Особенности защиты платформ виртуализации в период импортозамещения

ВЕРШИНИН ВАЛЕРИЙ
Руководитель отдела по работе с партнерами и заказчиками
ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»

E-MAIL: ISC@CONFIDENT.RU
WEB: WWW.DALLASLOCK.RU

КОНФИДЕНТ®
ГРУППА КОМПАНИЙ

Тысячи проектов ежегодно реализуются в России с использованием продуктов Dallas Lock

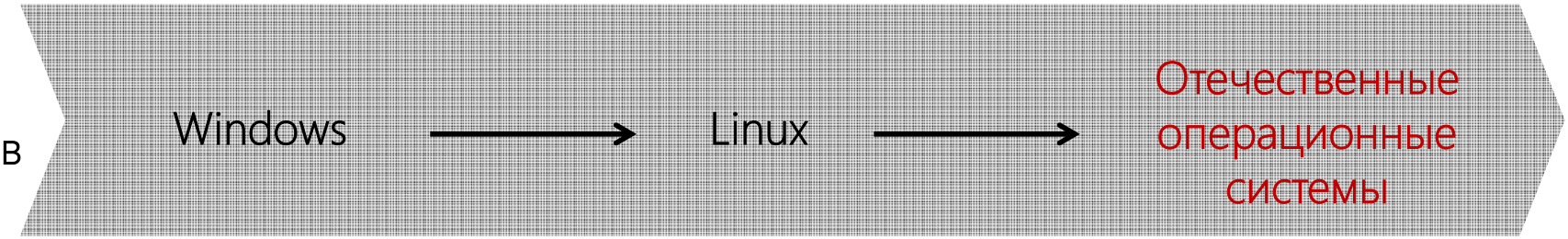
Какие тренды на импортозамещение в части сред виртуализации есть на рынке?

Что такое защищённая отечественная среда виртуализации и как перейти на неё с минимальными затратами?

Тренды импортозамещения

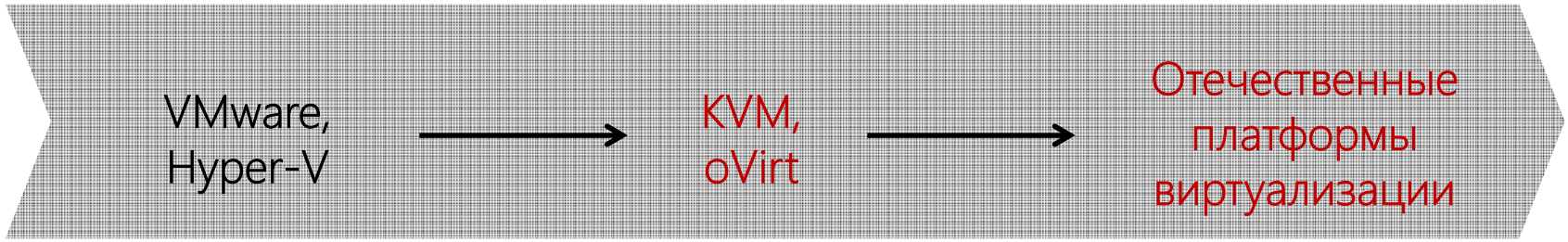
Для защиты применяются сертифицированные СЗИ от НСД

Защита рабочих станций и серверов

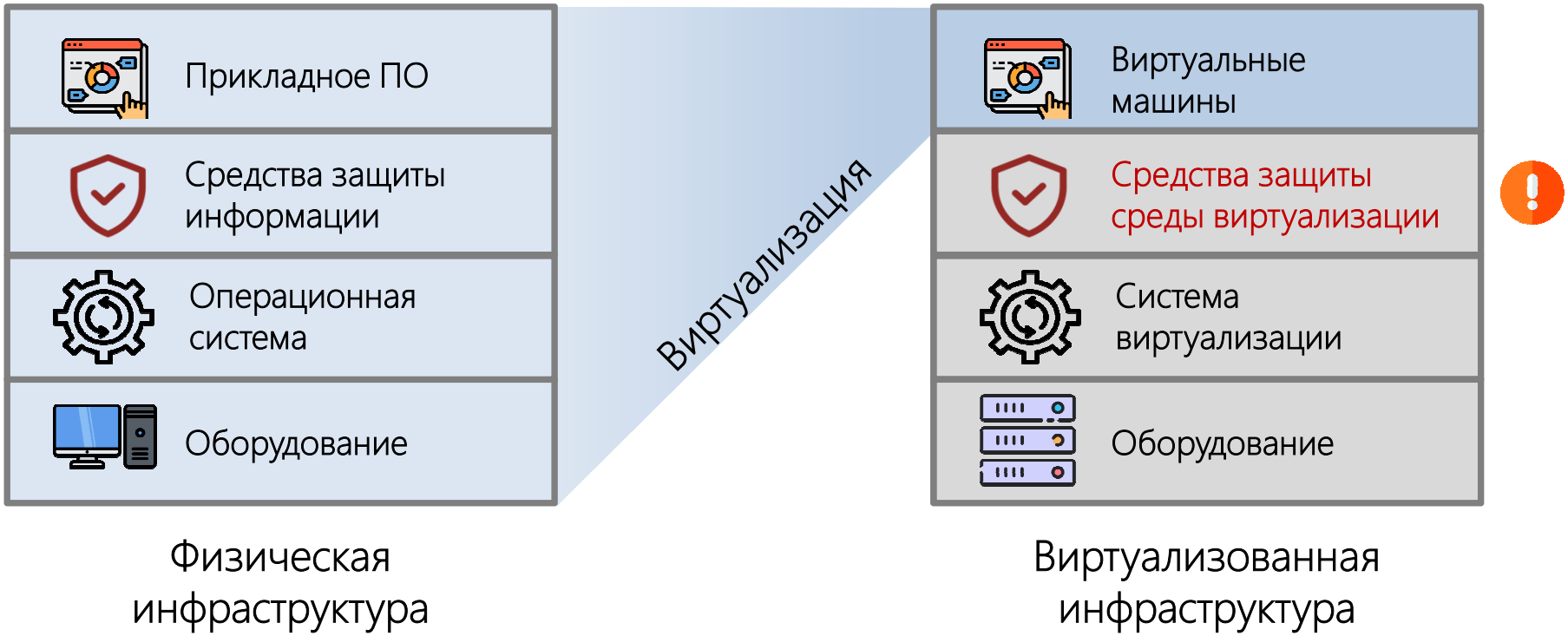


Для защиты применяются сертифицированные СЗИ ВИ

Защита среды виртуализации



Среда виртуализации



Защита среды виртуализации. Нормативное обеспечение

ГОСТ Р 56938—2016. Защита информации при использовании технологий виртуализации. Общие положения (1 июня 2016 г.)

ФСТЭК России

- Приказ № 21 (ПДн)
- Приказ № 17 (ГИС)
- Приказ № 31 (АСУ ТП)
- Приказ № 239 (КИИ)

Обязательные меры **защиты среды виртуализации**, для реализации которых необходимо использовать сертифицированные СЗИ

Рекомендации в области стандартизации Банка России. **Обеспечение информационной безопасности при использовании технологии виртуализации** (1 мая 2015 г.)

Группа мер «Защита среды виртуализации» (ЗСВ), Приказы № 17, 21 ФСТЭК России:

- **ЗСВ.1**: Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
- **ЗСВ.2**: Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
- **ЗСВ.3**: Регистрация событий безопасности в виртуальной инфраструктуре
- **ЗСВ.4**: Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры

Группа мер «Защита среды виртуализации» (ЗСВ), Приказы № 17, 21 ФСТЭК России (продолжение):

- **ЗСВ.5**: Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией
- **ЗСВ.6**: Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных
- **ЗСВ.7**: Контроль целостности виртуальной инфраструктуры и ее конфигураций
- …
- **ЗСВ.10**: Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей

Минимальные требования к сертификации СЗИ для защиты среды виртуализации:

«Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992)

«Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018)

Сертифицированное по РД СВТ СЗИ от НСД + УД

Требования по безопасности информации к средствам виртуализации

Функциональные возможности:

- Создание образов виртуальных машин
- Формирование среды выполнения виртуальных машин
- Централизованное управление виртуальными машинами и организацией взаимодействия между ними

Функции безопасности:

- Доверенная загрузка виртуальных машин
- Контроль целостности
- Регистрация событий безопасности
- Управление доступом
- Резервное копирование виртуальных машин
- Централизованное управление образами виртуальных машин и виртуальными машинами
- Идентификация и аутентификация пользователей

СЗИ ВИ Dallas Lock

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

Продукт сертифицирован ФСТЭК России по 5 классу защищённости СВТ от НСД и по 4 уровню доверия (УД 4). Сертификат ФСТЭК России № 3837 от 18.12.2017 г.

---

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

- CentOS
- Linux Mint
- Ubuntu
- oVirt

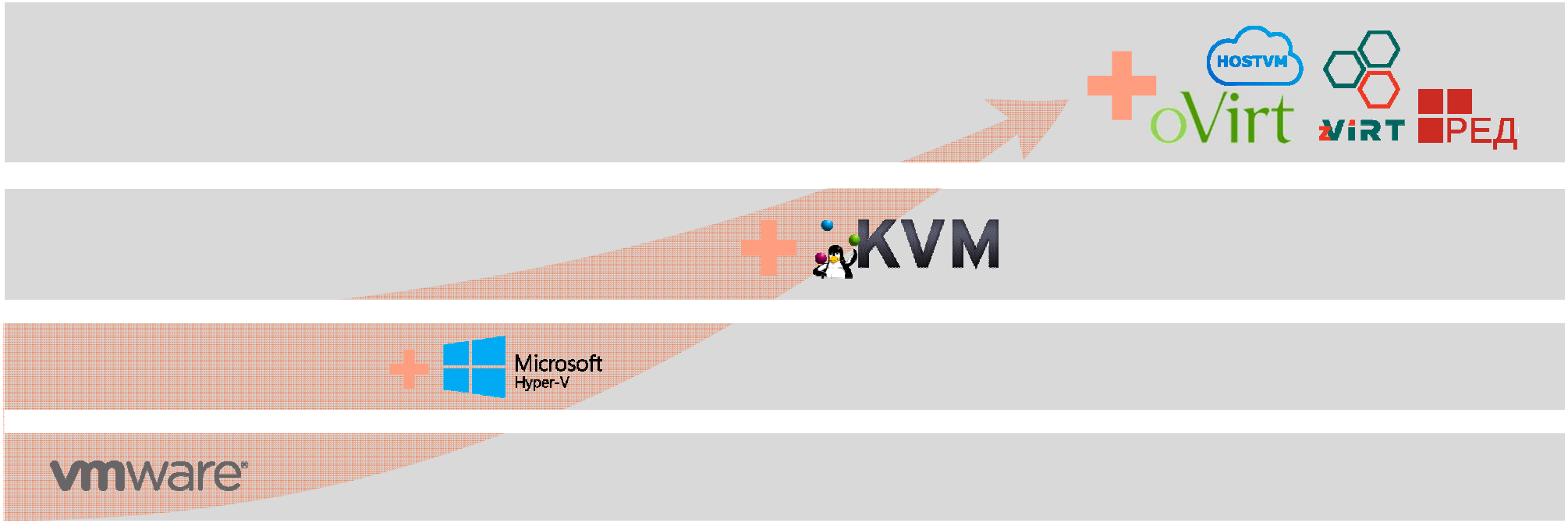
Отечественные платформы виртуализации

- Astra Linux
- zVirt
- «РЕД Виртуализация»
- HOSTVM

Универсальная лицензия на СЗИ

(не требует дополнительных вложений при переходе на KVM)

Поддержка платформ виртуализации в СЗИ ВИ Dallas Lock



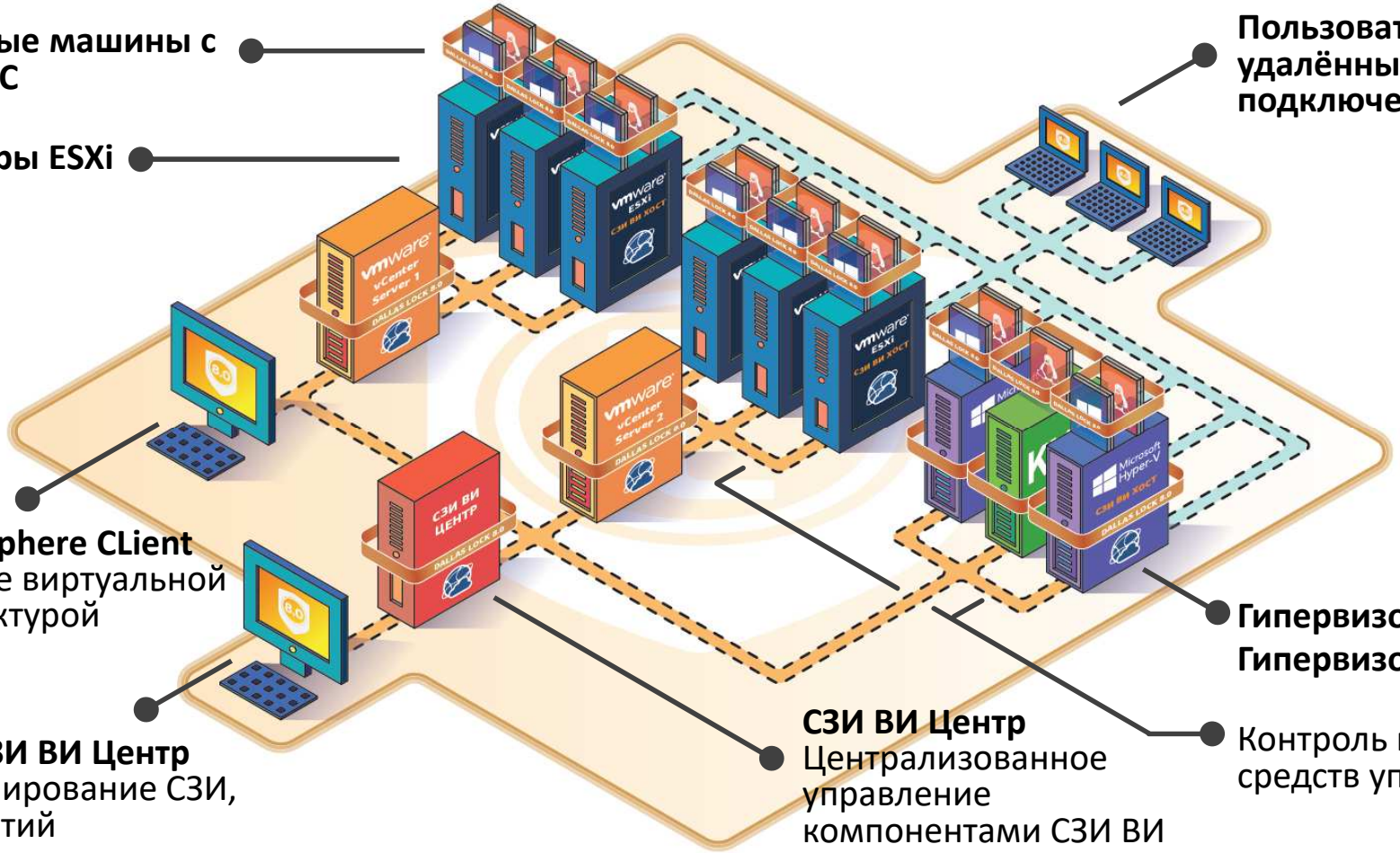
Поддерживается в сертифицированной версии

Архитектура СЗИ ВИ Dallas Lock

Виртуальные машины с гостевой ОС

Гипервизоры ESXi

Пользователи с удалённым подключением



Vmware vSphere CLient
Управление виртуальной инфраструктурой

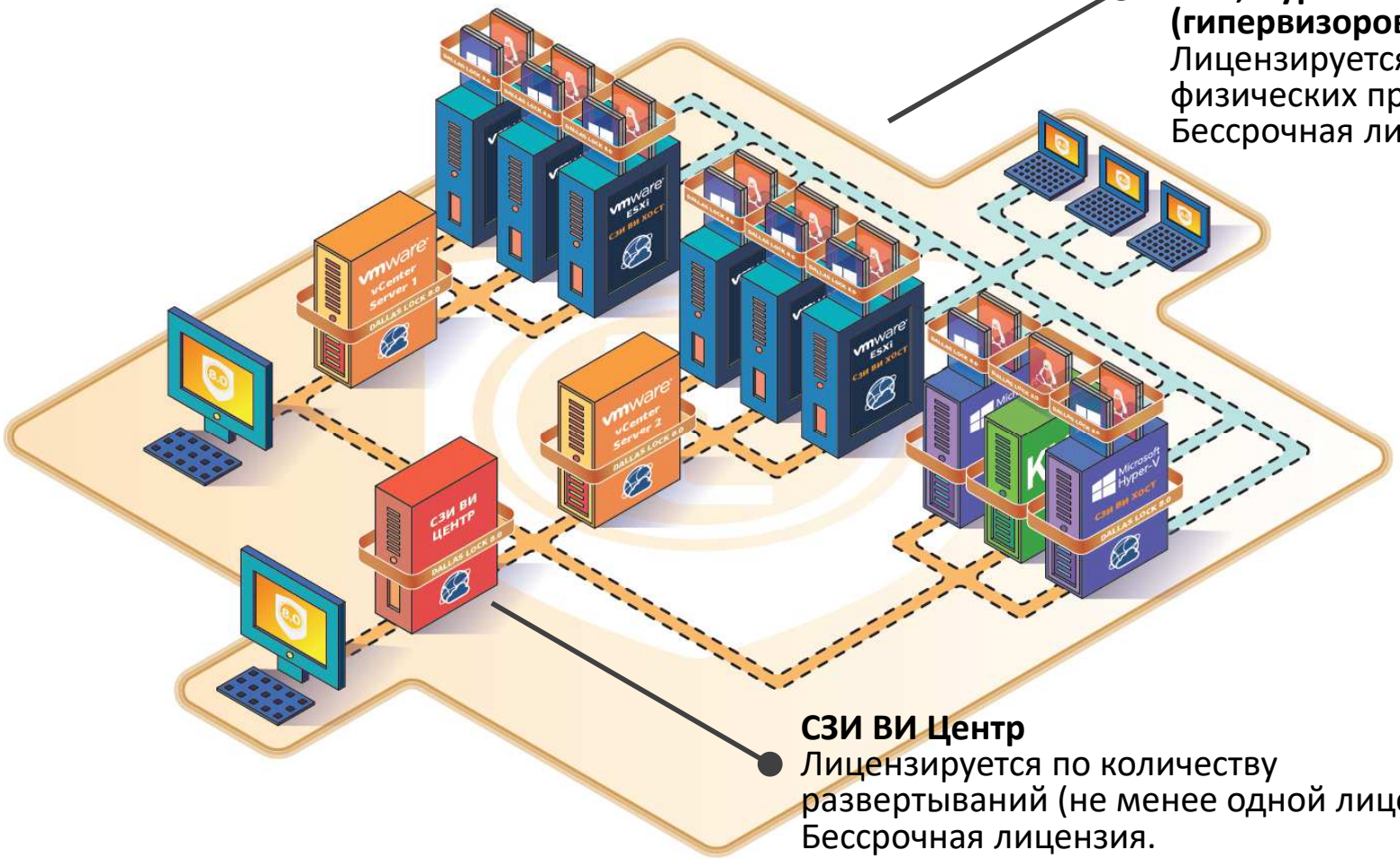
Консоль СЗИ ВИ Центр
Администрирование СЗИ, аудит событий

СЗИ ВИ Центр
Централизованное управление компонентами СЗИ ВИ

Гипервизоры MS Hyper-V
Гипервизоры KVM

Контроль гипервизоров и средств управления ВИ

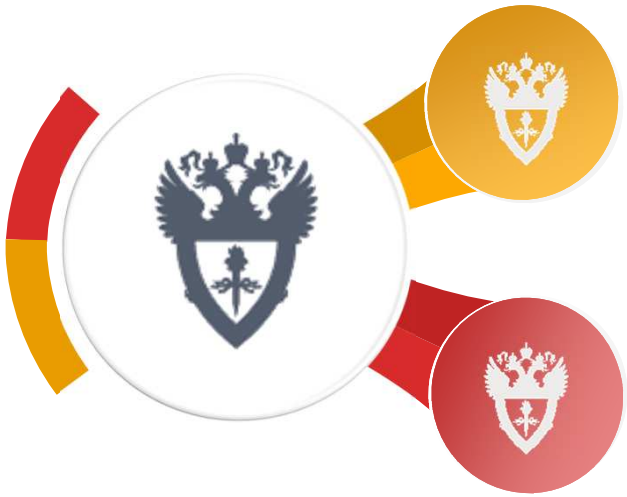
Лицензирование СЗИ ВИ Dallas Lock



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

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

Новинки в части нормативного обеспечения для защиты платформ виртуализации



Требования по безопасности информации к средствам контейнеризации

Требования по безопасности информации к средствам виртуализации

Актуальные вопросы централизованного управления ИТ и ИБ инфраструктурой

Особенности импортозамещения в ИТ и ИБ

Михаил Жванецкий и немного статистики

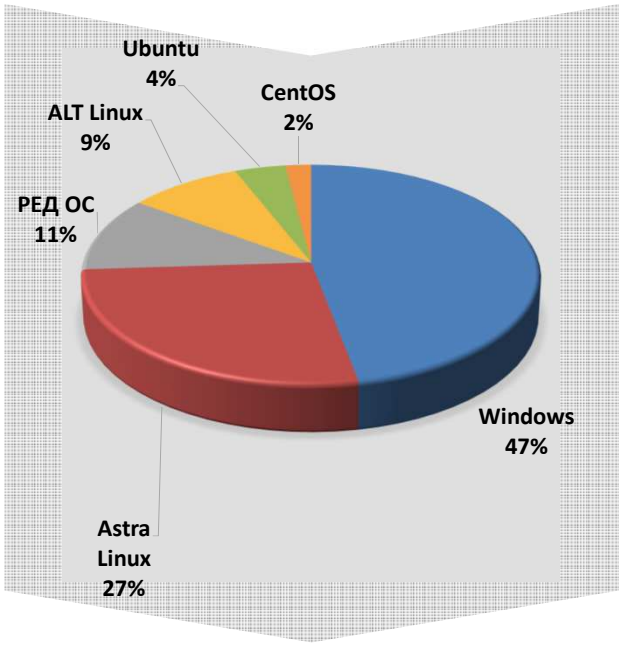
1 *Это все теория: красный свет, зеленый свет, а пока тебя не переедет, пока грузовик на себе не почувствуешь – никому не поверишь.*

2 *Нам говорят: — Вы неправильно делаете. И уходят.*
И мы не делаем никак, чтоб не ошибиться.

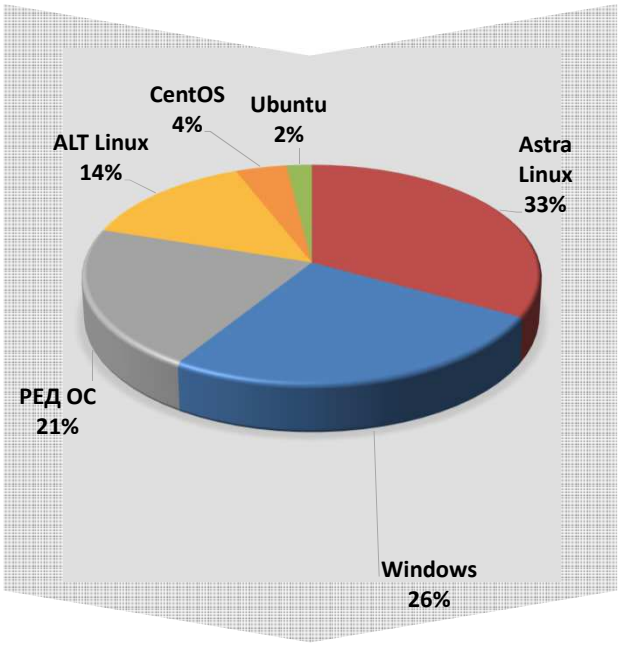
Билеты у спекулянта взял в кино. Оказалось, на вчера, в другом городе и не в кино, а куда-то в планетарий. Черт с ним. Но опыт приобрел.

3 *Мы лежим, сидим, валяемся, но на правильном пути.*

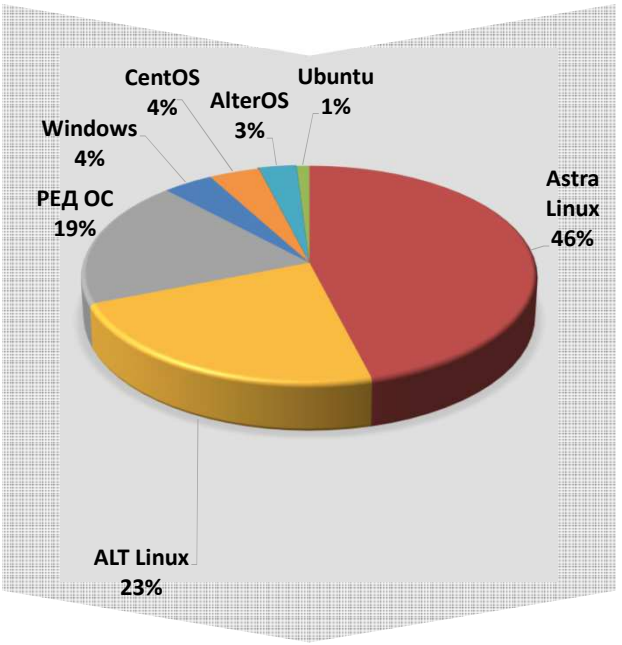
Востребованность ОС в проектах по защите информации в 2021, 2022, 2023 (прогноз)



2021



2022

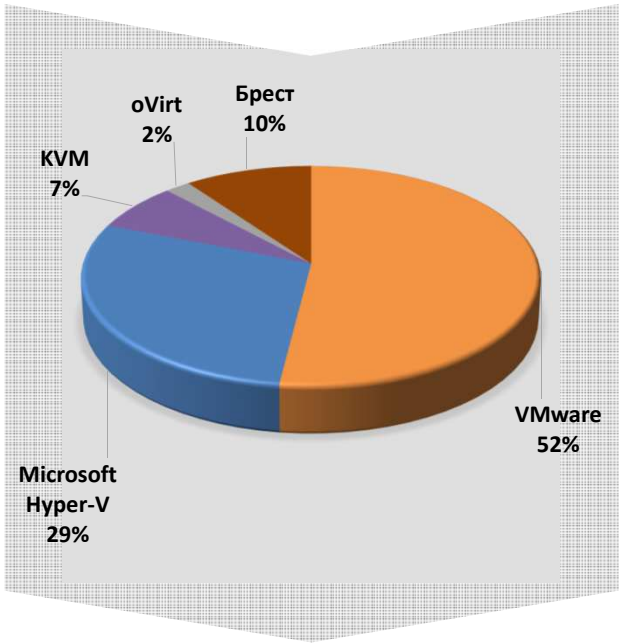


2023

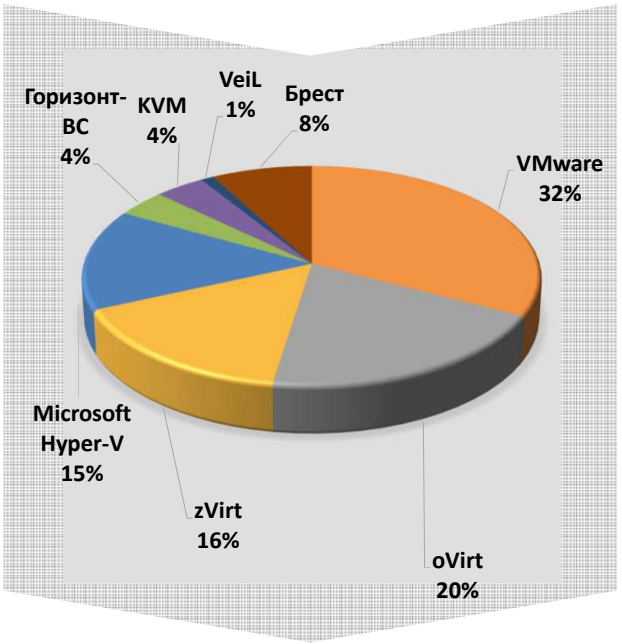
(прогноз)

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

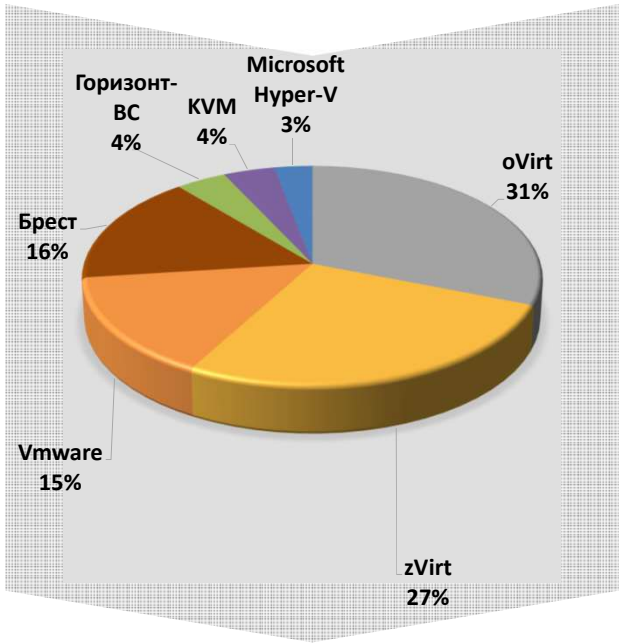
Востребованность систем виртуализации в проектах по защите информации в 2021, 2022, 2023 (прогноз)



2021



2022



2023

(прогноз)

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

Тренды импортозамещения

…лежим, сидим, валяемся, но на правильном пути…

Защита рабочих станций и серверов

Windows → Linux → Отечественные операционные системы

… не делаем никак, чтоб не ошибиться… - …но опыт приобрел…

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

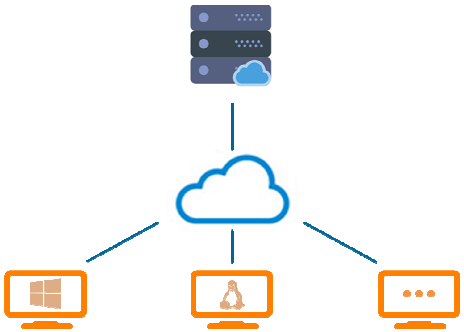
Результаты опроса авторизованных пользователей портала dallaslock.ru, сентябрь 2022 - январь 2023 г.

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

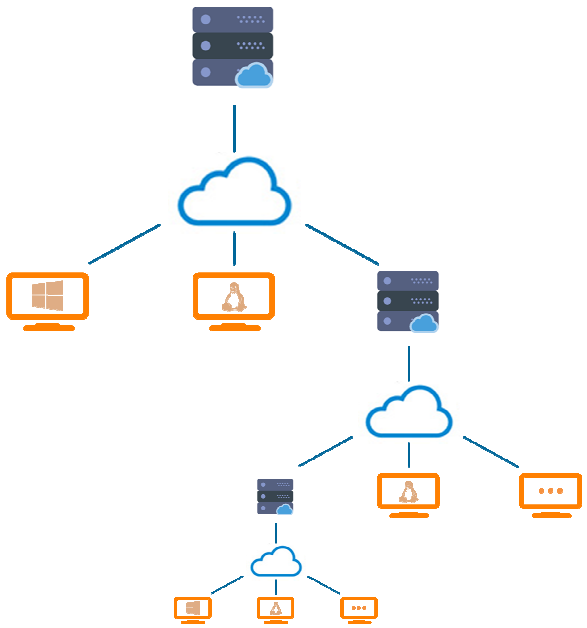
Центр управления



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

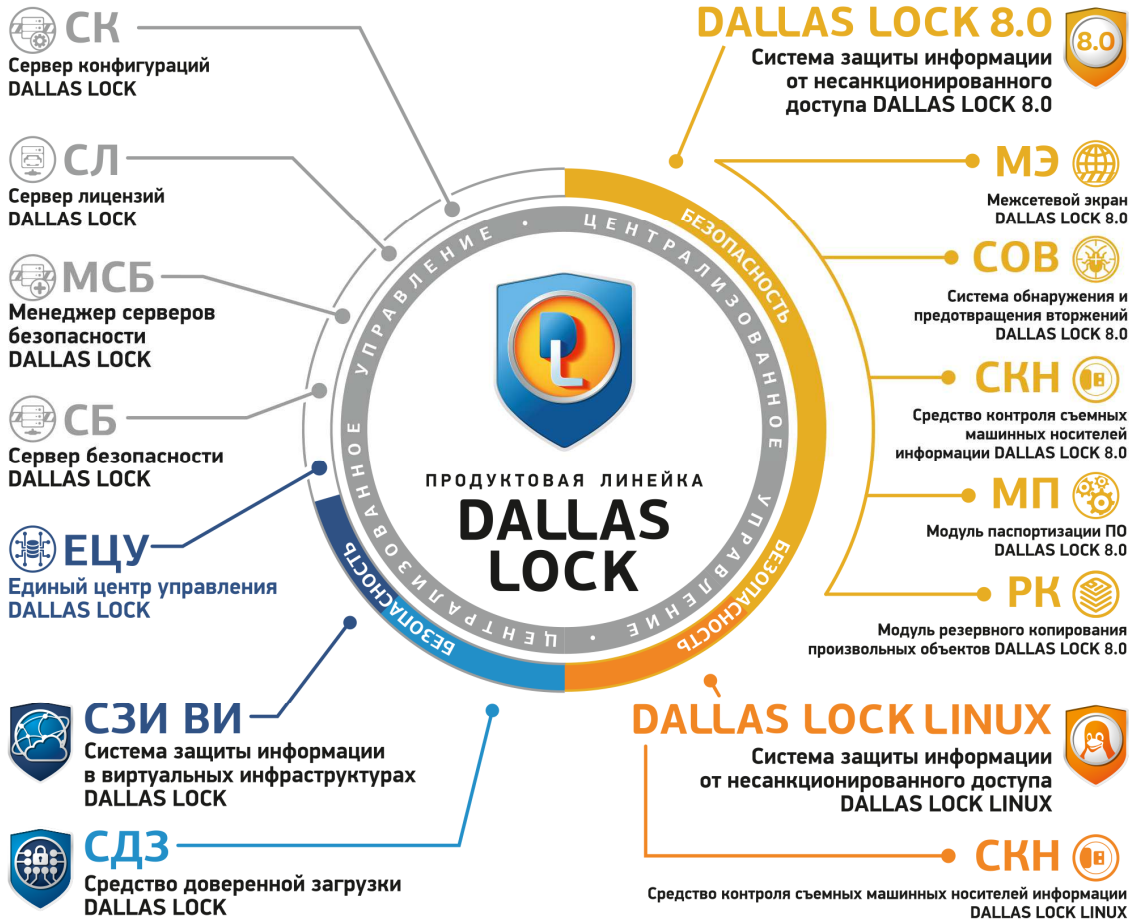


Кросс-платформенное решение для централизованного управления ИБ предприятия

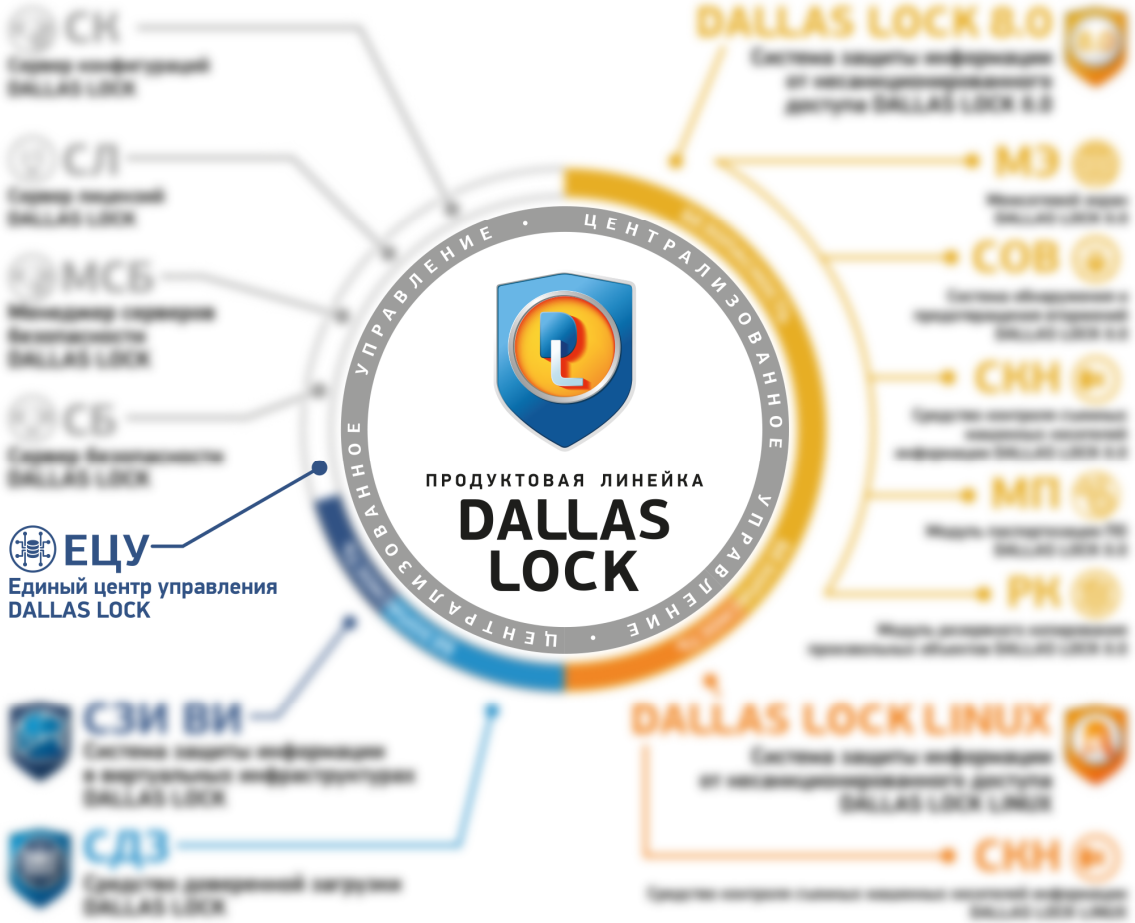
1. Поддержка российских ОС, в т ч сертифицированных ФСТЭК России
2. Управление СЗИ под Windows, Linux, российскими ОС, в тч СДЗ
3. Работа за NAT (Network Address Translation)
4. Управление не только СЗИ Dallas Lock - агент Windows/Linux/росс ОС

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

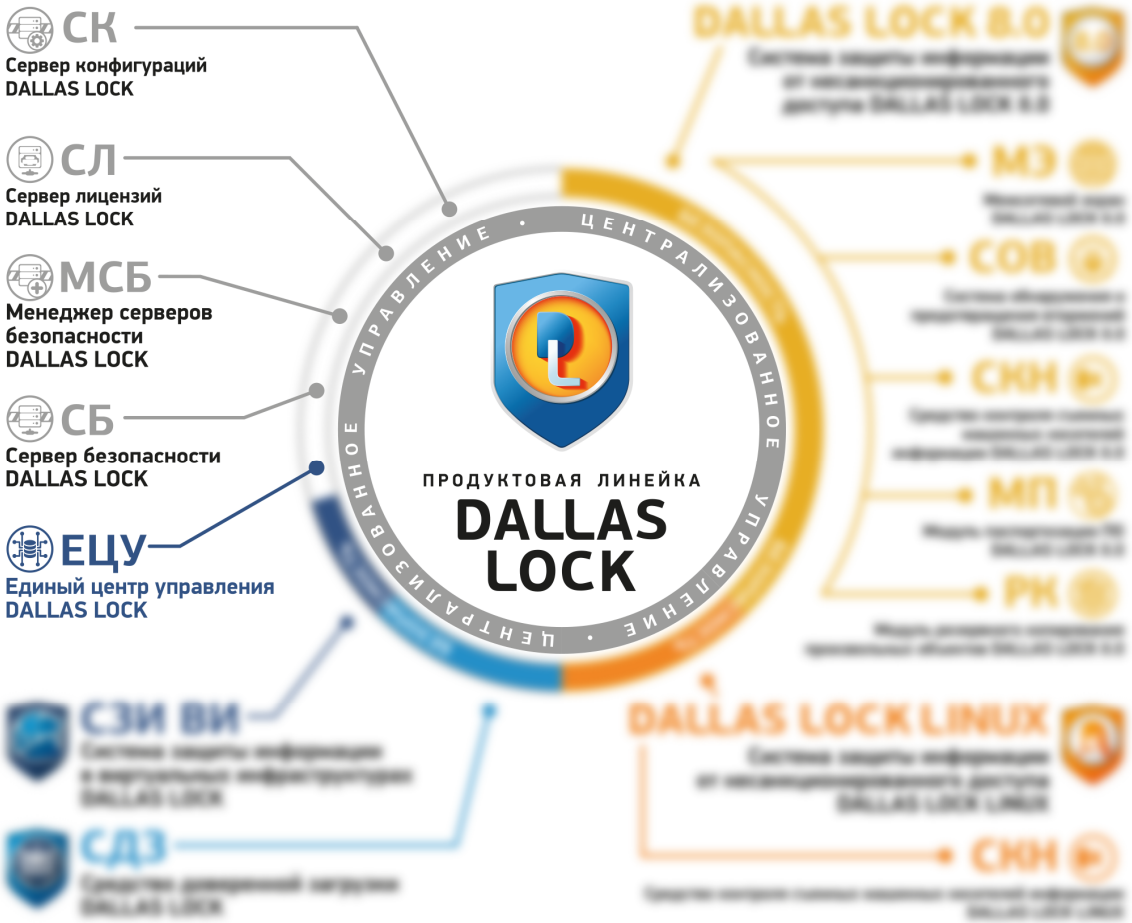
Dallas Lock


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
ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ · ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ · БЕЗОПАСНОСТЬ · БЕЗОПАСНОСТЬ
ПРОДУКТОВАЯ ЛИНЕЙКА
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

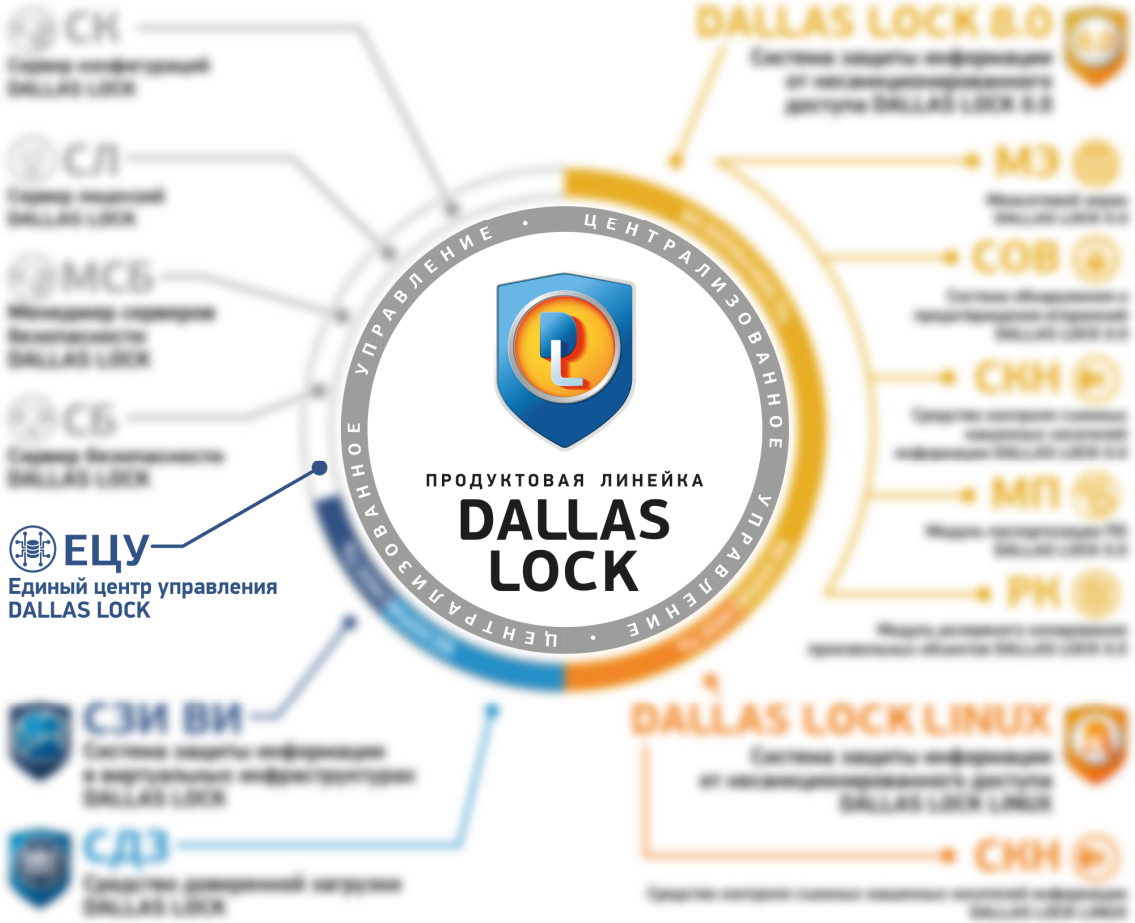
Dallas Lock


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

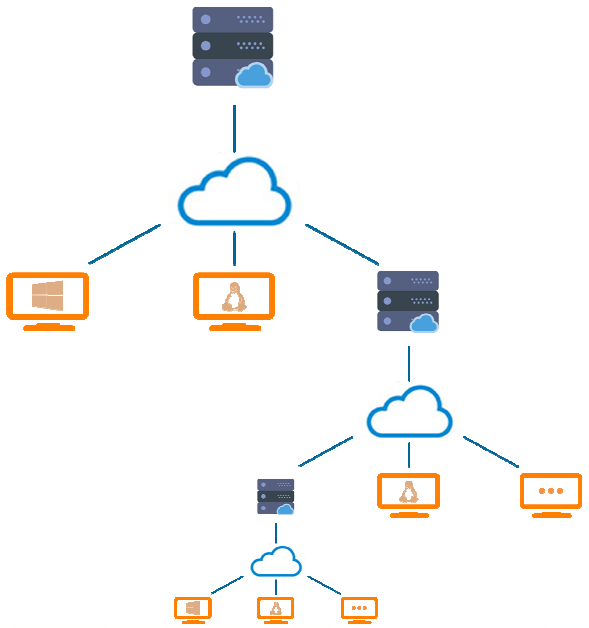
Dallas Lock


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
СЗИ ВИ
СДЗ
ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ
ПРОДУКТОВАЯ ЛИНЕЙКА
DALLAS LOCK
DALLAS LOCK 8.0
МЭ
СОВ
СКН
МП
РК
DALLAS LOCK LINUX
СКН

Dallas Lock


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

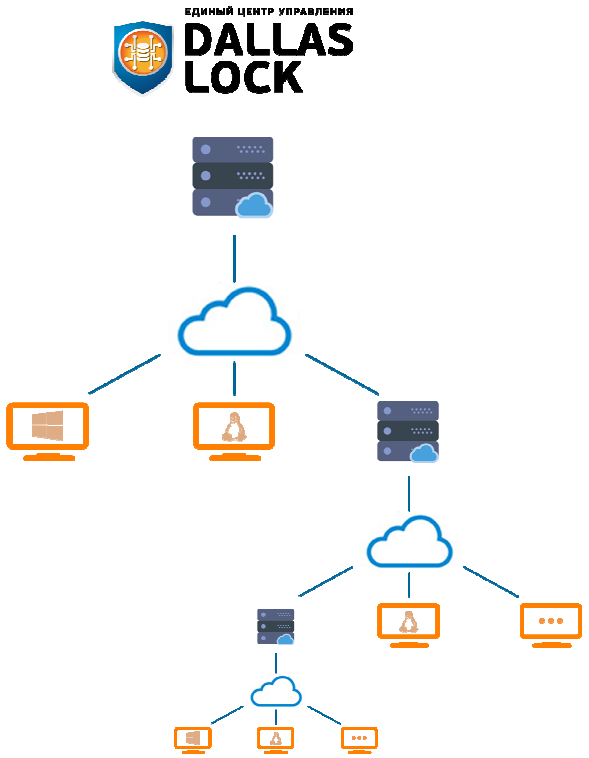
Единый центр управления Dallas Lock



Совместимость

Astra Linux Common Edition (Орел) 2.12;
Astra Linux Special Edition (Смоленск) 1.6;
Astra Linux Special Edition (Смоленск) 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;

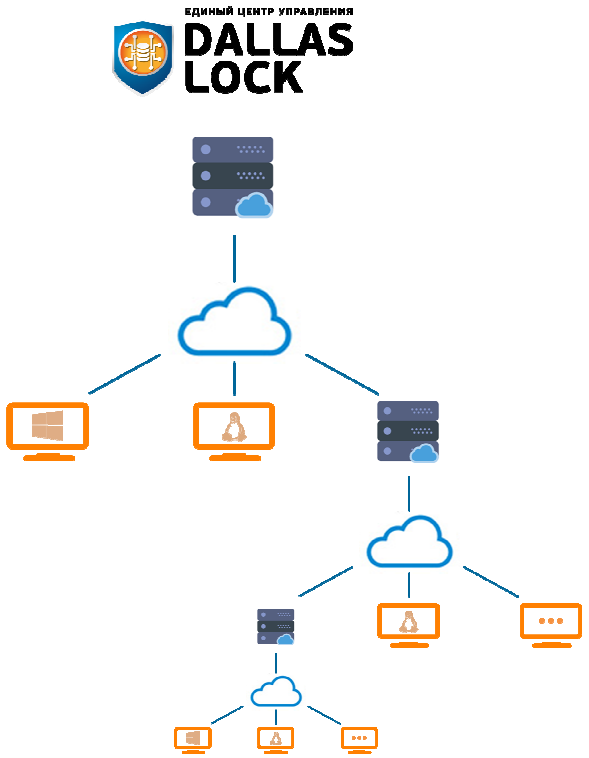
Единый центр управления Dallas Lock



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
- …

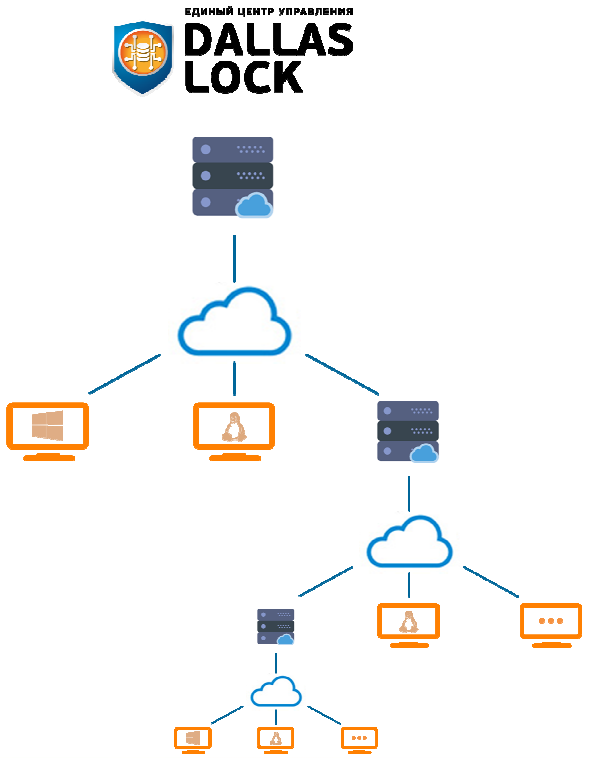
Единый центр управления Dallas Lock



Централизованное управление – основные функции

- Экспорта 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»
- …

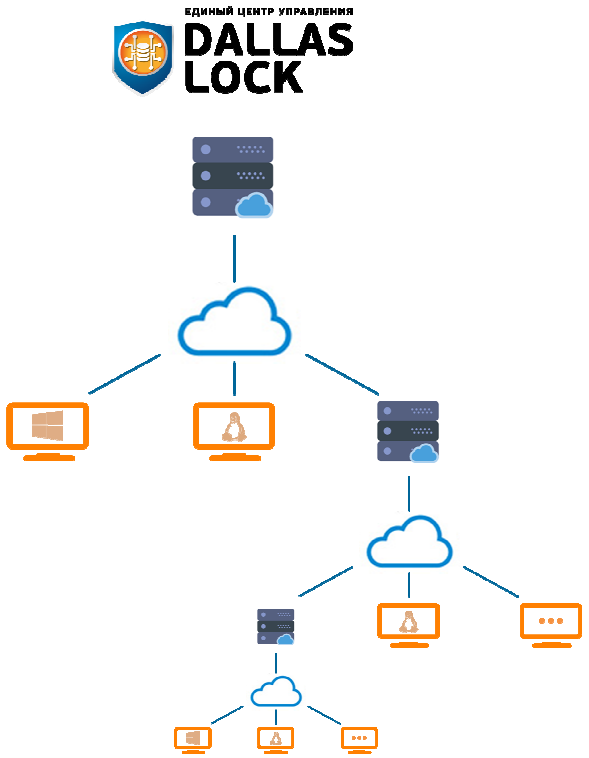
Единый центр управления Dallas Lock



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

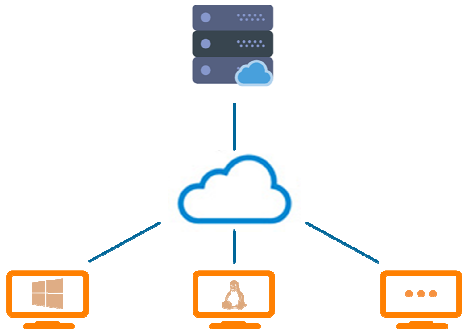


Удаленное управление <u>без</u> установленных СЗИ Dallas Lock

- 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

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

Прошлая жизнь как старое авто — умиляться можно,
но ездить — нет. Отъездили.

Михаил Жванецкий

Спасибо за внимание!

Вершинин Валерий
Руководитель отдела по работе с партнерами и заказчиками ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ ГК «КОНФИДЕНТ»

E-MAIL: ISC@CONFIDENT.RU
WEB: WWW.DALLASLOCK.RU