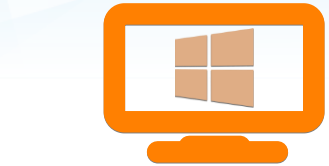
СДЗ Dallas Lock

СЗИ ВИ Dallas Lock

WAF Dallas Lock

Набор решений для защиты информации в физических и виртуализированных средах с централизованным управлением



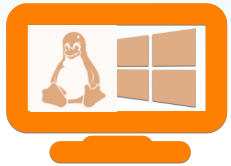
СДЗ Dallas Lock

СЗИ Dallas Lock 8.0

СДЗ Dallas Lock

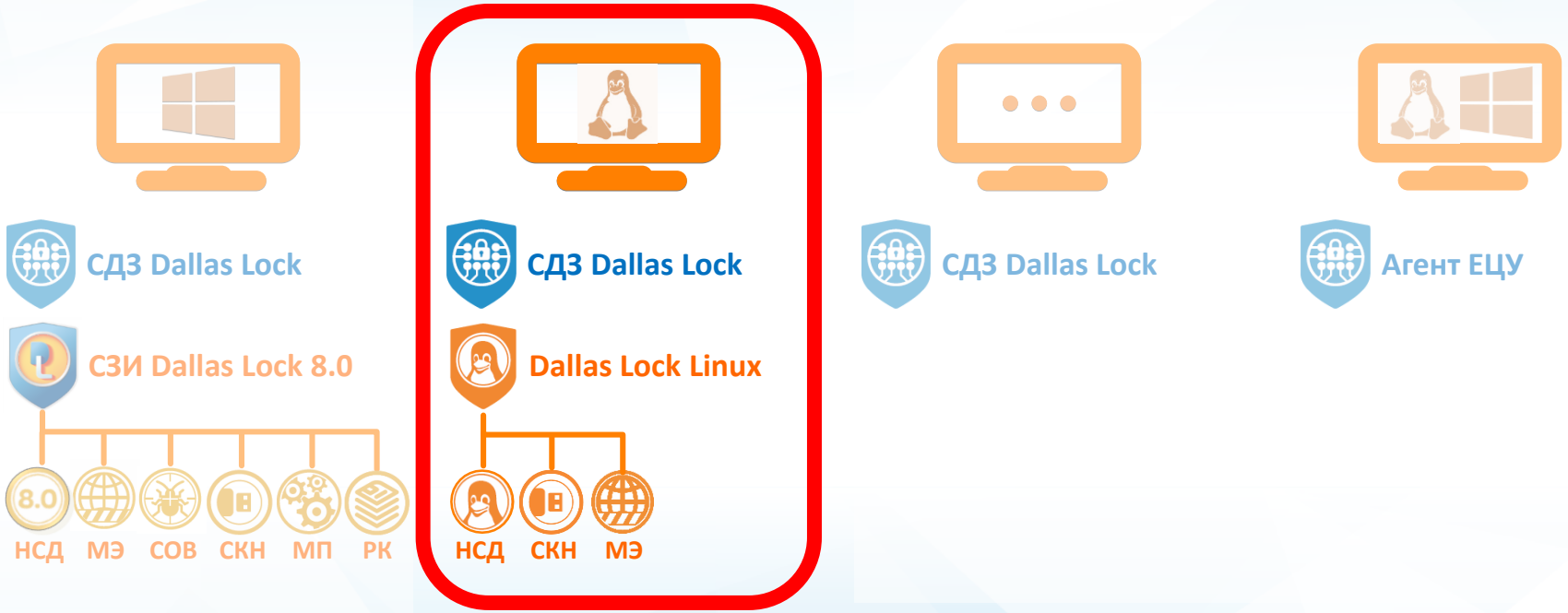
Dallas Lock Linux

СДЗ Dallas Lock



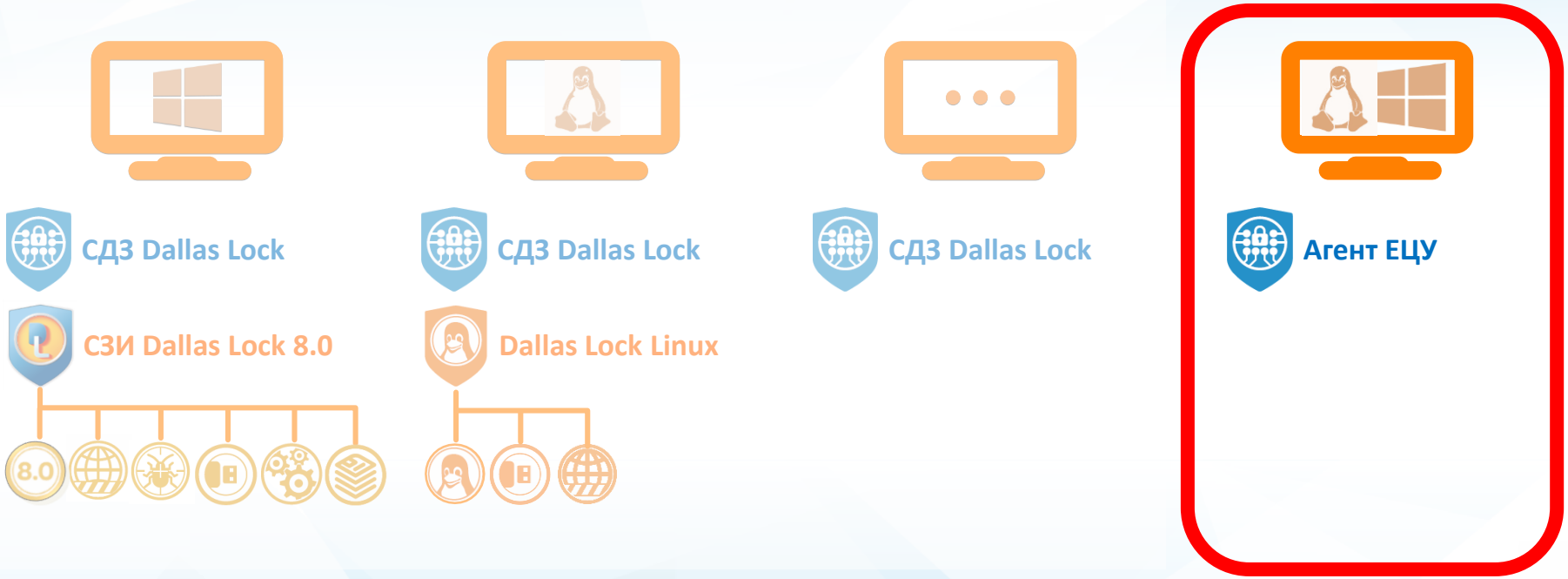
Агент ЕЦУ

СДЗ, СЗИ от НСД, МЭ, СОВ, СКН, МП и РК для ОС Windows



СДЗ, СЗИ от НСД, СКН и МЭ для ОС Linux, включая российские ОС

СДЗ для любых ОС



Агент ЕЦУ для ОС Windows и Linux

СДЗ Dallas Lock

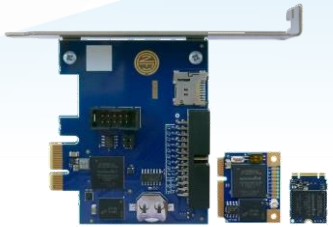
средство доверенной загрузки Dallas Lock — это два решения, которые блокируют попытки несанкционированной загрузки нештатной операционной системы. Используются для защиты конфиденциальной информации и информации, содержащей сведения, составляющие государственную тайну до уровня «совершенно секретно» включительно

СДЗ ПР Dallas Lock

средство доверенной загрузки уровня платы расширения

СДЗ УБ Dallas Lock

средство доверенной загрузки уровня базовой системы ввода-вывода



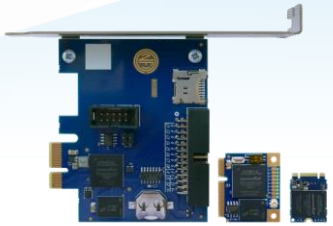
СДЗ ПР Dallas Lock

решение уровня платы расширения для защиты конфиденциальной информации и информации, содержащей сведения, составляющие государственную тайну до уровня «совершенно секретно» включительно

PCI-Express

Mini PCI-Express

M.2



СДЗ ПР Dallas Lock

решение уровня платы расширения для защиты конфиденциальной информации и информации, содержащей сведения, составляющие государственную тайну до уровня «совершенно секретно» включительно

В новой версии реализовано:

- администрирование и централизованное управление проводятся без использования ресурсов штатной ОС;
- полноценная поддержка UEFI и безопасного режима загрузки UEFI («Secureboot»);
- собственные часы с независимым источником питания;
- возможность отслеживать вскрытие корпуса выключенного компьютера;
- поддержка широкого спектра аппаратных идентификаторов.

СДЗ УБ Dallas Lock

решение уровня базовой системы ввода-вывода для защиты конфиденциальной информации и информации, содержащей сведения, составляющие государственную тайну до уровня «совершенно секретно» включительно

Ключевые возможности:

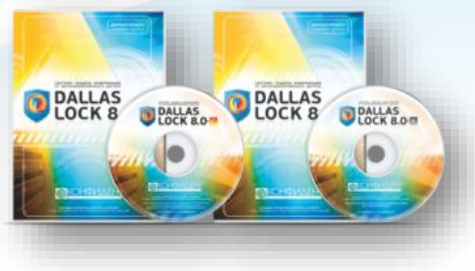
- блокировка загрузки нештатной операционной системы;
- контроль целостности программно-аппаратной среды;
- поддержка широкого спектра аппаратных идентификаторов;
- возможность централизованного управления в составе домена безопасности.

СДЗ УБ Dallas Lock

решение уровня базовой системы ввода-вывода для защиты конфиденциальной информации и информации, содержащей сведения, составляющие государственную тайну до уровня «совершенно секретно» включительно

Сертификат ФСТЭК России
по 2 классу защиты СДЗ уровня BIOS (ИТ.СДЗ.УБ2.ПЗ)
по 2 уровню доверия (УД 2)

Включен в единый реестр российских программ для ЭВМ и БД. Запись в реестре № 20592 от 14.12.2023 г.



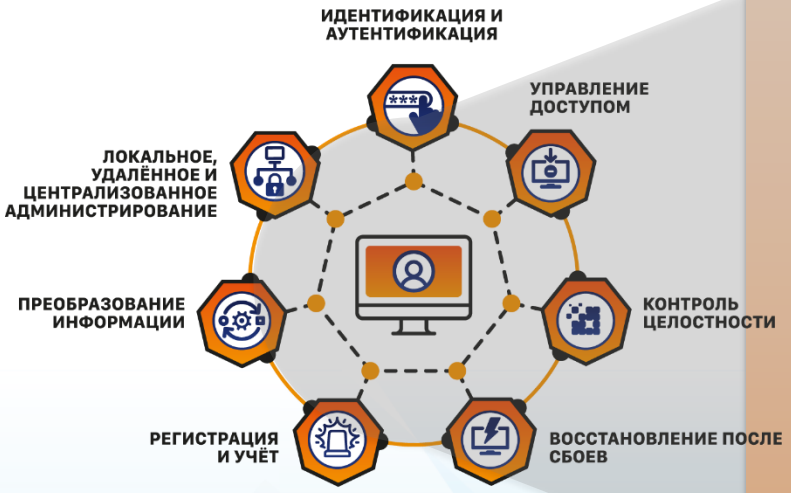
СЗИ Dallas Lock 8.0 для ОС Windows™

сертифицированная система защиты информации накладного типа для автономных АРМ и сложных сетевых инфраструктур

Dallas Lock 8.0-К
защита конфиденциальной информации

Dallas Lock 8.0-С
защита конфиденциальной информации и гостайны

Защита от НСД



Набор подключаемых модулей

МЭ — распределенный персональный межсетевой экран с централизованным управлением, аудитом событий ИБ

СОВ — гибридная система обнаружения и предотвращения вторжений уровня узла в программном исполнении

СКН — программное решение для контроля подключения устройств и отчуждения информации

МП — модуль паспортизации программного обеспечения для контроля его использования пользователями

РК — модуль резервного копирования произвольных пользовательских файлов и каталогов

СЗИ Dallas Lock 8.0 для ОС Windows™

сертифицированная система защиты информации накладного типа для автономных АРМ и сложных сетевых инфраструктур

В новой версии реализовано:

- совместимость с аппаратным идентификатором Guardant ID 2.0;
- автоматизированная миграция с СБ на ЕЦУ Dallas Lock;
- механизм защиты от вирусов-шифровальщиков.

Механизм защиты от вирусов-шифровальщиков

- является неотъемлемой частью модуля СОВ;
- имеет несколько режимов работы и возможность создания исключений;
- использует эвристические методы обнаружения;
- детектирует и принудительно завершает работу вредоносного ПО;
- восстанавливает зашифрованные файлы из теневых копий*;
- оповещает администратора об инциденте.

* Теневые копии начинают создаваться в момент обнаружения подозрительной активности. Механизм восстановления реализован и будет доступен в следующей версии Dallas Lock 8.0.

СЗИ Dallas Lock Linux

сертифицированная система защиты информации накладного типа для защиты конфиденциальной информации

Red Hat Enterprise Linux Server 7

CentOS 7

Альт 8 СП релиз 10
Альт Рабочая станция 9.0, 9.1, 9.2, 10, 10.1
Альт Сервер 10

Debian 10, 11

Ubuntu 18.04, 20.04

РЕД ОС 7.1, 7.2, 7.3 Муром

Astra Linux Special Edition 1.7

Astra Linux Common Edition 2.12, 2.12.40

ROSA Enterprise Linux Desktop/Server 7.3

Защита от НСД

Подключаемые модули

СКН — Средство контроля съёмных машинных носителей информации уровня подключения

МЭ — Межсетевой экран уровня узла

СОВ — Система обнаружения и предотвращения вторжений уровня узла*

* Получение сертификата соответствия планируется в 4 кв. 2024 г.

СЗИ Dallas Lock Linux

сертифицированная система защиты информации накладного типа для защиты конфиденциальной информации

В новой версии реализовано:

- расширен список поддерживаемых ОС, включая отечественные: Альт Linux, Astra Linux, РЕД ОС, ROSA;
- отказ от технологии подмены штатного ядра ОС;
- собственная дискреционная модель разграничения прав доступа на основе POSIX ACL;
- сертифицированный модуль МЭ (ИТ.МЭ.В4.ПЗ).

Система обнаружения вторжений уровня узла

- Консольная и графическая оболочки администрирования
- Анализ сетевого трафика
- Анализ событий журналов ОС
- Эвристический анализ
- Механизм обновления сигнатур

*** Получение сертификата соответствия планируется в 4 кв. 2024 г.**

СЗИ Dallas Lock Linux

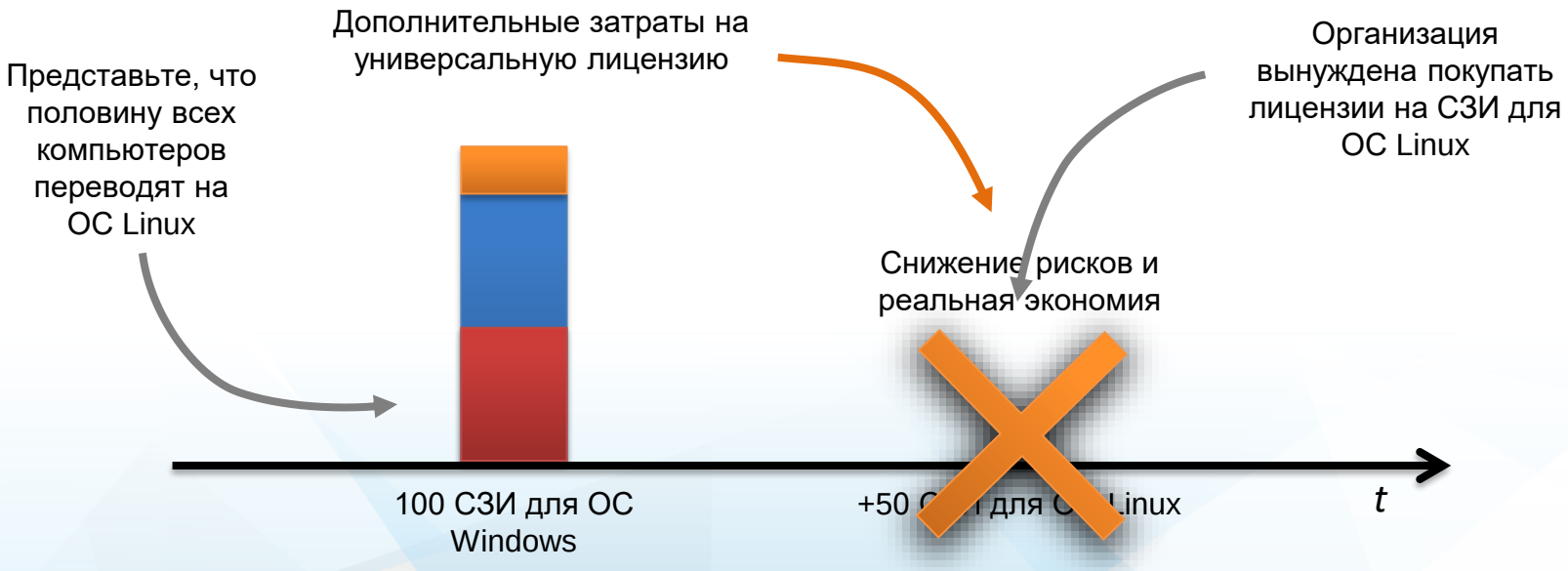
сертифицированная система защиты информации накладного типа для защиты конфиденциальной информации

Построение комплексной системы защиты информации в гетерогенной среде

+

универсальная лицензия на СЗИ

Пример


Представьте, что половину всех компьютеров переводят на ОС Linux
Дополнительные затраты на универсальную лицензию
Организация вынуждена покупать лицензии на СЗИ для ОС Linux
Снижение рисков и реальная экономия
100 СЗИ для ОС Windows
+50 СЗИ для ОС Linux
t

Универсальная лицензия даёт право на использование
СЗИ Dallas Lock 8.0-К (для ОС Windows™) или СЗИ НСД Dallas Lock Linux
по усмотрению конечного пользователя

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

СЗИ ВИ Dallas Lock

сертифицированная система защиты информации в виртуальных инфраструктурах, предназначенная для комплексной многофункциональной защиты конфиденциальной информации от несанкционированного доступа в виртуальных средах на базе oVirt, zVirt, «РЕД Виртуализация», HOSTVM, KVM, VMware vSphere и Microsoft Hyper-V

vmware®

- VMware vSphere 5.5
- VMware vSphere 6.0
- VMware vSphere 6.5
- VMware vSphere 6.7
- VMware vSphere 7.0

Microsoft Hyper-V

- Microsoft Hyper-V Server 2016
- Microsoft Hyper-V Server 2019

KVM

- Astra Linux Common Edition «Орёл»
- Astra Linux Special Edition «Смоленск»
- CentOS 7.5.1804
- Linux Mint 18.3
- Ubuntu 18.04.2 LTS

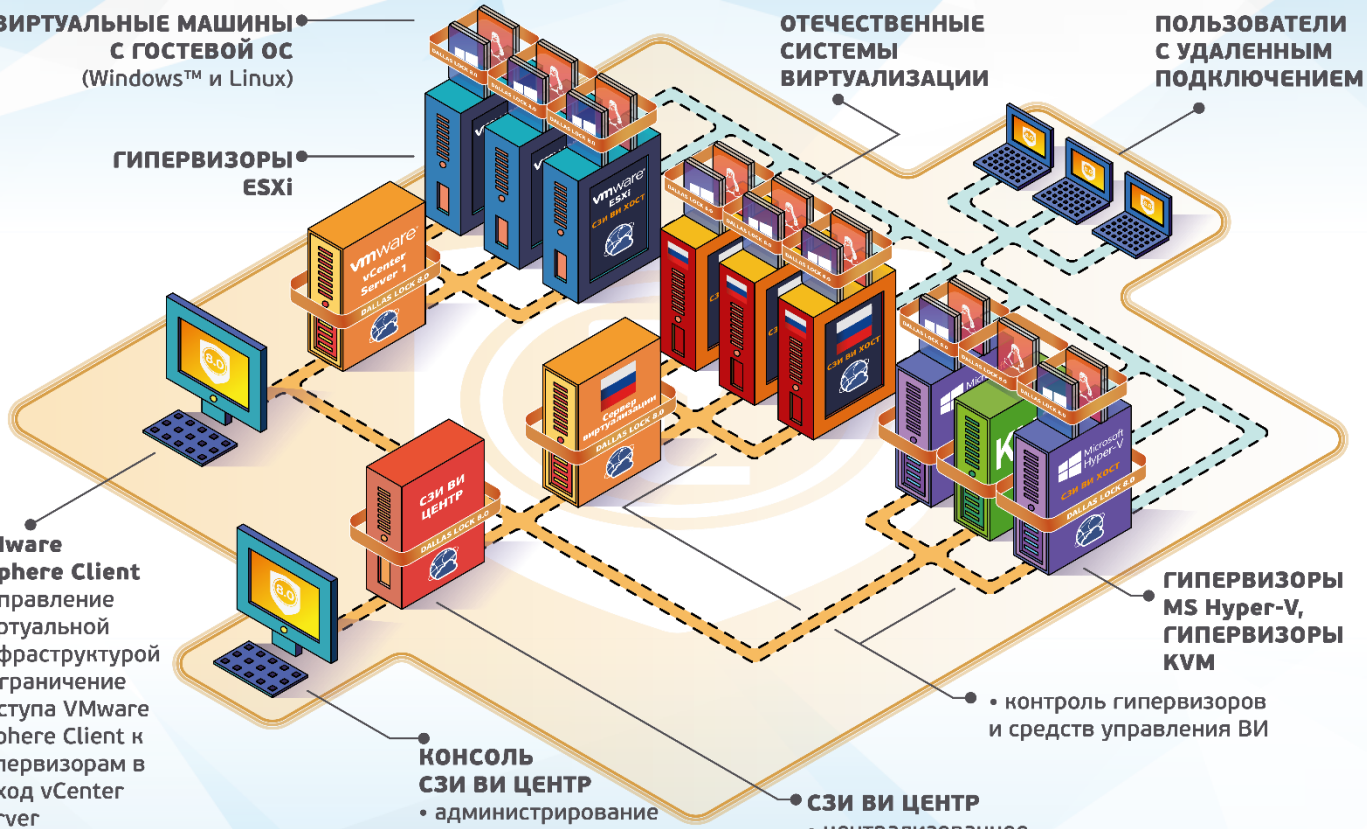
oVirt

- oVirt 4.4
- zVirt 3.0/3.1/3.3/4.0
- HOSTVM
- РЕД Виртуализация 7.3

Универсальная лицензия на СЗИ

(не требует дополнительных вложений при переходе на KVM)

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

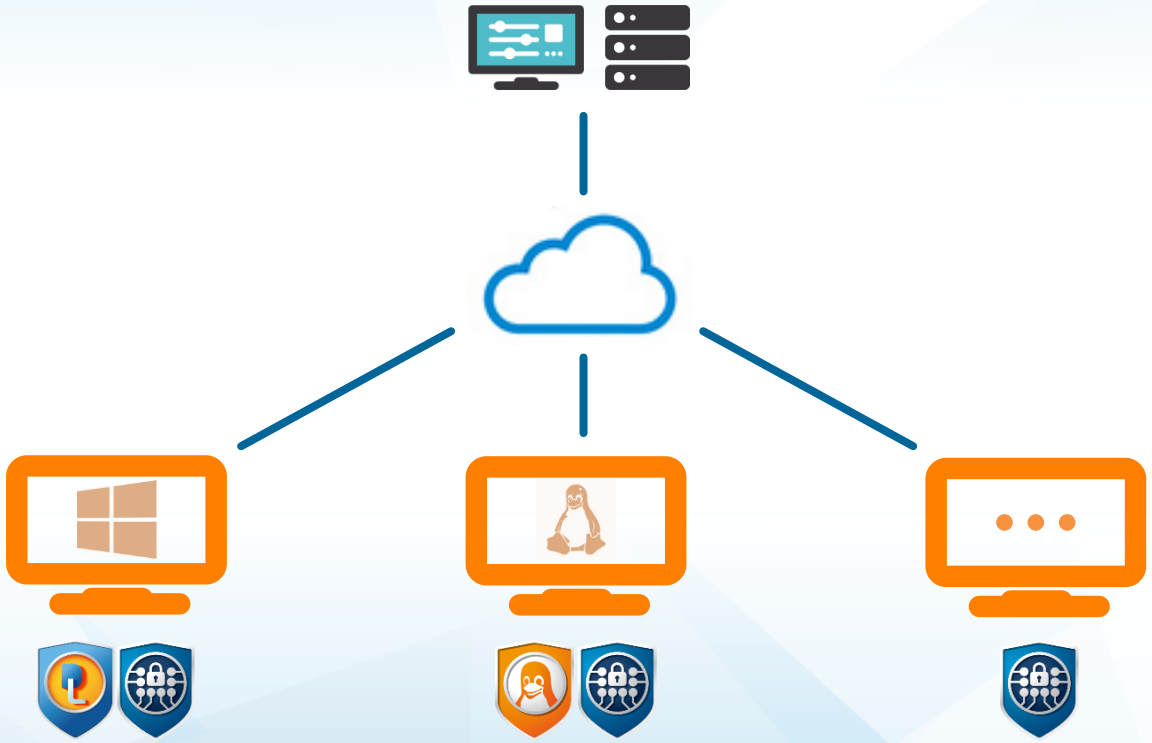


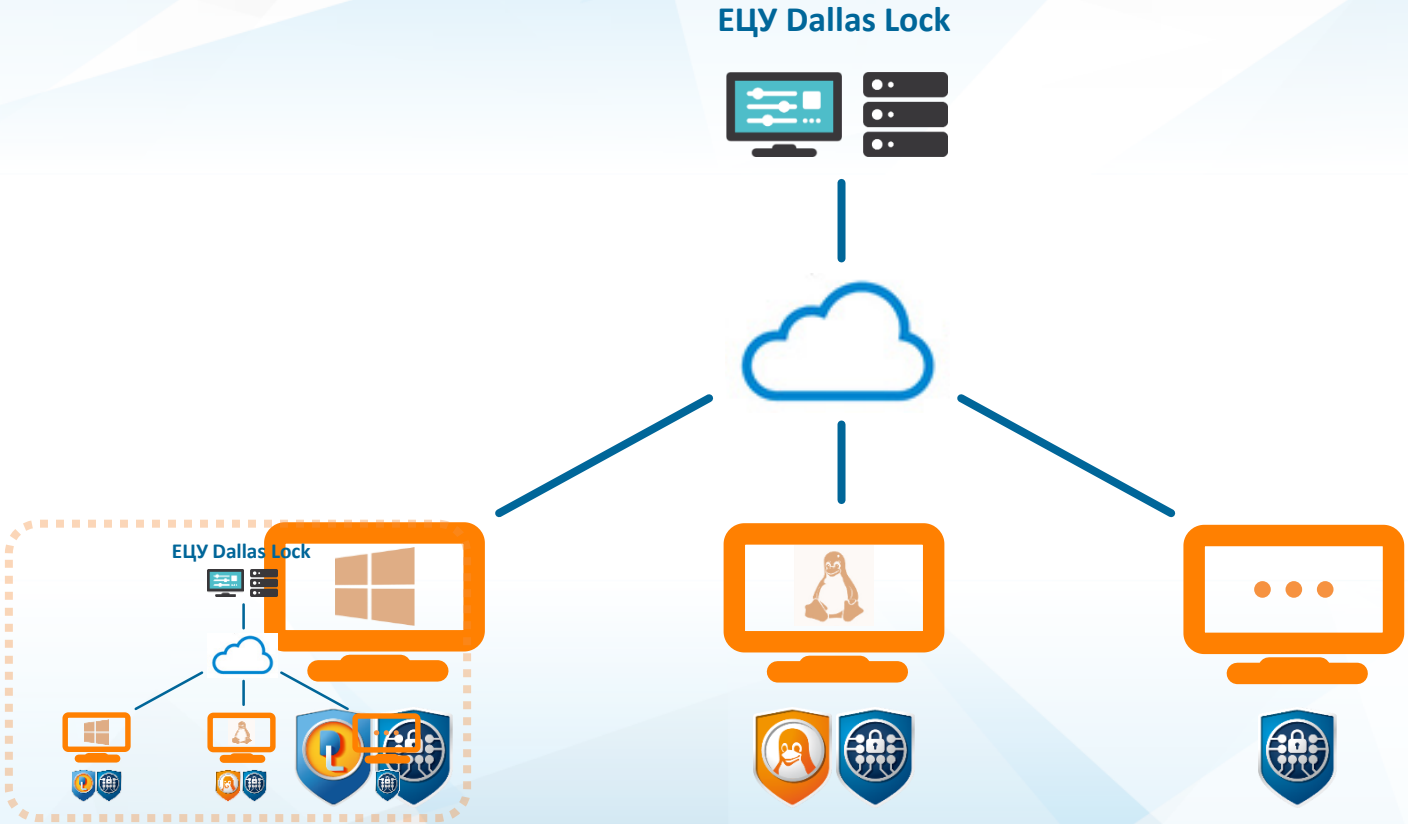
Архитектура СЗИ ВИ Dallas Lock

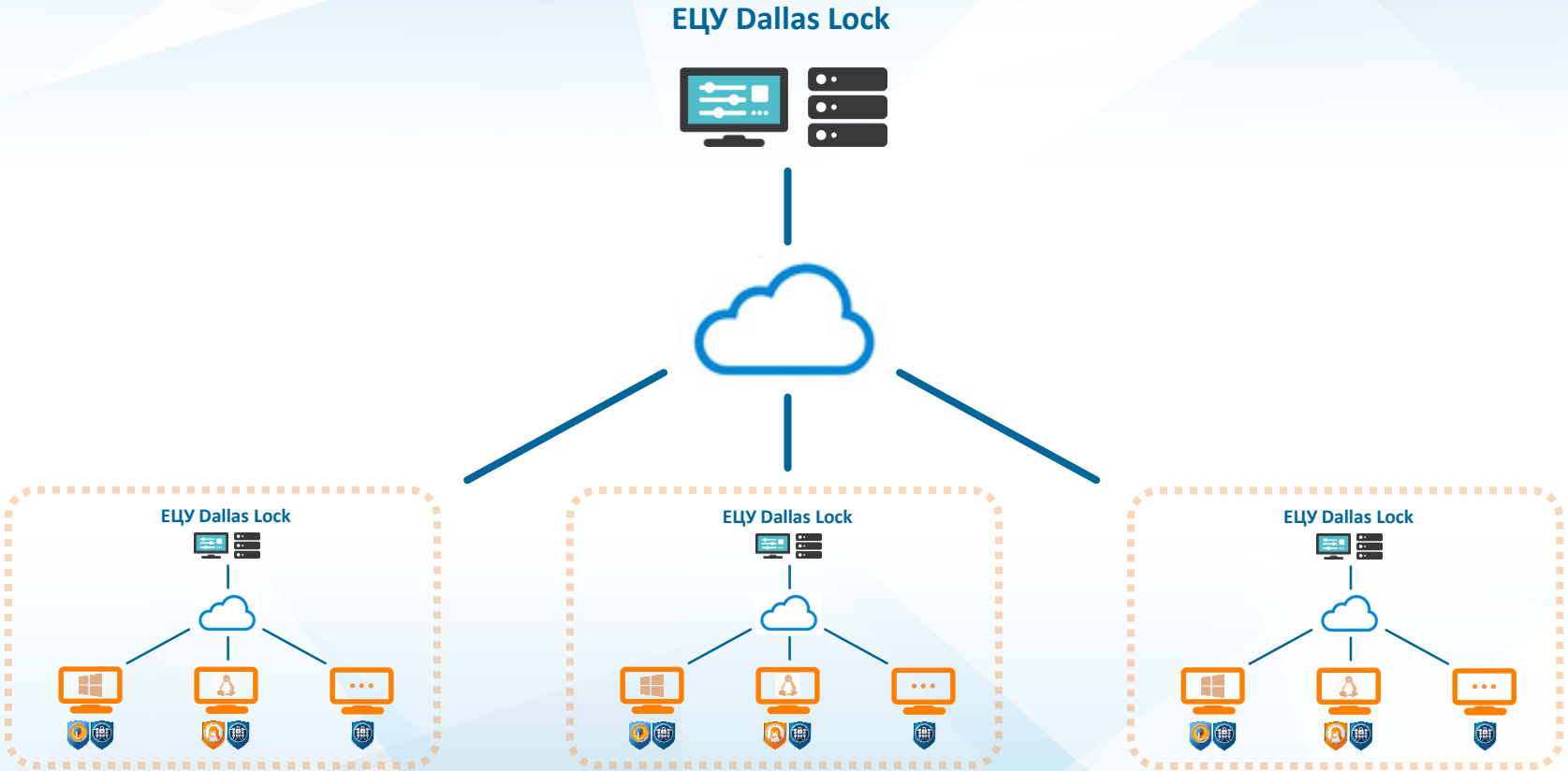
Лицензируется по количеству развертываний (не менее одной лицензии). Бессрочная лицензия.

Универсальная лицензия для ESXi, Hyper-V и KVM серверов (гипервизоров). Лицензируется по количеству физических процессоров. Бессрочная лицензия.

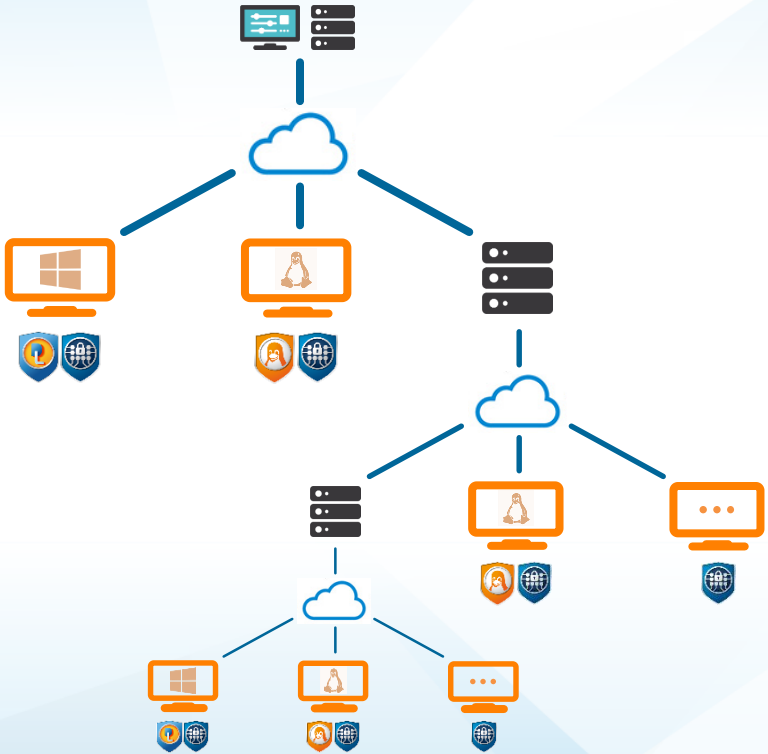
ЕЦУ Dallas Lock




ЕЦУ Dallas Lock
ЕЦУ Dallas Lock


ЕЦУ Dallas Lock
ЕЦУ Dallas Lock
ЕЦУ Dallas Lock
ЕЦУ Dallas Lock

ЕЦУ Dallas Lock



ЕЦУ Dallas Lock

единый кросс-платформенный центр управления, предназначенный для решения гораздо более широкого круга задач по сравнению с хорошо зарекомендовавшим себя Сервером безопасности Dallas Lock

Ключевые возможности:

- поддержка российских ОС, в том числе сертифицированных ФСТЭК России;
- управление СЗИ, находящимися за NAT;
- миграция клиентов с СБ Dallas Lock 8.0 на ЕЦУ с сохранением настроенных параметров;
- построение отказоустойчивых доменов и защита гетерогенных инфраструктур.

Ключевые возможности ЕЦУ Dallas Lock

Централизованное управление продуктовой линейкой Dallas Lock

Удаленный мониторинг компьютеров без установленных СЗИ

Контроль настроек сетевого оборудования

Интеграция со сторонними продуктами

- Антивирус Kaspersky
- SIEM-системы
- Службы каталогов

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.

Централизованное управление, включая сбор журналов и отчетов с рабочих станций и серверов без установленных средств и систем защиты информации, осуществляется с помощью **Агента ЕЦУ**.

Агент ЕЦУ дает возможность удаленного подключения к клиентским машинам с доступом к рабочему столу пользователя.

WAF Dallas Lock

межсетевой экран прикладного уровня, предназначенный для защиты веб-серверов, обслуживающих сайты, веб-службы и веб-приложения, от сетевых атак и нежелательного интернет-трафика.

WAF (Web Application Firewall)

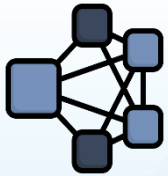
межсетевой экран уровня веб-приложений

Ключевые возможности WAF Dallas Lock

На прикладном уровне: анализ трафика веб-приложений и обнаружение вторжений
На транспортном и сетевом уровне: обнаружение атак на сетевую инфраструктуру

Защита от угроз из списка OWASP TOP 10, XSS, CSRF, bruteforce-атак
Инспекция SSL/TLS

GEO IP фильтр
Защита от DoS/DDoS
Поддержка протокола HTTP 2.0



Работа в режиме отказоустойчивого кластера
Графическая панель мониторинга системы с отображением статистики
Централизованный мониторинг и управление защитой из ЕЦУ Dallas Lock

Возможности Dallas Lock по выполнению мер защиты информации (Приказы ФСТЭК России 17 / 21 / 31 / 239):

- **Идентификация и аутентификация**
- **Управление доступом**
- **Ограничение программной среды**
- **Защита машинных носителей информации**
- **Аудит безопасности**
- Антивирусная защита
- **Предотвращение вторжений (компьютерных атак)**
- **Обеспечение целостности**
- **Обеспечение доступности информации**
- Защита технических средств и систем
- **Защита информационной (автоматизированной) системы и её компонентов**
- **Реагирование на инциденты информационной безопасности**
- **Управление конфигурацией**
- **Управление обновлениями программного обеспечения**
- Планирование мероприятий по обеспечению безопасности
- **Обеспечение действий в нештатных (непредвиденных) ситуациях**
- Информирование и обучение персонала

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

	СЗИ НСД DALLAS LOCK LINUX	СЗИ НСД DALLAS LOCK 8.0-K	СЗИ НСД DALLAS LOCK 8.0-C	СДЗ ПР DALLAS LOCK	СДЗ УБ DALLAS LOCK	СЗИ ВИ DALLAS LOCK	ЕЦУ DALLAS LOCK	WAF DALLAS LOCK
Тип СЗИ	ПО*	ПО*	ПО*	ПАК*	ПО*	ПО*	ПО*	ПО*
АС	до 1Г вкл.		до 2А (1Б) вкл.**	до 2А (1Б) вкл.	до 2А (1Б) вкл.	до 1Г вкл.	до 1Г вкл./до 2А (1Б) вкл.	до 1Г вкл.
ГИС / ПДн / АСУ ТП / КИИ	до 1 вкл.							
ФСТЭК России	№ 3594 от 04.07.2016 г.	№ 2720 от 25.09.2012 г.	№ 2945 от 16.08.2013 г.	№ 3666 от 25.11.2016 г.	№ 4786 от 13.03.2024 г.	№3837 от 18.12.2017 г.	№ 3594 от 04.07.2016 г. № 2720 от 25.09.2012 г. № 2945 от 16.08.2013 г.	Получение сертификата планируется в 3 кв. 2024 г.
	НСД 5	НСД 5	НСД 3			НСД 5		
	ИТ.СКН.П4.ПЗ	ИТ.СКН.П4.ПЗ ИТ.СКН.Н4.ПЗ	ИТ.СКН.П2.ПЗ ИТ.СКН.Н2.ПЗ	ИТ.СДЗ.ПР2.ПЗ	ИТ.СДЗ.УБ2.ПЗ			
	УД 4	УД 4	УД 2	УД 2	УД 2	УД 4	УД 4/УД 2	УД 4
	ИТ.МЭ.В4.ПЗ	ИТ.МЭ.В4.ПЗ	ИТ.МЭ.В4.ПЗ					ИТ.МЭ.Б4.ПЗ ИТ.МЭ.Г4.ПЗ
		ИТ.СОВ.У4.ПЗ	ИТ.СОВ.У4.ПЗ					ИТ.СОВ.С4.ПЗ
Минобороны России			№ 3902 от 23.03.2018 г.	№ 5695 от 31.03.2022 г.			№ 5695 от 31.03.022 г.	
			СВТ 3	ИТ.СДЗ.ПР2.ПЗ				
			МЭ 3					
			НДВ 2	НДВ 2			НДВ 2	
			РДВ	РДВ			РДВ	
			КИКТ	КИКТ				
Союз «Санкт-Петербургская торгово-промышленная палата»				СТ-1***				
Единый реестр российских программ для ЭВМ и БД	Приказ Минкомсвязи России № 426 от 06.09.2016 г. Запись в реестре № 1285 от 05.09.2016 г.	Приказ Минкомсвязи России № 165 от 18.04.2016 г. Запись в реестре № 407 от 18.04.2016 г.	Приказ Минкомсвязи России № 151 от 08.04.2016 г. Запись в реестре № 313 от 08.04.2016 г.	Приказ Минкомсвязи России № 487 от 07.10.2016 г. Запись в реестре № 2019 от 08.10.2016 г.	Приказ Минкомсвязи России от 14.12.2023 г. Запись в реестре № 20592 от 14.12.2023 г.	Приказ Минкомсвязи России № 487 от 07.10.2016 г. Запись в реестре № 2032 от 08.10.2016 г.	Приказ Минкомсвязи России № 768 от 27.07.2021 г. Запись в реестре № 11185 от 29.07.2021 г.	Приказ Минкомсвязи России от 15.03.2024 г. Запись в реестре № 21831 от 15.03.2024 г.

* ПО (Программное обеспечение), ПАК (Программно-аппаратный комплекс).
** МЭ и СОВ для СЗИ Dallas Lock 8.0-C — до 1Г включительно.
*** Сертификат, подтверждающий российское происхождение платы СДЗ Dallas Lock.

Уровни сертификации

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Спасибо за внимание!

Иван Дятлов

ВЕДУЩИЙ МЕНЕДЖЕР ПО РАБОТЕ С ПАРТНЕРАМИ
ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»

EMAIL: DIM@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU