Оглавление

[Общие сведения 3](#_Toc162604574)

[Описание Продуктовой линейки 4](#_Toc162604575)

[Графические материалы 4](#_Toc162604576)

[Информация о продуктовой линейке 5](#_Toc162604577)

[Dallas Lock 8.0-К 7](#_Toc162604578)

[Графические материалы 7](#_Toc162604579)

[Информация о продукте 7](#_Toc162604580)

[Dallas Lock 8.0-С 11](#_Toc162604581)

[Графические материалы 11](#_Toc162604582)

[Информация о продукте 11](#_Toc162604583)

[СЗИ НСД Dallas Lock Linux 15](#_Toc162604584)

[Графические материалы 15](#_Toc162604585)

[Информация о продукте 15](#_Toc162604586)

[СЗИ ВИ Dallas Lock 18](#_Toc162604587)

[Графические материалы 18](#_Toc162604588)

[Информация о продукте 18](#_Toc162604589)

[СДЗ Dallas Lock 22](#_Toc162604590)

[Графические материалы 22](#_Toc162604591)

[Информация о продукте 22](#_Toc162604592)

[WAF Dallas Lock 28](#_Toc162604593)

[Графические материалы 28](#_Toc162604594)

[Информация о продукте 29](#_Toc162604595)

[Межсетевой экран 33](#_Toc162604596)

[Графические материалы 33](#_Toc162604597)

[Информация о продукте 33](#_Toc162604598)

[Система обнаружения и предотвращения вторжений 36](#_Toc162604599)

[Графические материалы 36](#_Toc162604600)

[Информация о продукте 36](#_Toc162604601)

[Средство контроля съемных машинных носителей информации 39](#_Toc162604602)

[Графические материалы 39](#_Toc162604603)

[Информация о продукте 39](#_Toc162604604)

[Модуль паспортизации 43](#_Toc162604605)

[Графические материалы 43](#_Toc162604606)

[Информация о продукте 43](#_Toc162604607)

[Модуль Резервного копирования произвольных объектов 45](#_Toc162604608)

[Графические материалы 45](#_Toc162604609)

[Информация о продукте 45](#_Toc162604610)

[Сервер безопасности 47](#_Toc162604611)

[Графические материалы 47](#_Toc162604612)

[Информация о продукте 47](#_Toc162604613)

[Менеджер серверов безопасности 50](#_Toc162604614)

[Графические материалы 50](#_Toc162604615)

[Информация о продукте 50](#_Toc162604616)

[Сервер лицензий 53](#_Toc162604617)

[Графические материалы 53](#_Toc162604618)

[Информация о продукте 53](#_Toc162604619)

[Сервер конфигураций 56](#_Toc162604620)

[Графические материалы 56](#_Toc162604621)

[Информация о продукте 56](#_Toc162604622)

[Единый центр управления 58](#_Toc162604623)

[Графические материалы 58](#_Toc162604624)

[Информация о продукте 58](#_Toc162604625)

[Общее описание «О компании» ЦЗИ ООО «Конфидент» 63](#_Toc162604626)

[Графические материалы 63](#_Toc162604627)

[Описание компании 63](#_Toc162604628)

[Описание «О компании» Группы компаний «Конфидент» 65](#_Toc162604629)

[Графические материалы 65](#_Toc162604630)

[Описание компании 65](#_Toc162604631)

# Общие сведения

Пояснения по использованию файлов различного формата:

В сопроводительных материалах графические элементы по всем продуктам рассортированы по соответствующим папкам и представлены в 3-х форматах:

.ai — векторный формат, программа Adobe Illustrator, предназначен для полиграфии и всего чего угодно;

.eps — векторный формат, мульти платформенный, предназначен для полиграфии и всего чего угодно;

.png — растровый формат, с прозрачным фоном, предназначен для web (150 dpi).

Все графические материалы в одном архиве .zip:

<https://dallaslock.ru/upload/dallasdocs/marketing_materials.zip>

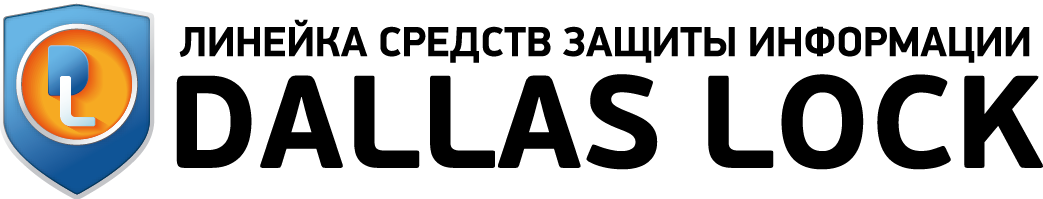
# Описание Продуктовой линейки

## Графические материалы

Ссылка на графические материалы:

<https://dallaslock.ru/upload/dallasdocs/products_dallas_lock.zip>

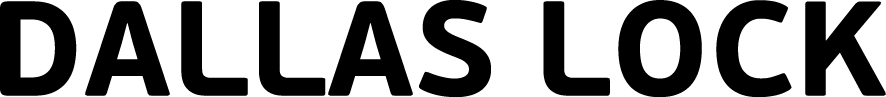
Значок продуктовой линейки (строка)



Значок продуктовой линейки (прямоугольник)



Надпись отдельно



Значок отдельно



## Информация о продуктовой линейке

**Малое**

Продуктовая линейка Центра защиты информации компании «Конфидент» представлена современными средствами защиты информации для платформ Windows и Linux.

**Среднее**

Продуктовая линейка Центра защиты информации компании «Конфидент» представлена современными средствами защиты информации для платформ Windows и Linux.

Продукты компании «Конфидент» применяются для защиты конфиденциальной информации и информации, составляющей государственную тайну до уровня «совершенно секретно» включительно

**Большое**

Продуктовая линейка Центра защиты информации компании «Конфидент» представлена современными средствами защиты информации для платформ Windows и Linux. Решения компании позволяют привести информационные системы в соответствие требованиям законодательства и создать их комплексную многофункциональную защиту.

Продукты компании «Конфидент» применяются для защиты конфиденциальной информации и информации, составляющей государственную тайну до уровня «совершенно секретно» включительно.

**Ключевые особенности**

**Краткий список**

* соответствие российскому законодательству в сфере ИБ (сертификаты ФСТЭК России, сертификаты Минобороны России);
* «бесшовная» интеграция продуктов Dallas Lock между собой;
* выгодные условия первичного приобретения и последующего сопровождения.

**Средний список**

* соответствие российскому законодательству в сфере ИБ (сертификаты ФСТЭК России, сертификаты Минобороны России);
* решение широкого спектра задач заказчиков по защите информации — не только приведение в соответствие требованиям законодательства;
* «бесшовная» интеграция продуктов Dallas Lock между собой;
* расширенный функционал централизованного управления с возможностью построения отказоустойчивых доменов безопасности;
* защита сложных гетерогенных сетевых инфраструктур с минимальными затратами;
* выгодные условия первичного приобретения и последующего сопровождения;
* обеспечение комплексной информационной безопасности.

**Длинный список**

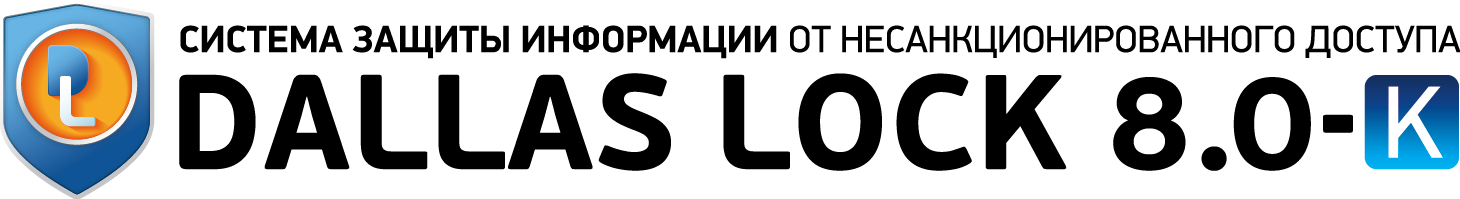
* соответствие российскому законодательству в сфере ИБ (сертификаты ФСТЭК России, сертификаты Минобороны России);
* регулярное продление сертификатов и сертификация новой функциональности;
* решение широкого спектра задач заказчиков по защите информации — не только приведение в соответствие требованиям законодательства;
* «бесшовная» интеграция продуктов Dallas Lock между собой;
* совместимость с ИТ/ИБ-решениями других производителей;
* расширенный функционал централизованного управления с возможностью построения отказоустойчивых доменов безопасности;
* защита сложных гетерогенных сетевых инфраструктур с минимальными затратами;
* выгодные условия первичного приобретения и последующего сопровождения;
* обеспечение комплексной информационной безопасности.

# Dallas Lock 8.0-К

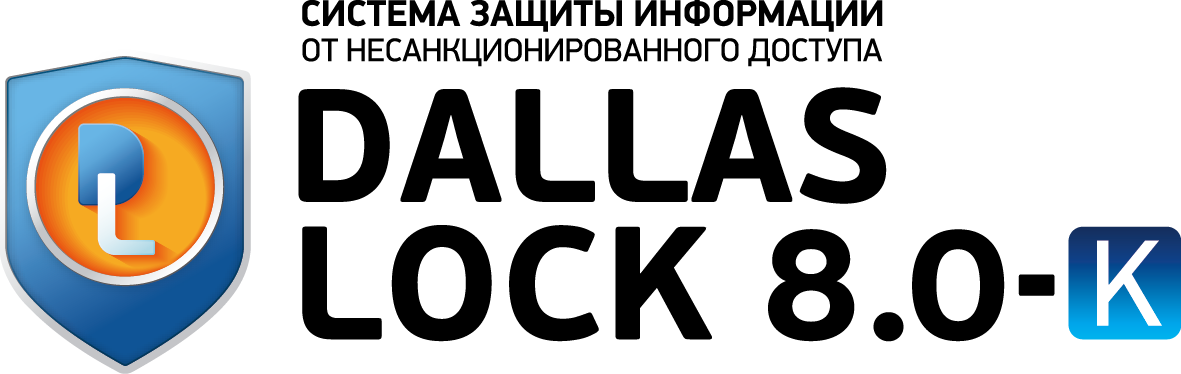
## Графические материалы

Ссылка на графические материалы: <https://dallaslock.ru/upload/dallasdocs/szi_nsd_dallas_lock_8.0-K.zip>

Значок продукта (строка)



Значок продукта (прямоугольник)



## Информация о продукте

**Краткое название**

СЗИ НСД Dallas Lock 8.0-К

**Развернутое название**

Сертифицированная система защиты информации от несанкционированного доступа Dallas Lock 8.0-К

Позиционирование

Программный комплекс средств защиты конфиденциальной информации от несанкционированного доступа в локальных и сетевых АРМ под управлением ОС семейства Windows.

Описание

**Малое**

СЗИ НСД Dallas Lock 8.0-К — сертифицированная система защиты конфиденциальной информации от несанкционированного доступа накладного типа в автономных и сетевых АРМ.

**Среднее**

СЗИ НСД Dallas Lock 8.0-К — сертифицированная система защиты конфиденциальной информации от несанкционированного доступа накладного типа. Предназначена для автономных персональных компьютеров и компьютеров в составе локально-вычислительной сети.

**Большое**

СЗИ НСД Dallas Lock 8.0-К — сертифицированная система защиты конфиденциальной информации от несанкционированного доступа накладного типа. Предназначена для автономных персональных компьютеров и компьютеров в составе локально-вычислительной сети, работающих под управлением ОС семейства Windows.

Комплексная защита конечной точки обеспечивается набором сертифицированных модулей СЗИ Dallas Lock 8.0-К:

* Межсетевой экран;
* Система обнаружения и предотвращения вторжений;
* СКН уровня подключения съемных носителей;
* СКН уровня отчуждения (переноса) информации;
* Модуль паспортизации программного обеспечения;
* Резервное копирование произвольных объектов.

Ключевые особенности

**Короткий список**

* СЗИ Dallas Lock 8.0 интегрируется с учётными записями и правами Active Directory, но корректно работает и вне Windows-доменов;
* для корректной работы Сервера безопасности Dallas Lock не требуется ни серверной ОС, ни сторонней СУБД;
* СЗИ Dallas Lock 8.0 включает сертифицированные модули: защита от НСД, СКН уровня подключения съемных носителей, СКН уровня отчуждения (переноса) информации, МЭ, СОВ, а также модуль паспортизации программного обеспечения, модуль Резервного копирования произвольных объектов и модуль Безопасной среды («песочницы»).

**Средний список**

* СЗИ Dallas Lock 8.0 интегрируется с учётными записями и правами Active Directory, но корректно работает и вне Windows-доменов;
* для корректной работы Сервера безопасности Dallas Lock не требуется ни серверной ОС, ни сторонней СУБД;
* защита конфиденциальной информации от несанкционированного доступа;
* СЗИ Dallas Lock 8.0 включает сертифицированные модули: защита от НСД, СКН уровня подключения съемных носителей, СКН уровня отчуждения (переноса) информации, МЭ, СОВ, а также Модуль паспортизации программного обеспечения, модуль Резервного копирования произвольных объектов и модуль Безопасной среды («песочницы»);
* дискреционный принцип разграничения доступа к информационным ресурсам;
* аудит действий пользователей;
* объединение защищенных ПК для централизованного управления механизмами безопасности;
* контроль целостности файловой системы, программно-аппаратной среды и реестра;
* приведение АС, ГИС, АСУ ТП, КИИ и систем обработки ПДн в соответствие законодательству РФ по защите информации;
* собственные механизмы управления безопасностью;
* набор сертифицированных механизмов, которые интегрированы между собой.

**Длинный список**

* СЗИ Dallas Lock 8.0 интегрируется с учётными записями и правами Active Directory, но корректно работает и вне Windows-доменов;
* для корректной работы Сервера безопасности Dallas Lock не требуется ни серверной ОС, ни сторонней СУБД;
* СЗИ Dallas Lock 8.0 включает сертифицированные модули: защита от НСД, СКН уровня подключения съемных носителей, СКН уровня отчуждения (переноса) информации, МЭ, СОВ, а также Модуль паспортизации программного обеспечения, модуль Резервного копирования произвольных объектов и модуль Безопасной среды («песочницы»);
* защита конфиденциальной информации от несанкционированного доступа на персональных, портативных и мобильных компьютерах (ноутбуках и планшетных ПК), серверах (файловых, контроллерах домена и терминального доступа), работающих как автономно, так и в составе ЛВС;
* поддерживает виртуальные среды;
* дискреционный принцип разграничения доступа к информационным ресурсам и подключаемым устройствам в соответствии со списками пользователей и их правами доступа (матрица доступа);
* аудит действий пользователей — санкционированных и без соответствующих прав, ведение журналов регистрации событий;
* контроль целостности файловой системы, программно-аппаратной среды и реестра;
* объединение защищенных ПК для централизованного управления механизмами безопасности;
* приведение АС, ГИС, АСУ ТП, КИИ и систем обработки ПДн в соответствие законодательству РФ по защите информации;
* собственные механизмы управления безопасностью;
* набор сертифицированных механизмов, которые интегрированы между собой.

Информация о сертификации

СЗИ Dallas Lock 8.0-K сертифицирована ФСТЭК России на соответствие 4 уровню доверия (УД 4), 5 классу защищенности СВТ от НСД, 4 классу защиты МЭ (ИТ.МЭ.В4.ПЗ), 4 классу защиты СОВ (ИТ.СОВ.У4.ПЗ), 4 классу защиты СКН (ИТ.СКН.П4.ПЗ, ИТ.СКН.Н4.ПЗ).

Сертификат № 2720 от 25 сентября 2012 г.

Цифровую копию сертификата вы можете скачать в личном кабинете на сайте dallaslock.ru или получить по электронной почте, отправив запрос в коммерческий департамент: [isc@confident.ru](mailto:isc@confident.ru)

Приказом Минкомсвязи России № 165 от 18.04.2016 г. СЗИ НСД Dallas Lock 8.0-К, а также входящие в него Сервер безопасности и Сервер лицензий, включены в единый реестр российских программ для ЭВМ и БД.

Номер записи реестра — № 407 от 18.04.2016 г.

Ссылка: <https://reestr.digital.gov.ru/reestr/301756/?sphrase_id=2327134>

Ссылка на страницу продукта на сайте вендора

<https://dallaslock.ru/products/szi-nsd-dallas-lock/szi-ot-nsd-dallas-lock-8-0-k/>

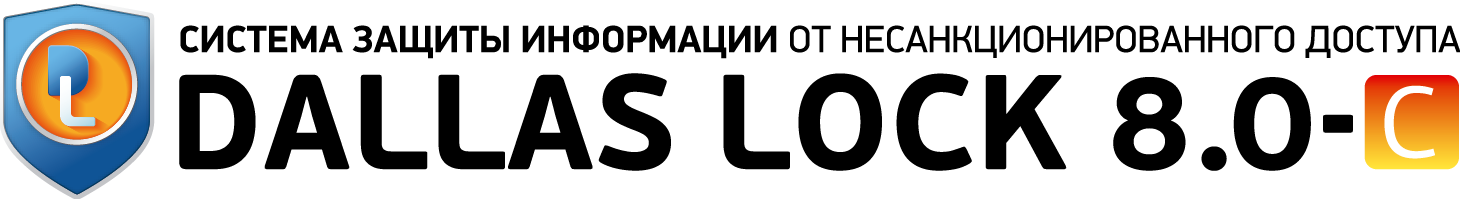
# Dallas Lock 8.0-С

## Графические материалы

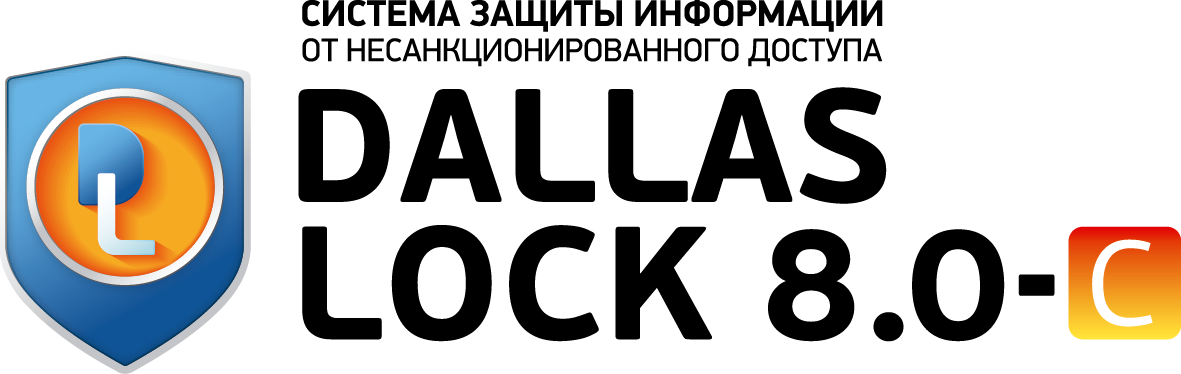
Ссылка на графические материалы:

<https://dallaslock.ru/upload/dallasdocs/szi_nsd_dallas_lock_8.0-C.zip>

Значок продукта



Значок продукта (прямоугольник)

****

## Информация о продукте

**Краткое название**

СЗИ НСД Dallas Lock 8.0-С

**Развернутое название**

Сертифицированная система защиты информации от несанкционированного доступа Dallas Lock 8.0-С

Позиционирование

Программный комплекс средств защиты конфиденциальной информации и информации, содержащей сведения, составляющие государственную тайну до уровня «совершенно секретно» включительно, в локальных и сетевых АРМ под управлением ОС семейства Windows.

Описание

**Малое**

СЗИ НСД Dallas Lock 8.0-С — система защиты конфиденциальной и секретной (до уровня «совершенно секретно» включительно) информации от несанкционированного доступа.

**Среднее**

СЗИ НСД Dallas Lock 8.0-C — сертифицированная система защиты конфиденциальной и секретной (до уровня «совершенно секретно» включительно) информации от несанкционированного доступа накладного типа в персональных компьютерах с ОС семейства Windows.

**Большое**

СЗИ НСД Dallas Lock 8.0-C — сертифицированная система защиты конфиденциальной и секретной (до уровня «совершенно секретно» включительно) информации от несанкционированного доступа накладного типа в персональных компьютерах с ОС семейства Windows.

Комплексная защита конечной точки обеспечивается набором сертифицированных модулей СЗИ Dallas Lock 8.0-С:

* Межсетевой экран;
* Система обнаружения и предотвращения вторжений;
* СКН уровня подключения съемных носителей;
* СКН уровня отчуждения (переноса) информации;
* Модуль паспортизации программного обеспечения;
* Резервное копирование произвольных объектов.

Ключевые особенности

**Короткий список**

* СЗИ Dallas Lock 8.0 интегрируется с учётными записями и правами Active Directory, но корректно работает и вне Windows-доменов;
* для корректной работы Сервера безопасности Dallas Lock не требуется ни серверной ОС, ни сторонней СУБД;
* СЗИ Dallas Lock 8.0 включает сертифицированные модули: защита от НСД, СКН уровня подключения съемных носителей, СКН уровня отчуждения (переноса) информации, МЭ, СОВ, а также Модуль паспортизации программного обеспечения, модуль Резервного копирования произвольных объектов и модуль Безопасной среды («песочницы»).

**Средний список**

* СЗИ Dallas Lock 8.0 интегрируется с учётными записями и правами Active Directory, но корректно работает и вне Windows-доменов;
* для корректной работы Сервера безопасности Dallas Lock не требуется ни серверной ОС, ни сторонней СУБД;
* СЗИ Dallas Lock 8.0 включает сертифицированные модули: защита от НСД, СКН уровня подключения съемных носителей, СКН уровня отчуждения (переноса) информации, МЭ, СОВ, а также Модуль паспортизации программного обеспечения, модуль Резервного копирования произвольных объектов и модуль Безопасной среды («песочницы»);
* защита конфиденциальной и секретной (до уровня «совершенно секретно» включительно) информации от несанкционированного доступа;
* дискреционный и мандатный принципы разграничения доступа к информационным ресурсам;
* аудит действий пользователей;
* объединение защищенных ПК для централизованного управления механизмами безопасности;
* контроль целостности файловой системы, программно-аппаратной среды и реестра;
* приведение АС, ГИС, АСУ ТП, КИИ и систем обработки ПДн в соответствие законодательству РФ по защите информации.

**Длинный список**

* СЗИ Dallas Lock 8.0 интегрируется с учётными записями и правами Active Directory, но корректно работает и вне Windows-доменов;
* для корректной работы Сервера безопасности Dallas Lock не требуется ни серверной ОС, ни сторонней СУБД;
* СЗИ Dallas Lock 8.0 включает сертифицированные модули: защита от НСД, СКН уровня подключения съемных носителей, СКН уровня отчуждения (переноса) информации, МЭ, СОВ, а также Модуль паспортизации программного обеспечения, модуль Резервного копирования произвольных объектов и модуль Безопасной среды («песочницы»);
* защита информации от несанкционированного доступа на персональных компьютерах, портативных и мобильных компьютерах (ноутбуках и планшетных ПК), серверах (файловых, контроллерах домена и терминального доступа), работающих как автономно, так и в составе ЛВС. Поддерживает виртуальные среды;
* дискреционный и мандатный принципы разграничения доступа к информационным ресурсам и подключаемым устройствам;
* аудит действий пользователей — санкционированных и без соответствующих прав, ведение журналов регистрации событий;
* контроль целостности файловой системы, программно-аппаратной среды и реестра;
* объединение защищенных ПК для централизованного управления механизмами безопасности;
* приведение АС, ГИС, АСУ ТП, КИИ и систем обработки ПДн в соответствие законодательству РФ по защите информации.

Информация о сертификации

СЗИ Dallas Lock 8.0-C сертифицирована ФСТЭК России на соответствие 2 уровню доверия (УД 2), 3 классу защищенности от НСД, классу защиты МЭ ИТ.МЭ.В4.П3, классу защиты СОВ ИТ.СОВ.У4.ПЗ, классу защиты СКН ИТ.СКН.П2.ПЗ и ИТ.СКН.Н2.ПЗ.

Сертификат ФСТЭК России № 2945 от 16 августа 2013 г.

Цифровую копию сертификата вы можете скачать в личном кабинете на сайте dallaslock.ru или получить по электронной почте, отправив запрос в коммерческий департамент: [isc@confident.ru](mailto:isc@confident.ru)

Приказом Минкомсвязи России № 151 от 08.04.2016 г. СЗИ НСД Dallas Lock 8.0-С, а также входящие в него Сервер безопасности и Сервер лицензий, включены в единый реестр российских программ для ЭВМ и БД.

Номер записи реестра — № 313 от 08.04.2016 г.

Ссылка: <https://reestr.digital.gov.ru/reestr/301662/?sphrase_id=2327134>

Ссылка на страницу продукта на сайте вендора

<https://dallaslock.ru/products/szi-nsd-dallas-lock/szi-ot-nsd-dallas-lock-8-0-s/>

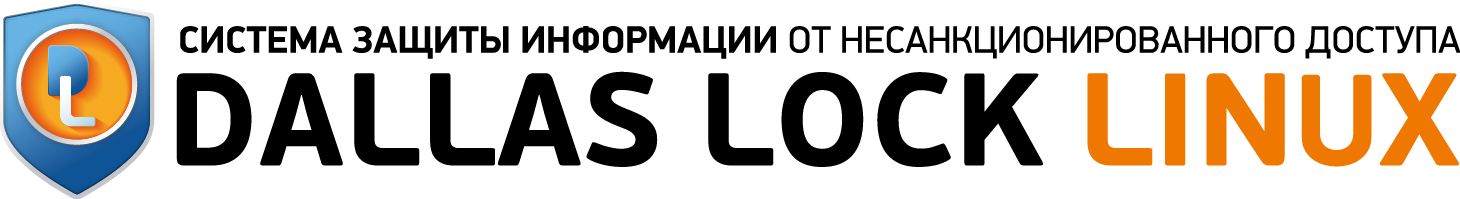
# СЗИ НСД Dallas Lock Linux

## Графические материалы

Ссылка на графические материалы:

<https://dallaslock.ru/upload/dallasdocs/szi_nsd_dallas_lock_Linux.zip>

Значок продукта (строка)



Значок продукта (прямоугольник)



## Информация о продукте

**Краткое название**

СЗИ НСД Dallas Lock Linux

**Развернутое название**

Система защиты конфиденциальной информации от несанкционированного доступа Dallas Lock Linux

Позиционирование

Программный комплекс средств защиты информации в ОС семейства Linux с возможностью подключения аппаратных идентификаторов.

Описание продукта

**Малое**

СЗИ НСД Dallas Lock Linux — система защиты конфиденциальной информации в локальных и сетевых АРМ под управлением ОС семейства Linux.

**Среднее**

СЗИ НСД Dallas Lock Linux — сертифицированная система защиты конфиденциальной информации накладного типа для персональных компьютеров (автономных и в составе локально-вычислительной сети) под управлением ОС семейства Linux.

**Большое**

СЗИ НСД Dallas Lock Linux — сертифицированная система защиты конфиденциальной информации накладного типа предназначена для автономных персональных компьютеров и компьютеров в составе локально-вычислительной сети.

Представляет собой программный комплекс средств защиты информации от несанкционированного доступа в ОС семейства Linux с возможностью подключения аппаратных идентификаторов. Легко интегрируется в сложные сетевые инфраструктуры, благодаря собственному набору сертифицированных решений.

Ключевые особенности

**Короткий список**

* поддержка широкого набора Linux-дистрибутивов, в том числе Astra Linux Common Edition, Альт Linux и РЕД ОС;
* собственные сертифицированные механизмы управления информационной безопасностью;
* удобное централизованное управление в случае одновременного использования компьютеров ОС Windows и ОС Linux.

**Средний список**

* поддержка широкого набора Linux-дистрибутивов, в том числе Astra Linux Common Edition, Альт Linux и РЕД ОС;
* собственные сертифицированные механизмы управления информационной безопасностью;
* удобное централизованное управление в случае одновременного использования компьютеров ОС Windows и ОС Linux;
* современный графический интерфейс (GUI);
* сервис-ориентированная архитектура;
* «бесшовная» интеграция с другими решениями продуктовой линейки Dallas Lock;
* контроль целостности программного обеспечения;
* выполнение требований законодательства РФ по защите информации ограниченного доступа.

**Длинный список**

* поддержка широкого набора Linux-дистрибутивов, в том числе Astra Linux Common Edition, Альт Linux и РЕД ОС;
* собственные сертифицированные механизмы управления информационной безопасностью;
* удобное централизованное управление в случае одновременного использования компьютеров ОС Windows и ОС Linux;
* современный графический интерфейс (GUI);
* сервис-ориентированная архитектура (позволит использовать СЗИ НСД Dallas Lock Linux для защиты сложных распределённых систем с учетом повышенных требований к масштабируемости и управляемости);
* «бесшовная» интеграция с другими решениями продуктовой линейки Dallas Lock;
* контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации;
* выполнение требований законодательства РФ по защите информации ограниченного доступа.

Информация о сертификации

СЗИ НСД Dallas Lock Linux сертифицирована ФСТЭК России на соответствие по 5 классу защищенности СВТ от НСД, 4 классу защиты СКН (ИТ.СКН.П4.ПЗ), 4 уровню доверия (УД 4).

Сертификат ФСТЭК России № 3594 от 04 июля 2016 г.

Цифровую копию сертификата вы можете скачать в личном кабинете на сайте dallaslock.ru или получить по электронной почте, отправив запрос в коммерческий департамент: [isc@confident.ru](mailto:isc@confident.ru)

Приказом Минкомсвязи России № 426 от 06.09.2016 г. Dallas Lock Linux включен в единый реестр российских программ для ЭВМ и БД.

Номер записи реестра — № 1285 от 05.09.2016 г.

Ссылка: <https://reestr.digital.gov.ru/reestr/302635/?sphrase_id=2327134>

Ссылка на страницу продукта на сайте вендора

<https://dallaslock.ru/products/szi-nsd-dallas-lock-linux/>

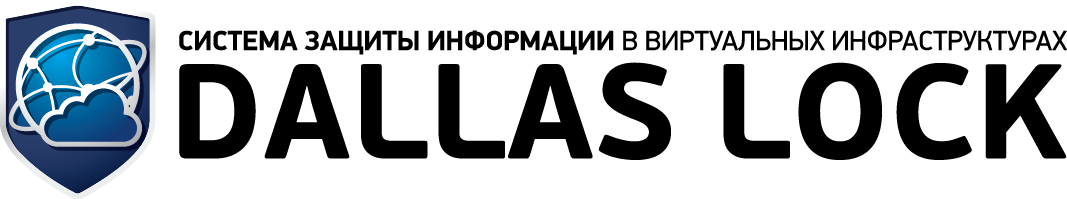
# СЗИ ВИ Dallas Lock

## Графические материалы

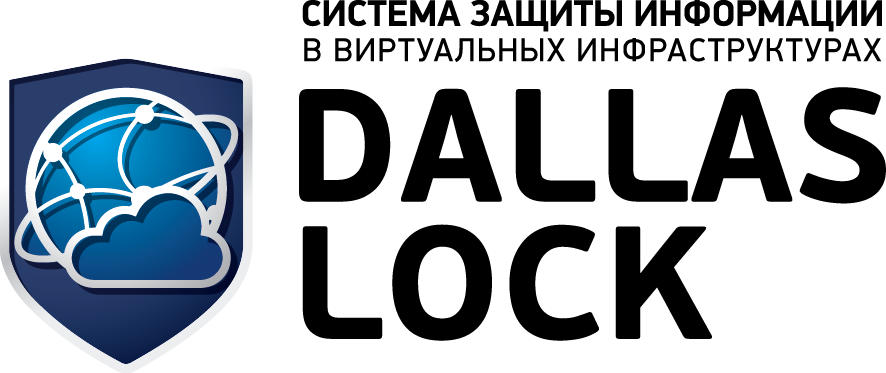
Ссылка на графические материалы:

<https://dallaslock.ru/upload/dallasdocs/szi_vi_dallas_lock.zip>

Значок продукта



Значок продукта (прямоугольник)



## Информация о продукте

**Краткое название**

СЗИ ВИ Dallas Lock

**Развернутое название**

Сертифицированная система защиты информации в виртуальных инфраструктурах Dallas Lock

Позиционирование

Система защиты информации от несанкционированного доступа в виртуальных средах на базе oVirt, zVirt, «РЕД Виртуализация», HOSTVM, KVM, VMware vSphere и Microsoft Hyper-V.

Описание

**Малое**

СЗИ ВИ Dallas Lock — сертифицированная система защиты информации в виртуальных инфраструктурах на базе oVirt, zVirt, «РЕД Виртуализация», HOSTVM, KVM, VMware vSphere и Microsoft Hyper-V.

**Среднее**

СЗИ ВИ Dallas Lock — система защиты информации в виртуальных инфраструктурах. Обеспечивает защиту конфиденциальной информации от несанкционированного доступа в виртуальных средах на базе oVirt, zVirt, «РЕД Виртуализация», HOSTVM, KVM, VMware vSphere и Microsoft Hyper-V. Имеет две версии: «стандартную» и «расширенную».

**Большое**

СЗИ ВИ Dallas Lock — система защиты информации в виртуальных инфраструктурах, предназначенная для комплексной и многофункциональной защиты конфиденциальной информации от несанкционированного доступа в виртуальных средах на базе oVirt, zVirt, «РЕД Виртуализация», HOSTVM, KVM, VMware vSphere и Microsoft Hyper-V. Имеет две версии: «стандартную» и «расширенную».

Комплексная защита обеспечивается, в том числе модулями системы:

* сервер безопасности виртуальной инфраструктуры;
* клиентская часть СЗИ НСД Dallas Lock 8.0;
* агент Dallas Lock.

Ключевые особенности «стандартной» версии

**Короткий список**

* сканирование настроек виртуальной инфраструктуры;
* интеграция с ролевой моделью VMware;
* работа с несколькими облаками виртуализации;
* легко интегрируется в виртуальную инфраструктуру любого размера и вида. Минимизируется время, необходимое для настройки и запуска системы;

**Средний список**

* сканирование настроек виртуальной инфраструктуры;
* интеграция с ролевой моделью VMware;
* работа с несколькими облаками виртуализации;
* легко интегрируется в виртуальную инфраструктуру любого размера и вида. Минимизируется время, необходимое для настройки и запуска системы;
* продвинутый механизм контроля целостности;
* возможность управления несколькими серверами виртуализации из единой консоли;
* лицензирование по количеству физических процессоров гипервизора ESXi;
* соответствие требованиям ФСТЭК России в части защиты среды виртуализации;
* возможно построение комплексного решения по защите информации в виртуализованной и физической ИТ-инфраструктуре;
* фильтрация сетевого трафика по предустановленным правилам;
* регистрация событий безопасности в виртуальной среде.

**Длинный список**

* сканирование настроек виртуальной инфраструктуры;
* интеграция с ролевой моделью VMware;
* работа с несколькими облаками виртуализации;
* легко интегрируется в виртуальную инфраструктуру любого размера и вида. Минимизируется время, необходимое для настройки и запуска системы;
* продвинутый механизм контроля целостности (в том числе контроль целостности образа BIOS ВМ, настроек и конфигураций ВМ до загрузки гостевой ОС);
* возможность управления несколькими серверами виртуализации из единой консоли.
* лицензирование по количеству физических процессоров гипервизора ESXi, а не виртуальных машин. Возможно гибкое управление квотами на количество физических процессоров (с помощью дополнительного модуля Сервера лицензий Dallas Lock).
* соответствие требованиям ФСТЭК России в части защиты среды виртуализации;
* возможно построение комплексного решения по защите информации в виртуализованной и физической ИТ-инфраструктуре с использованием всего спектра интегрированных между собой решений из продуктовой линейки СЗИ Dallas Lock.
* фильтрация сетевого трафика по предустановленным правилам с возможностью их редактирования или гибкой настройки;
* регистрация событий безопасности в виртуальной среде, гибкая настройка аудита гипервизора и прозрачное взаимодействие с механизмами системы виртуализации;
* доверенная загрузка виртуальных машин;
* зачистка остаточной информации виртуальных машин.

Дополнительные особенности «расширенной» версии

* мониторинг виртуальной инфраструктуры с помощью графической панели;
* поддержка серверов управления vCenter Linked Mode;
* поддержка VMware Auto-Deploy;
* поддержка vCenter High Availability;
* контроль управления серверами Hyper-V через System Center Virtual Machine Manager;
* контроль управления через Failover Cluster Manager;
* поддержка VMware Fault Tolerance.

Информация о сертификации

СЗИ ВИ Dallas Lock сертифицировано на соответствие требованиям ФСТЭК России по 5 классу защищенности СВТ от НСД и 4 уровню доверия (УД 4).

Сертификат ФСТЭК России: № 3837 от 18 декабря 2017 г.

Цифровую копию сертификата вы можете скачать в личном кабинете на сайте dallaslock.ru или получить по электронной почте, отправив запрос в коммерческий департамент: [isc@confident.ru](mailto:isc@confident.ru)

Приказом Минкомсвязи России № 487 от 07.10.2016 г. СЗИ ВИ Dallas Lock включен в единый реестр российских программ для ЭВМ и БД.

Номер записи реестра — № 2032 от 08.10.2016 г.

Ссылка: <https://reestr.digital.gov.ru/reestr/303382/?sphrase_id=2327198>

Ссылка на страницу продукта на сайте вендора

<https://dallaslock.ru/products/szi-vi-dallas-lock/>

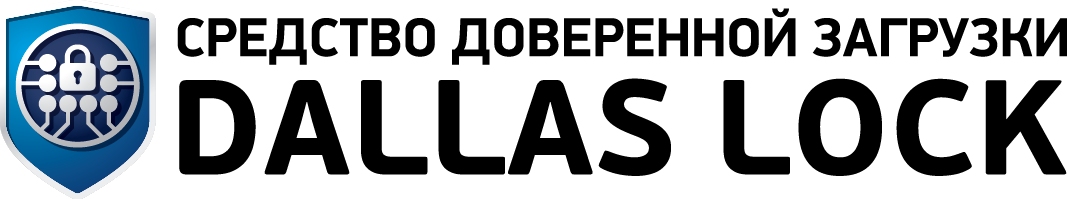
# СДЗ Dallas Lock

## Графические материалы

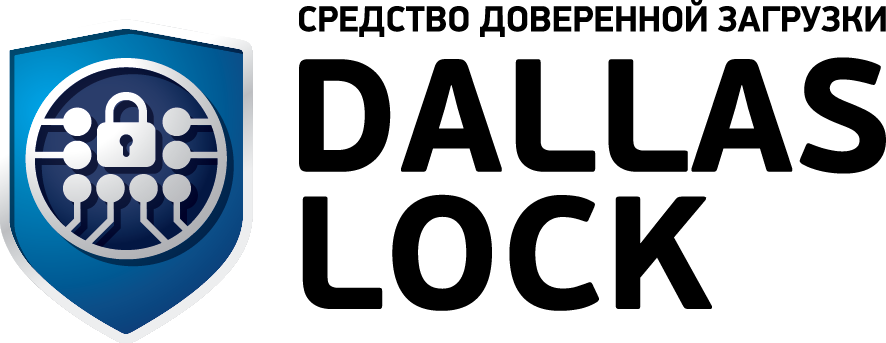
Ссылка на графические материалы:

<https://dallaslock.ru/upload/dallasdocs/sdz_dallas_lock.zip>

Значок продукта (строка)



Значок продукта (прямоугольник)



## Информация о продукте

**Краткое название**

СДЗ Dallas Lock

**Развернутое название**

Средство доверенной загрузки Dallas Lock

Позиционирование

Решение уровня платы расширения, предназначенное для защиты информации, содержащей сведения, составляющие государственную тайну до уровня «совершенно секретно» включительно, и иной информации с ограниченным доступом.

Описание продукта

**Малое**

СДЗ Dallas Lock — это два решения, которые блокируют попытки несанкционированной загрузки нештатной операционной системы.

**Среднее**

СДЗ Dallas Lock — это два решения, которые блокируют попытки несанкционированной загрузки нештатной операционной системы. СДЗ ПР — решение уровня платы расширения. СДЗ УБ — решение уровня базовой системы ввода-вывода.

**Большое**

СДЗ Dallas Lock — это два решения, которые блокируют попытки несанкционированной загрузки нештатной операционной системы. СДЗ ПР — решение уровня платы расширения. СДЗ УБ — решение уровня базовой системы ввода-вывода.

Оба решения предназначены для защиты информации, содержащей сведения, составляющие государственную тайну до уровня «совершенно секретно» включительно, и иной информации с ограниченным доступом.

Ключевые особенности СДЗ ПР

**Короткий список**

* полноценная поддержка UEFI и безопасного режима загрузки UEFI («Secureboot»). Совместимость со многими современными моделями компьютеров;
* собственные часы с независимым источником питания. Возможность отслеживать вскрытие корпуса выключенного компьютера;
* администрирование и централизованное управление проводится без использования ресурсов штатной ОС. Поддерживаются доменные учётные записи;
* контроль целостности загружаемой операционной системы.

**Средний список**

* полноценная поддержка UEFI и безопасного режима загрузки UEFI («Secureboot»). Совместимость со многими современными моделями компьютеров;
* собственные часы с независимым источником питания. Возможность отслеживать вскрытие корпуса выключенного компьютера;
* администрирование и централизованное управление проводится без использования ресурсов штатной ОС. Поддерживаются доменные учётные записи;
* хранение ключевой, служебной и другой необходимой информации в энергонезависимой памяти платы СДЗ;
* поддерживается широкий спектр аппаратных идентификаторов;
* контроль целостности загружаемой операционной системы;
* разграничение доступа к управлению СДЗ;
* датчик вскрытия корпуса (для варианта исполнения — PCIe «KT-500»);
* наличие собственных часов с независимым источником питания (для варианта исполнения — PCIe «KT-500»);
* несколько вариантов исполнения – для шин и разъемов PCI-E, miniPCI-E, M.2;
* централизованное управление.

**Длинный список**

* полноценная поддержка UEFI и безопасного режима загрузки UEFI («Secureboot»). Совместимость со многими современными моделями компьютеров;
* собственные часы с независимым источником питания. Возможность отслеживать вскрытие корпуса выключенного компьютера;
* администрирование и централизованное управление проводится без использования ресурсов штатной ОС. Поддерживаются доменные учётные записи;
* хранение ключевой, служебной и другой необходимой информации в энергонезависимой памяти платы СДЗ;
* поддерживается широкий спектр аппаратных идентификаторов: USB-ключи и смарт-карты Aladdin eToken Pro/Java, Рутокен, JaCarta (JaCarta ГОСТ, JaCarta PKI), электронные ключи Touch Memory (iButton), ESMART;
* контроль целостности загружаемой операционной системы, блокирование загрузки операционной системы при нарушении целостности загружаемой программной среды (операционной системы);
* возможность сохранения (восстановления) параметров конфигурации СДЗ на различные носители информации;
* разграничение доступа к управлению СДЗ;
* датчик вскрытия корпуса (для варианта исполнения — PCIe «KT-500»);
* наличие собственных часов с независимым источником питания (для варианта исполнения — PCIe «KT-500»);
* несколько вариантов исполнения – для шин и разъемов PCI-E, miniPCI-E, M.2;
* централизованное управление.

Информация о сертификации СДЗ ПР

СДЗ Dallas Lock сертифицировано ФСТЭК России на соответствие требованиям к СДЗ по 2 классу защиты ИТ.СДЗ.ПР2.ПЗ и 2 уровню доверия (УД 2).

Сертификат ФСТЭК России № 3666 от 25 ноября 2016 г.

СДЗ Dallas Lock сертифицировано Минобороны России на соответствие требованиям к СДЗ по 2 классу защиты ИТ.СДЗ.ПР2.ПЗ, 2 уровню контроля отсутствия НДВ, РДВ, КИКТ.

Сертификат Минобороны России № 5695 от 31 марта 2022 г.

СДЗ Dallas Lock сертифицировано союзом «Санкт-Петербургская торгово-промышленная палата» по форме СТ-1. Сертификат официально подтверждает, что Российская Федерация является страной происхождения СДЗ Dallas Lock, а также то, что оно соответствует всем требованиям к происхождению, установленным к таким товарам.

Сертификат СТ-1 от 21 сентября 2020 г.

Приказом Минкомсвязи России № 487 от 07.10.2016 г. СДЗ Dallas Lock включен в единый реестр российских программ для ЭВМ и БД.

Номер записи реестра — № 2019 от 08.10.2016 г.

Ссылка: <https://reestr.digital.gov.ru/reestr/303369/?sphrase_id=2327198>

Также СДЗ Dallas Lock включен в реестр Минпромторга России: заключение № 55687/11 от 10.06.2022.

Реестровая запись № 1267\1\2022.

Ссылка: <https://gisp.gov.ru/goods/#/product/2663638>

Цифровые копии сертификатов вы можете скачать в личном кабинете на сайте dallaslock.ru или получить по электронной почте, отправив запрос в коммерческий департамент: [isc@confident.ru](mailto:isc@confident.ru)

Ключевые особенности СДЗ УБ

**Короткий список**

* блокирование загрузки операционной системы;
* контроль целостности программно-аппаратной среды;
* поддерживается широкий спектр аппаратных идентификаторов: USB-ключи и смарт-карты.

**Средний список**

* блокирование загрузки операционной системы. Изделие позволяет блокировать загрузку операционной системы при следующих событиях:
  + выявление попыток загрузки нештатной операционной системы;
  + превышение числа неудачных попыток аутентификации пользователя;
  + нарушение целостности средства доверенной загрузки, загружаемой программной среды, состава аппаратных компонентов;
  + критичные типы сбоев и ошибок, для которых требуется аварийная поддержка и восстановление и которые затрагивают функции безопасности и не могут быть устранены.
* контроль целостности программно-аппаратной среды. СДЗ УБ Dallas Lock позволяет осуществлять контроль целостности следующих типов объектов:
  + «Файловая система»;
  + «Реестр ОС MS Windows»;
  + «Области диска»;
  + «CMOS»;
  + «Таблицы SMBIOS»;
  + «Образы BIOS»;
  + «Аппаратная конфигурация»;
  + «Программное обеспечение СДЗ УБ».
* поддерживается широкий спектр аппаратных идентификаторов. Поддерживаемые аппаратные идентификаторы: USB-ключи и смарт-карты:
  + Aladdin
  + USB-ключи и смарт-карты Рутокен;
  + электронные ключи Touch Memory;
  + USB-ключи и смарт-карты ESMART;
  + USB-ключи и смарт-карты JaCarta;
  + USB-ключи Guardant.

**Длинный список**

* блокирование загрузки операционной системы. Изделие позволяет блокировать загрузку операционной системы при следующих событиях:
  + выявление попыток загрузки нештатной операционной системы;
  + превышение числа неудачных попыток аутентификации пользователя;
  + нарушение целостности средства доверенной загрузки, загружаемой программной среды, состава аппаратных компонентов;
  + критичные типы сбоев и ошибок, для которых требуется аварийная поддержка и восстановление и которые затрагивают функции безопасности и не могут быть устранены.
* контроль целостности программно-аппаратной среды. СДЗ УБ Dallas Lock позволяет осуществлять контроль целостности следующих типов объектов:
  + «Файловая система»;
  + «Реестр ОС MS Windows»;
  + «Области диска»;
  + «CMOS»;
  + «Таблицы SMBIOS»;
  + «Образы BIOS»;
  + «Аппаратная конфигурация»;
  + «Программное обеспечение СДЗ УБ».
* поддерживается широкий спектр аппаратных идентификаторов. Поддерживаемые аппаратные идентификаторы: USB-ключи и смарт-карты:
  + Aladdin (Aladdin eToken Pro/Java);
  + USB-ключи и смарт-карты Рутокен (Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен ЭЦП 3.0);
  + электронные ключи Touch Memory (iButton);
  + USB-ключи и смарт-карты ESMART (ESMART Token, ESMART Token ГОСТ);
  + USB-ключи и смарт-карты JaCarta (JaCarta ГОСТ, JaCarta SF/ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta-2 ГОСТ, JaCarta PKI);
  + USB-ключи Guardant ID 2.0.

Информация о сертификации СДЗ УБ

СДЗ УБ Dallas Lock сертифицировано ФСТЭК России на соответствие требованиям к СДЗ уровня базовой системы ввода-вывода по 2 классу защиты ИТ.СДЗ.УБ2.ПЗ и 2 уровню доверия (УД 2).

Сертификат ФСТЭК России № 4786 от 13 марта 2024 г.

СДЗ УБ Dallas Lock включено в реестр Минкомсвязи России от 14 декабря 2023 г.

Реестровая запись: № 20592 от 14 декабря 2023 г.

Ссылка: <https://reestr.digital.gov.ru/reestr/2012017/?sphrase_id=4238775>

Цифровые копии сертификатов вы можете скачать в личном кабинете на сайте dallaslock.ru или получить по электронной почте, отправив запрос в коммерческий департамент: isc@confident.ru

Ссылка на страницу продукта на сайте вендора

СДЗ ПР Dallas Lock: <https://dallaslock.ru/products/sdz-dallas-lock/sdz-pr-dallas-lock/>

СДЗ УБ Dallas Lock: <https://dallaslock.ru/products/sdz-dallas-lock/sdz-ub-dallas-lock/>

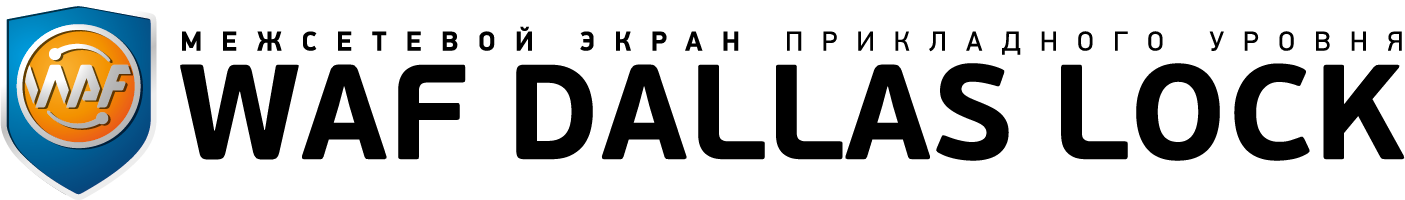
# WAF Dallas Lock

## Графические материалы

Ссылка на графические материалы:

<https://dallaslock.ru/upload/dallasdocs/waf-logos.7z>

Значок продукта



Значок продукта (прямоугольник)



## Информация о продукте

**Краткое название**

WAF Dallas Lock

**Развернутое название**

Межсетевой экран прикладного уровня Dallas Lock

Позиционирование

WAF Dallas Lock предназначен для защиты веб-серверов, расположенных в демилитаризованной зоне (DMZ), и сетевой инфраструктуры (LAN) от угроз, исходящих из глобальной сети Интернет (WAN).

Описание

**Малое**

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.

**Среднее**

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. Включает в себя два функциональных модуля: WAF (Web Application Firewall) и UTM (Unified Threat Management).

**Большое**

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. Включает в себя два функциональных модуля:

WAF (Web Application Firewall) — межсетевой экран уровня веб-приложений;

UTM (Unified Threat Management) — межсетевой экран уровня логических границ сети и система обнаружения вторжений уровня сети.

Ключевые особенности

**Короткий список**

* высокоуровневая защита. Прикладной уровень — атака на веб-приложение;
* низкоуровневая защита. Транспортный и сетевой уровень — атака на сетевую инфраструктуру;
* защита от угроз из списка OWASP TOP 10: XSS, CSRF, bruteforce-атак;
* защита корпоративных ресурсов от информационных атак известных типов в режиме 24/7;

**Средний список**

* высокоуровневая защита. Прикладной уровень — атака на веб-приложение;
* низкоуровневая защита. Транспортный и сетевой уровень — атака на сетевую инфраструктуру;
* защита от угроз из списка OWASP TOP 10: XSS, CSRF, bruteforce-атак;
* защита корпоративных ресурсов от информационных атак известных типов в режиме 24/7;
* анализ трафика веб-приложений и обнаружение атак (вторжений). Анализ XML-API и JSON и поддержка протокола HTTP/2. Инспекция SSL/TLS;
* отображение нагрузки на информационные ресурсы компании. Общая графическая панель мониторинга системы с отображением статистики;
* обнаружение подозрительной активности пользователей веб-приложений;
* блокирование попыток сетевых атак при работе с веб-приложениями;

**Длинный список**

* высокоуровневая защита. Прикладной уровень — атака на веб-приложение;
* низкоуровневая защита. Транспортный и сетевой уровень — атака на сетевую инфраструктуру;
* защита от угроз из списка OWASP TOP 10: XSS, CSRF, bruteforce-атак;
* защита корпоративных ресурсов от информационных атак известных типов в режиме 24/7;
* анализ трафика веб-приложений и обнаружение атак (вторжений). Анализ XML-API и JSON и поддержка протокола HTTP/2. Инспекция SSL/TLS;
* отображение нагрузки на информационные ресурсы компании. Общая графическая панель мониторинга системы с отображением статистики;
* обнаружение подозрительной активности пользователей веб-приложений;
* блокирование попыток сетевых атак при работе с веб-приложениями;
* гибкая настройка правил и политик фильтрации трафика. Возможность создавать собственные правила защиты;
* настройка параметров защиты отдельно для каждого ресурса;
* централизованный мониторинг и управление защитой нескольких веб-приложений из единой консоли;
* интеграция c SIЕМ-системами по протоколу syslog в формате leef;
* журналирование инцидентов информационной безопасности.

Информация о сертификации

WAF Dallas Lock находится на сертификации на соответствие требованиям по безопасности информации ФСТЭК России (окончание сертификации – 2 квартал 2024 года): по 4 классу защиты МЭ (ИТ.МЭ.Б4.ПЗ), по 4 классу защиты МЭ (ИТ.МЭ.Г4.ПЗ), по 4 классу защиты СОВ уровня сети (ИТ.СОВ.С4.ПЗ), по 4 уровню доверия (УД 4).

WAF Dallas Lock включен в реестр Минкомсвязи России 15 марта 2024 г.

Реестровая запись: № 21831 от 15 марта 2024 г.

Ссылка: <https://reestr.digital.gov.ru/reestr/2224058/?sphrase_id=4238775>

Ссылка на страницу продукта на сайте вендора

<https://dallaslock.ru/products/waf-dallas-lock/>

**Дополнительные модули и продукты**

# Межсетевой экран

## Графические материалы

Ссылка на графические материалы:

<https://dallaslock.ru/upload/dallasdocs/me_2021.zip>

Значок продукта



## Информация о продукте

**Краткое название**

МЭ Dallas lock

**Полное название**

Межсетевой экран Dallas Lock

Позиционирование

Сертифицированный модуль СЗИ НСД Dallas Lock 8.0, выполняющий функции персонального межсетевого экрана с централизованным управлением.

Описание

**Малое**

Межсетевой экран Dallas Lock — сертифицированный модуль СЗИ НСД Dallas Lock 8.0, выполняющий функции персонального межсетевого экрана с централизованным управлением.

**Среднее**

Межсетевой экран Dallas Lock предназначен для защиты рабочих станций и серверов от несанкционированного доступа посредством осуществления контроля и фильтрации сетевых пакетов, проходящих через сетевые интерфейсы.

**Большое**

Межсетевой экран Dallas Lock — сертифицированный модуль СЗИ НСД Dallas Lock 8.0. Предназначен для защиты рабочих станций и серверов от несанкционированного доступа посредством осуществления контроля и фильтрации проходящих через сетевые интерфейсы ПК сетевых пакетов в соответствии с заданными правилами.

Тесно интегрирован с СЗИ НСД Dallas Lock 8.0, что позволяет производить централизованное развертывание и управление НСД и МЭ из единого общего интерфейса.

Ключевые особенности

**Короткий список**

* возможность полного блокирования передачи данных по определенным сетевым протоколам;
* блокировка неблагонадежных ресурсов в сети Интернет как с использованием IP-адреса, так и по URL сайта;
* гибкая настройка отдельных правил фильтрации, а также возможность выполнения групповых операций над правилами.

**Средний список**

* возможность полного блокирования передачи данных по определенным сетевым протоколам;
* блокировка неблагонадежных ресурсов в сети Интернет как с использованием IP-адреса, так и по URL сайта;
* гибкая настройка отдельных правил фильтрации, а также возможность выполнения групповых операций над правилами;
* возможность применения для защиты конфиденциальной информации в ИТ-инфраструктурах, имеющих подключения к сетям общего пользования;
* «бесшовная» интеграция с СЗИ НСД Dallas Lock 8.0;
* гибкая настройка уведомлений о попытках нарушения сетевых правил;
* дополнительные механизмы защиты от некорректных действий администратора безопасности.

**Длинный список**

* возможность полного блокирования передачи данных по определенным сетевым протоколам;
* блокировка неблагонадежных ресурсов в сети Интернет как с использованием IP-адреса, так и по URL сайта;
* гибкая настройка отдельных правил фильтрации, а также возможность выполнения групповых операций над правилами;
* первый в России сертифицированный межсетевой экран с поддержкой Windows 10;
* возможность применения для защиты конфиденциальной информации в ИТ-инфраструктурах, имеющих подключения к сетям общего пользования;
* «бесшовная» интеграция с СЗИ НСД Dallas Lock 8.0 с возможностью полноценного централизованного управления из единой консоли Сервера безопасности Dallas Lock 8.0;
* настройка правил прикладного уровня с возможностью контроля определенных приложений (исполняемых модулей);
* настройка правил на уровне указания сетевых драйверов (в частности, для корректной работы приложений типа «банк-клиент»);
* настройка правил, действующих для определенных пользователей (групп пользователей и групп компьютеров при использовании Сервера безопасности Dallas Lock 8.0);
* гибкая настройка уведомлений о попытках нарушения сетевых правил с возможностью запуска внешнего процесса при срабатывании правил;
* дополнительные механизмы защиты от некорректных действий администратора безопасности, позволяющие сохранить возможность удаленного переконфигурирования в случае применения некорректных настроек (полной сетевой блокировки).

Информация о сертификации

Межсетевой экран Dallas Lock поставляется только в комплекте с СЗИ НСД Dallas Loсk 8.0 и сертифицирован в соответствии с требованиями ФСТЭК России по 4-му классу защищенности МЭ ИТ.МЭ.В4.П3 и Минобороны России по 3 классу защищенности МЭ (в составе СЗИ НСД Dallas Loсk 8.0).

Сертификаты ФСТЭК России:

1. Для СЗИ НСД Dallas Loсk 8.0-К — № 2720 от 25 сентября 2012 г.
2. Для СЗИ НСД Dallas Loсk 8.0-С — № 2945 от 16 августа 2013 г.

Сертификаты Минобороны России:

Для СЗИ НСД Dallas Loсk 8.0-С — № 3902 от 23 марта 2018 г.

Цифровые копии сертификатов вы можете скачать в личном кабинете на сайте dallaslock.ru или получить по электронной почте, отправив запрос в коммерческий департамент: isc@confident.ru

# Система обнаружения и предотвращения вторжений

## Графические материалы

Ссылка на графические материалы:

<https://dallaslock.ru/upload/dallasdocs/sov_2021.zip>

Значок продукта



## Информация о продукте

**Краткое название**

СОВ Dallas Lock

**Развернутое название**

Система обнаружения и предотвращения вторжений Dallas Lock

Позиционирование

Защита информационных ресурсов от преднамеренного несанкционированного доступа к ним или несанкционированных воздействий на них со стороны внешних или внутренних нарушителей.

Описание

**Малое**

Система обнаружения и предотвращения вторжений Dallas Lock — сертифицированная гибридная система обнаружения и предотвращения вторжений уровня узла в программном исполнении.

**Среднее**

Система обнаружения и предотвращения вторжений Dallas Lock — модуль СЗИ Dallas Lock 8.0. Является сертифицированной гибридной системой обнаружения и предотвращения вторжений уровня узла в программном исполнении.

**Большое**

Система обнаружения и предотвращения вторжений Dallas Lock — сертифицированная гибридная система обнаружения и предотвращения вторжений уровня узла в программном исполнении.

Является модулем СЗИ Dallas Lock 8.0 и реализует защиту от попыток неавторизованного доступа в компьютерную систему или сеть, слежения за попытками нарушения безопасности путем анализа поведения (активности) приложений, анализа журналов операционной системы и прикладного ПО.

Ключевые особенности

**Короткий список**

* сигнатурный и эвристический анализ сетевого траффика, журналов ОС и приложений на предмет нештатных ситуаций и попыток проведения вторжений, а также аномалий в поведении ОС и пользователей;
* применение гибких настроек реагирования на попытки нарушения безопасности (уведомления, блокировки IP-адреса злоумышленника и т. д.);
* осуществление перехвата вызова функций ОС сторонними приложениями с возможностью гибкой настройки ограничения доступа к системным функциям для недоверенных приложений;
* возможность запуска потенциально опасных объектов в Безопасной среде («песочнице»).

**Средний список**

* сигнатурный и эвристический анализ сетевого траффика, журналов ОС и приложений на предмет нештатных ситуаций и попыток проведения вторжений, а также аномалий в поведении ОС и пользователей;
* применение гибких настроек реагирования на попытки нарушения безопасности (уведомления, блокировки IP-адреса злоумышленника и т. д.);
* осуществление перехвата вызова функций ОС сторонними приложениями с возможностью гибкой настройки ограничения доступа к системным функциям для недоверенных приложений;
* возможность запуска потенциально опасных объектов в Безопасной среде («песочнице»);
* обеспечение защиты от атак на сетевые протоколы различных уровней модели OSI;

**Длинный список**

* сигнатурный и эвристический анализ сетевого траффика, журналов ОС и приложений на предмет нештатных ситуаций и попыток проведения вторжений, а также аномалий в поведении ОС и пользователей;
* применение гибких настроек реагирования на попытки нарушения безопасности (уведомления, блокировки IP-адреса злоумышленника и т. д.);
* осуществление перехвата вызова функций ОС сторонними приложениями с возможностью гибкой настройки ограничения доступа к системным функциям для недоверенных приложений;
* возможность запуска потенциально опасных объектов в Безопасной среде («песочнице»);
* обеспечение защиты от атак на сетевые протоколы различных уровней модели OSI;
* обновление сигнатур сетевых атак и сигнатур анализа журналов ОС и приложений.

Информация о сертификации

СОВ Dallas Lock поставляется только в комплекте с СЗИ НСД Dallas Loсk 8.0 и сертифицирован в соответствии с требованиями ФСТЭК России к средствам обнаружения и предотвращения вторжений в составе СЗИ НСД Dallas Loсk 8.0.

* для редакции 8.0-К — сертифицировано по классу защиты СОВ ИТ.СОВ.У4.ПЗ;
* для редакции 8.0-С — сертифицировано по классу защиты СОВ ИТ.СОВ.У4.ПЗ.

Сертификаты ФСТЭК России:

1. Для СЗИ НСД Dallas Loсk 8.0-К — № 2720 от 25 сентября 2012 г.
2. Для СЗИ НСД Dallas Loсk 8.0-С — № 2945 от 16 августа 2013 г.

Цифровые копии сертификатов вы можете скачать в личном кабинете на сайте dallaslock.ru или получить по электронной почте, отправив запрос в коммерческий департамент: isc@confident.ru

# Средство контроля съемных машинных носителей информации

## Графические материалы

Ссылка на графические материалы:

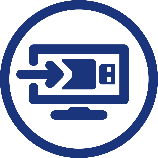
<https://dallaslock.ru/upload/dallasdocs/skn_2021.zip>

Значок продукта

Общий логотип



СКН уровня подключения съёмных носителей



СКН уровня отчуждения (переноса) информации



## Информация о продукте

**Краткое название**

СКН Dallas Lock

**Полное название**

Средство контроля съемных машинных носителей информации Dallas Lock

Позиционирование

Средство защиты от утечки данных с преобразованием информации на съемных машинных носителях.

Описание

**Малое**

Средство контроля съемных машинных носителей информации (СКН) Dallas Lock организует учет съемных носителей информации и предотвращает утечки информации через сменные накопители.

**Среднее**

СКН Dallas Lock — это два сертифицированных модуля в составе СЗИ Dallas Lock 8.0. Модуль СКН уровня подключения съемных носителей позволяет разграничивать доступ пользователей информационной системы к сменным накопителям.

Модуль СКН уровня отчуждения (переноса) информации предотвращает утечки информации через сменные накопители.

**Большое**

СКН Dallas Lock — это два сертифицированных ФСТЭК России модуля в составе СЗИ Dallas Lock 8.0.

Модуль СКН уровня подключения съемных носителей позволяет разграничивать доступ пользователей информационной системы к сменным накопителям — осуществляет контроль подключения накопителей.

Модуль СКН уровня отчуждения (переноса) информации предотвращает утечки информации через сменные накопители, защищает информацию в том числе от внутренних нарушителей.

Ключевые особенности СКН уровня подключения съёмных носителей

**Короткий список**

* ограничение возможности использования конкретных съемных носителей информации на конкретном АРМ;
* гарантированное исключение утечек информации за счёт применения преобразованных носителей информации;
* удобное централизованное управление съёмными носителями и ключами преобразования.

**Средний список**

* ограничение возможности использования конкретных съемных носителей информации на конкретном АРМ;
* гарантированное исключение утечек информации за счёт применения преобразованных носителей информации;
* удобное централизованное управление съёмными носителями и ключами преобразования;
* первое в России средство контроля съемных машинных носителей информации с поддержкой Windows 10;
* полная интеграция с СЗИ НСД Dallas Lock 8.0;
* расширенный список разрешённых/запрещённых к использованию устройств (все типы подключений, все типы портов и устройств);
* «прозрачное» преобразование съёмных накопителей.

**Длинный список**

* ограничение возможности использования конкретных съемных носителей информации на конкретном АРМ;
* гарантированное исключение утечек информации за счёт применения преобразованных носителей информации;
* удобное централизованное управление съёмными носителями и ключами преобразования;
* первое в России средство контроля съемных машинных носителей информации с поддержкой Windows 10;
* полная интеграция с СЗИ НСД Dallas Lock 8.0 с возможностью полноценного централизованного управления из единой консоли Сервера безопасности Dallas Lock 8.0;
* расширенный список разрешённых/запрещённых к использованию устройств (все типы подключений, все типы портов и устройств);
* «прозрачное» преобразование съёмных накопителей;
* создание с помощью ключа преобразования такого накопителя, с информацией на котором работа возможна только на рабочих станциях, защищенных СЗИ Dallas Lock 8.0 с модулем СКН, при условии наличия и совпадения ключа преобразования.

Ключевые особенности СКН уровня отчуждения (переноса) информации

* преобразование информации «на лету» при чтении и записи. От пользователя не требуется никаких дополнительных действий для работы с преобразованными накопителями — функции преобразования происходят незаметно для пользователя, который привычным образом работает с накопителем через программу «Проводник Windows»;
* защита от утечек информации через внутреннего нарушителя. Ключи преобразования хранятся в защищённой области компьютера и пользователь не может получить к ним доступ. Такой подход практически полностью исключает доступ к информации на накопителях за пределами организации;
* возможность легитимно и безопасно переносить конфиденциальную информацию между АРМ, группами АРМ и доменами безопасности Dallas Lock. Решение соответствует Требованиям ФСТЭК России к СКН уровня отчуждения информации и предназначено для переноса информации ограниченного доступа на сменные накопители.

Информация о сертификации

СКН Dallas Lock уровня подключения съёмных носителей соответствует требованиям ФСТЭК России к СКН уровня подключения:

* для редакции 8.0-К — сертифицировано по классу защиты СКН ИТ.СКН.П4.ПЗ;
* для редакции 8.0-С — сертифицировано по классу защиты СКН ИТ.СКН.П2.ПЗ.

СКН Dallas Lock уровня отчуждения (переноса) информации соответствует требованиям ФСТЭК России:

* для редакции 8.0-К — сертифицировано по классу защиты СКН ИТ.СКН.Н4.ПЗ;
* для редакции 8.0-С — сертифицировано по классу защиты СКН ИТ.СКН.Н2.ПЗ.

Сертификаты ФСТЭК России:

1. Для СЗИ НСД Dallas Loсk 8.0-К — № 2720 от 25 сентября 2012 г.
2. Для СЗИ НСД Dallas Loсk 8.0-С — № 2945 от 16 августа 2013 г.

Цифровую копию сертификата вы можете скачать в личном кабинете на сайте dallaslock.ru или получить по электронной почте, отправив запрос в коммерческий департамент: isc@confident.ru

# Модуль паспортизации

## Графические материалы

Ссылка на графические материалы:

<https://dallaslock.ru/upload/dallasdocs/mp_2021.zip>

Значок продукта



## Информация о продукте

**Краткое название**

МП Dallas Lock

**Полное название**

Модуль паспортизации Dallas Lock

Позиционирование

Программное средство для создания и визирования паспортов программного обеспечения на рабочих местах пользователей.

Описание продукта

Модуль паспортизации программного обеспечения предназначен для создания и визирования паспортов программного обеспечения на рабочих местах пользователей с помощью Сервера конфигураций Dallas Lock. Позволяет администратору информационной безопасности контролировать по требованию или по расписанию список исполняемых файлов на компьютере пользователя.

Ключевые особенности

* возможность формировать Проект паспорта ПО, Паспорт ПО, в том числе по маске с указанием расширений файлов;
* возможность утверждать Паспорт ПО с помощью установки простой электронной подписи;
* возможность проверять соответствие текущего списка ПО пользователя и эталонного списка, хранящегося на Сервере конфигураций Dallas Lock;
* централизованное управление паспортами ПО.

# Модуль Резервного копирования произвольных объектов

## Графические материалы

Ссылка на графические материалы:

<https://dallaslock.ru/upload/dallasdocs/rk_2021.zip>

Значок продукта



## Информация о продукте

**Краткое название**

РК Dallas Lock

**Полное название**

Резервное копирование произвольных объектов Dallas Lock

Позиционирование

Инструмент для автоматизированного восстановления безвозвратно модифицированных или удаленных файлов и каталогов.

Описание продукта

**Малое**

Резервное копирование произвольных объектов (РК) Dallas Lock — это модуль, основной задачей которого является автоматизированное восстановление безвозвратно модифицированных или удаленных файлов и каталогов.

**Среднее**

Резервное копирование произвольных объектов (РК) Dallas Lock — это модуль, основной задачей которого является автоматизированное восстановление безвозвратно модифицированных или удаленных файлов и каталогов.

Позволяет создавать задания на резервное копирование файлов и каталогов, выбирать количество и размещение сохранения резервных копий, определять периодичность и расписание их создания, а также предоставляет возможность восстанавливать защищаемые объекты из резервных копий и удалять резервные копии.

Ключевые особенности

* возможность выбрать количество и размещение сохранения резервных копий;
* возможность определять периодичность и расписание создания резервных копий;
* возможность восстанавливать защищаемые объекты из резервных копий и удалять резервные копии.

Информация о сертификации

Функциональная возможность резервного копирования произвольных объектов реализует следующие базовые меры защиты для 1 уровня/класса защищенности или категории значимости руководящих документов ФСТЭК России:

* ОДТ.4 «Периодическое резервное копирование информации на резервные машинные носители информации»;
* ОДТ.5 «Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала».

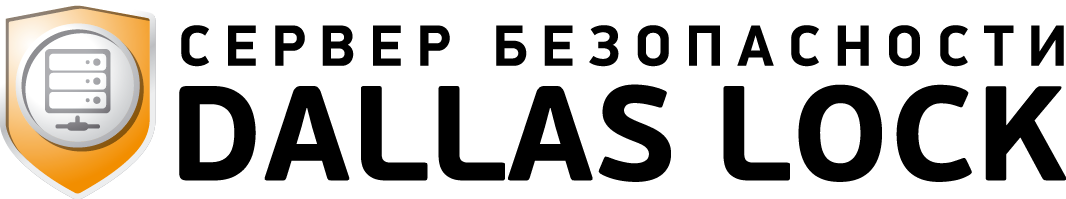
# Сервер безопасности

## Графические материалы

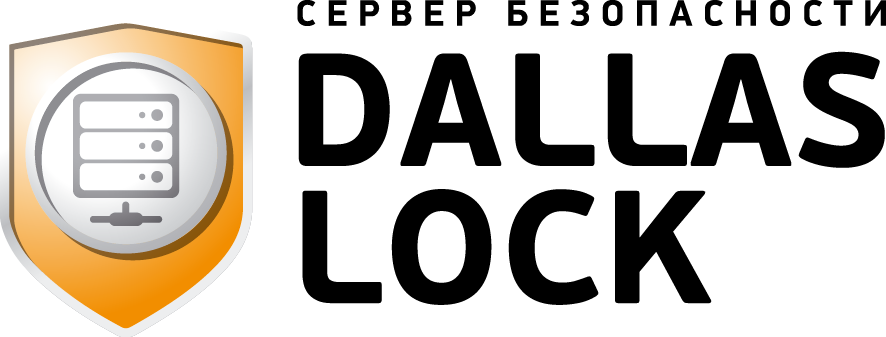
Ссылка на графические материалы:

<https://dallaslock.ru/upload/dallasdocs/sb_dallas_lock.zip>

Значок продукта



Значок продукта (прямоугольник)



## Информация о продукте

**Краткое название**

СБ Dallas Lock

**Полное название**

Сервер безопасности Dallas Lock

Позиционирование

Инструмент, позволяющий объединять защищаемые компьютеры в Домен безопасности для централизованного и оперативного управления.

Описание

**Малое**

Сервер безопасности Dallas Lock — инструмент, позволяющий объединять защищаемые компьютеры в Домен безопасности для централизованного и оперативного управления.

**Среднее**

Сервер безопасности Dallas Lock — инструмент, который устанавливается на отдельный компьютер, защищенный СЗИ НСД Dallas Lock 8.0. Позволяет объединять защищаемые компьютеры в Домен безопасности для централизованного и оперативного управления.

**Большое**

Сервер безопасности Dallas Lock — инструмент, который устанавливается на отдельный компьютер, защищенный СЗИ НСД Dallas Lock 8.0. Позволяет объединять защищаемые компьютеры в Домен безопасности для централизованного и оперативного управления.

Реализован в двух редакциях: «К» (для защиты конфиденциальной информации) и «С» (для защиты конфиденциальной информации, а также для защиты информации, содержащей сведения, составляющие государственную тайну до уровня «совершенно секретно» включительно).

Ключевые особенности

**Короткий список**

* централизованное управления всеми защитными модулями: Dallas Lock 8.0, Dallas Lock Linux, СДЗ Dallas Lock;
* централизованное управление учётными записями и группами пользователей, в том числе тесная интеграция с Active Directory;
* централизованный сбор журналов с клиентских АРМ, визуализация событий и инцидентов в консоли Сервера безопасности.

**Средний список**

* централизованное управления всеми защитными модулями: Dallas Lock 8.0, Dallas Lock Linux, СДЗ Dallas Lock;
* централизованное управление учётными записями и группами пользователей, в том числе тесная интеграция с Active Directory;
* централизованный сбор журналов с клиентских АРМ, визуализация событий и инцидентов в консоли Сервера безопасности;
* централизованное управление политиками безопасности клиентов;
* не требуется ни серверной ОС, ни сторонней СУБД для корректной работы Сервера безопасности Dallas Lock;
* расширенная ролевая модель позволяет разграничить права для администраторов информационной безопасности;
* централизованный сбор журналов с клиентов;
* управление доступом к ресурсам файловой системы и к устройствам на клиентах;
* просмотр состояния отдельных клиентов;
* объединение клиентов в группы;
* оповещение о событиях НСД в рамках Домена безопасности.

**Длинный список**

* централизованное управления всеми защитными модулями: Dallas Lock 8.0, Dallas Lock Linux, СДЗ Dallas Lock;
* централизованное управление учётными записями и группами пользователей, в том числе тесная интеграция с Active Directory;
* централизованный сбор журналов с клиентских АРМ, визуализация событий и инцидентов в консоли Сервера безопасности;
* централизованное управление политиками безопасности клиентов;
* централизованный сбор журналов с клиентов;
* управление доступом к ресурсам файловой системы и к устройствам на клиентах;
* просмотр состояния отдельных клиентов;
* объединение клиентов в группы;
* оповещение о событиях несанкционированного доступа в рамках Домена безопасности.
* сервер безопасности приобретается отдельно и лицензируется по количеству управляемых клиентских рабочих станций. При значительном количестве таких станций затраты на приобретение Сервера безопасности Dallas Lock нивелируются экономией ресурсов администратора безопасности информации;
* если нет связи между Сервером безопасности Dallas Lock и клиентской станцией, то клиент продолжает работать с прежними настройками, в автономном режиме;
* сервер безопасности устанавливается на ОС Windows любой версии, с которой совместим СЗИ НСД Dallas Lock 8.0. Это позволяет сэкономить на приобретении серверной ОС.

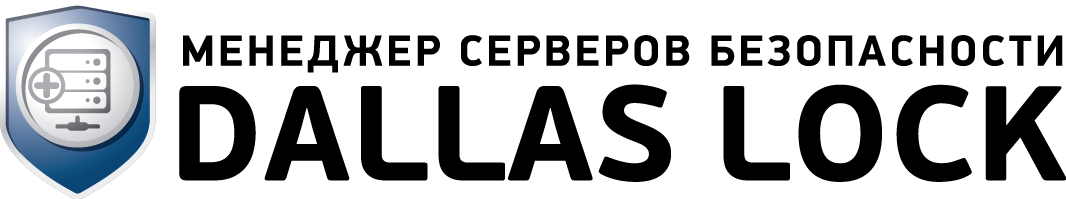
# Менеджер серверов безопасности

## Графические материалы

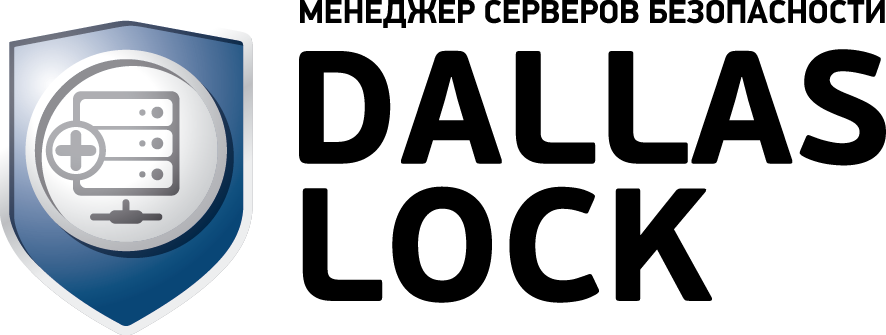
Ссылка на графические материалы:

<https://dallaslock.ru/upload/dallasdocs/manager_server_safety_dallas_lock.zip>

Значок продукта (строка)



Значок продукта (прямоугольник)



## Информация о продукте

**Краткое название**

МСБ Dallas Lock

**Полное название**

Менеджер серверов безопасности Dallas Lock

Позиционирование

Построение отказоустойчивых систем и кластеров безопасности с централизованным управлением на основе Сервера безопасности Dallas Lock.

Описание

**Малое**

Менеджер серверов безопасности Dallas Lock — инструмент, обеспечивает удобное управление несколькими Доменами безопасности в крупных, в том числе распределенных сетях.

**Среднее**

Менеджер серверов безопасности Dallas Lock — инструмент, обеспечивает удобное управление несколькими Доменами безопасности в крупных, в том числе распределенных сетях. Поставляется в комплекте с Сервером безопасности Dallas Lock.

**Большое**

Менеджер серверов безопасности Dallas Lock — инструмент, обеспечивает удобное управление несколькими Доменами безопасности в крупных, в том числе распределенных сетях. Поставляется в комплекте с Сервером безопасности Dallas Lock и устанавливается на отдельный компьютер, защищенный СЗИ НСД Dallas Lock 8.0.

Позволяет создавать трехуровневую модель централизованного управления защитой информации, включив под свое управление несколько Серверов безопасности и, тем самым создав Лес безопасности.

Ключевые особенности

**Короткий список**

* сбор журналов с определенного Домена безопасности, либо со всех Доменов безопасности, входящих в данный Лес безопасности;
* централизованное применение политик безопасности;
* модуль поставляется бесплатно и позволяет реплицировать серверы безопасности, создавая отказоустойчивые кластеры безопасности.

**Средний список**

* сбор журналов с определенного Домена безопасности, либо со всех Доменов безопасности, входящих в данный Лес безопасности;
* централизованное применение политик безопасности;
* подключение к Серверу безопасности для удаленного сетевого или централизованного управления;
* модуль поставляется бесплатно и позволяет реплицировать серверы безопасности, создавая отказоустойчивые кластеры безопасности;
* существенно упрощает управление распределенной инфраструктурой системы защиты Dallas Lock.

**Длинный список**

* сбор журналов с определенного Домена безопасности, либо со всех Доменов безопасности, входящих в данный Лес безопасности;
* централизованное применение политик безопасности;
* подключение к Серверу безопасности для удаленного сетевого или централизованного управления;
* модуль поставляется бесплатно и позволяет реплицировать серверы безопасности, создавая отказоустойчивые кластеры безопасности;
* существенно упрощает управление распределенной инфраструктурой системы защиты Dallas Lock, повышает производительность системы, улучшает защиту благодаря удобному применению групповых политик безопасности.

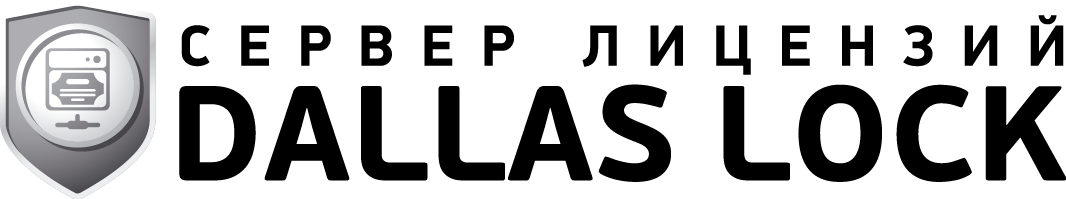
# Сервер лицензий

## Графические материалы

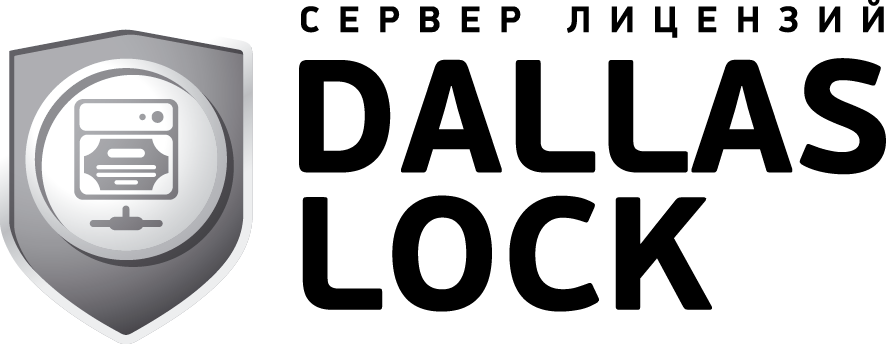
Ссылка на графические материалы:

<https://dallaslock.ru/upload/dallasdocs/sl_dallas_lock.zip>

Значок продукта (строка)



Значок продукта (прямоугольник)



## Информация о продукте

**Краткое название**

СЛ Dallas Lock

**Полное название**

Сервер лицензий Dallas Lock

Позиционирование

Специальное решение для объединения всех имеющихся в компании лицензии на программное обеспечение Dallas Lock в едином пуле, откуда производится их динамическое распределение.

Описание

**Малое**

Сервер лицензий Dallas Lock — специальное решение, объединяющее все имеющиеся в компании лицензии на программное обеспечение Dallas Lock в едином пуле.

**Среднее**

Сервер лицензий Dallas Lock — специальное решение, объединяющее все имеющиеся в компании лицензии на программное обеспечение Dallas Lock в едином пуле, откуда производится их динамическое распределение.

**Большое**

Сервер лицензий Dallas Lock — специальное решение, объединяющее все имеющиеся в компании лицензии на программное обеспечение Dallas Lock в едином пуле, откуда производится их динамическое распределение.

Такая схема работы упрощает управление жизненным циклом лицензий и обеспечивает гибкое перераспределение квот лицензий по каждому домену безопасности без потери гибкости управления информационной безопасностью.

Ключевые особенности

**Короткий список**

* механизм динамического распределения лицензий на терминальные подключения, позволяющий балансировать нагрузку на серверы;
* нет необходимости установки дополнительных драйверов для поддержки аппаратных ключей на Сервер безопасности или терминальный сервер;
* гибкое перераспределение лицензий на централизованное управление для нескольких Серверов безопасности как устанавливаемых отдельно.

**Средний список**

* нет необходимости установки дополнительных драйверов для поддержки аппаратных ключей на Сервер безопасности или терминальный сервер;
* механизм динамического распределения лицензий на терминальные подключения, позволяющий балансировать нагрузку на серверы;
* гибкое перераспределение лицензий на централизованное управление для нескольких Серверов безопасности как устанавливаемых отдельно, так и в одном Домене безопасности в качестве дублирующих друг друга (репликация Серверов безопасности).
* применяя механизмы репликации Серверов безопасности, динамического распределения лицензий Сервером лицензий на базе Домена безопасности (или Леса безопасности) можно построить отказоустойчивый кластер, способный выдерживать высокие нагрузки.

**Длинный список**

* возможность в качестве Сервера безопасности или терминального сервера использовать виртуальные машины под управлением гипервизора Hyper-V (данный гипервизор не поддерживает проброс USB-устройств, можно вынести использование аппаратных ключей на физическую машину с установленным Сервером лицензий);
* нет необходимости установки дополнительных драйверов для поддержки аппаратных ключей на Сервер безопасности или терминальный сервер;
* нет необходимости приобретения и использования нескольких аппаратных ключей, если используется несколько Серверов безопасности и терминальных серверов;
* механизм динамического распределения лицензий на терминальные подключения, позволяющий балансировать нагрузку на серверы;
* гибкое перераспределение лицензий на централизованное управление для нескольких Серверов безопасности как устанавливаемых отдельно, так и в одном Домене безопасности в качестве дублирующих друг друга (репликация Серверов безопасности).
* Сервер лицензий сводит к минимуму трудозатраты на управление лицензиями терминальных подключений, лицензиями в рамках нескольких доменов безопасности.
* применяя механизмы репликации Серверов безопасности, динамического распределения лицензий Сервером лицензий на базе Домена безопасности (или Леса безопасности) можно построить отказоустойчивый кластер, способный выдерживать высокие нагрузки.
* затраты на приобретение Сервера лицензий ниже, чем на закупку нескольких отдельных Серверов безопасности. В дополнение к остальным преимуществам, Сервер лицензий становится лучшим выбором для больших распределенных инфраструктур с неравномерной нагрузкой на серверы и меняющимся количеством клиентов на местах.

# Сервер конфигураций

## Графические материалы

Ссылка на графические материалы:

<https://dallaslock.ru/upload/dallasdocs/server_konfiguraciy.zip>

Значок продукта (строка)



Значок продукта (прямоугольник)



## Информация о продукте

**Краткое название**

СК Dallas Lock

**Полное название**

Сервер конфигураций Dallas Lock

Позиционирование

Сервер конфигураций Dallas Lock позволяет создавать и визировать паспорта программного обеспечения на клиентских АРМ. Позволяет администратору информационной безопасности контролировать по требованию или по расписанию список исполняемых файлов на компьютере пользователя.

Описание продукта

Модуль «Сервер конфигураций Dallas Lock» – программное средство, предназначенное для контроля за изменением состава программного обеспечения и контроля целостности файлов программного обеспечения, установленного на компьютерах и серверах в локальной вычислительной сети, составления Проектов паспортов и утверждения Паспортов программного обеспечения.

Ключевые особенности

* сбор по сети информации о программном обеспечении ПК с установленным СЗИ НСД Dallas Lock 8.0;
* возможность отслеживать изменения в установленном программном обеспечении на клиентах;
* возможность выполнять контроль и фиксацию состояния программной среды;
* возможность формировать Проект паспорта ПО, Паспорт ПО;
* возможность утверждать Паспорт ПО с помощью установки простой электронной подписи;
* возможность создавать и редактировать права учетных записей СК.

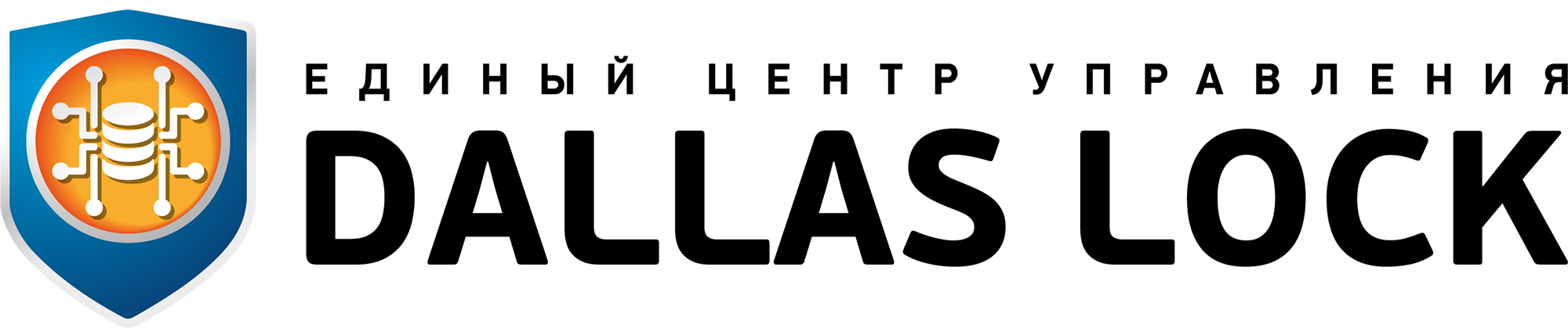
# Единый центр управления

## Графические материалы

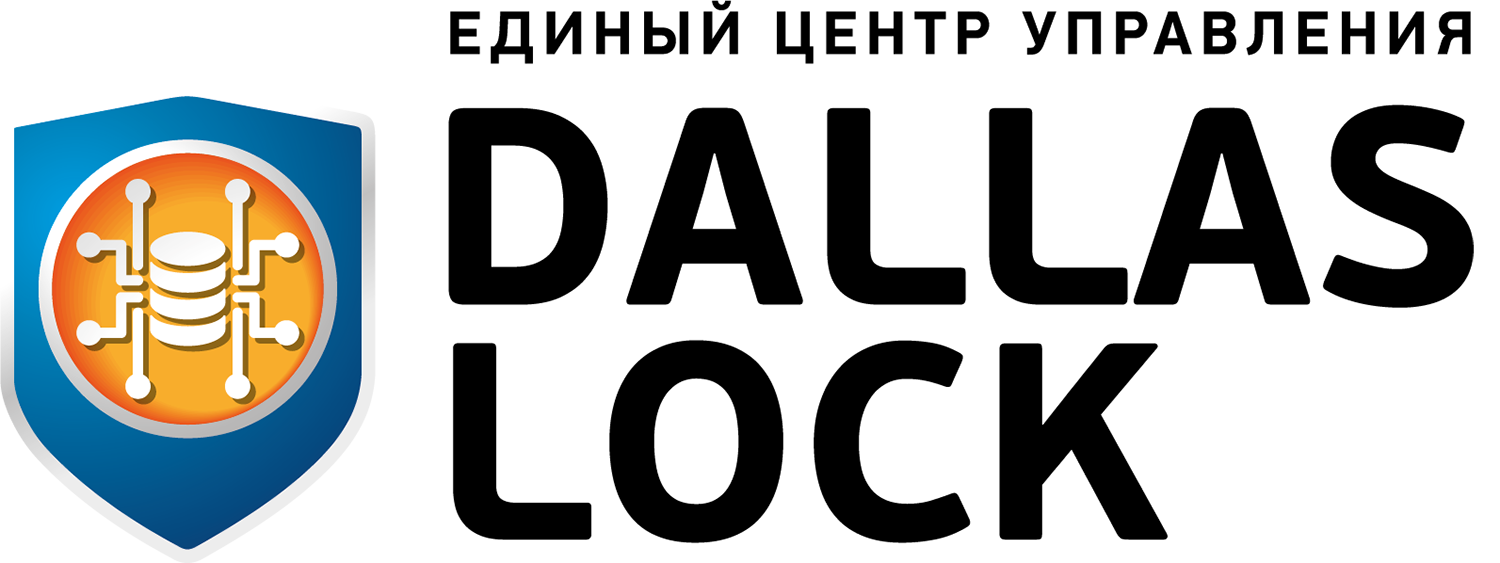
Ссылка на графические материалы:

<https://dallaslock.ru/upload/dallasdocs/ECU_dallas_lock.zip>

Значок продукта (строка)



Значок продукта (прямоугольник)



## Информация о продукте

**Краткое название**

ЕЦУ Dallas Lock

**Полное название**

Единый центр управления Dallas Lock

Позиционирование

Единый кросс-платформенный центр управления, который контролирует безопасность всей ИТ-инфраструктуры организации вне зависимости от её структуры и масштабов и предназначен для контроля целостности настроек активного сетевого оборудования, управления решениями Dallas Lock.

Описание

**Малое**

Единый центр управления Dallas Lock — кросс-платформенный центр управления, контролирующий безопасность всей ИТ-инфраструктуры организации вне зависимости от её структуры и масштабов.

**Среднее**

Единый центр управления Dallas Lock — кросс-платформенный центр управления, контролирующий безопасность всей ИТ-инфраструктуры организации вне зависимости от её структуры и масштабов. Предназначен для контроля целостности настроек активного сетевого оборудования, управления решениями Dallas Lock.

**Большое**

Единый центр управления Dallas Lock — кросс-платформенный центр управления, предназначенный для решения гораздо более широкого круга задач по сравнению с хорошо зарекомендовавшим себя Сервером безопасности Dallas Lock. Контролирует целостность настроек активного сетевого оборудования, решает задачи централизованного управления решениями продуктовой линейки Dallas Lock (СЗИ Dallas Lock 8.0 редакций «К» и «С», СЗИ НСД Dallas Lock Linux, СЗИ ВИ Dallas Lock, СДЗ Dallas Lock и другие продукты компании).

Ключевые особенности

**Короткий список**

* 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;
* позволяет создавать иерархическую структуру доменов безопасности с наследованием значений параметров безопасности. Дерево доменов безопасности может быть сколько угодно большим и сложным. Переключение между настройками каждого домена безопасности происходит интуитивно понятно;
* является кросс-платформенным решением и совместим 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, РЕД ОС 7.3 Муром. Список поддерживаемых ОС постоянно пополняется;
* позволяет управлять СЗИ 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 удалённых компьютерах в сложных сетях.

**Средний список**

* 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;
* позволяет создавать иерархическую структуру доменов безопасности с наследованием значений параметров безопасности. Дерево доменов безопасности может быть сколько угодно большим и сложным. Переключение между настройками каждого домена безопасности происходит интуитивно понятно;
* является кросс-платформенным решением и совместим 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, РЕД ОС 7.3 Муром. Список поддерживаемых ОС постоянно пополняется;
* позволяет управлять СЗИ 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 удалённых компьютерах в сложных сетях;
* репликация функциональности серверов;
* «бесшовная» интеграция с другими решениями продуктовой линейки Dallas Lock;
* настраиваемая система оповещений об инцидентах безопасности;
* управление доступом на основе ролей;

**Длинный список**

* 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;
* позволяет создавать иерархическую структуру доменов безопасности с наследованием значений параметров безопасности. Дерево доменов безопасности может быть сколько угодно большим и сложным. Переключение между настройками каждого домена безопасности происходит интуитивно понятно;
* является кросс-платформенным решением и совместим 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, РЕД ОС 7.3 Муром. Список поддерживаемых ОС постоянно пополняется;
* позволяет управлять СЗИ 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 удалённых компьютерах в сложных сетях;
* репликация функциональности серверов;
* «бесшовная» интеграция с другими решениями продуктовой линейки Dallas Lock;
* настраиваемая система оповещений об инцидентах безопасности;
* управление доступом на основе ролей;
* отображение структуры домена в виде дерева;
* объединение компьютеров в группы для удобства аудита и управления;
* общая графическая панель мониторинга защищенности системы с отображением статистики;
* оповещения об инцидентах безопасности в консоли;
* интеграция списка учетных записей и групп пользователей с Active Directory;
* централизованное отслеживание состояния и целостности объектов домена безопасности;
* ведение централизованного аудита событий домена безопасности;
* удаленное развертывание средств защиты информации на АРМ;
* сигнализация об инцидентах безопасности в домене безопасности;
* квитирование и комментирование записей об инцидентах безопасности в домене безопасности;
* графическое представление информации об инцидентах на разных уровнях иерархии домена безопасности.

Информация о сертификации

Единый центр управления (сборка 211.1) прошел процедуру испытаний ФСТЭК России в составе СЗИ Dallas Lock 8.0 редакций «К» и «С» (сборка 10.5.0.803) и СЗИ НСД Dallas Lock Linux (сборка 3.31.58).

Единый центр управления (сборка 145.1) прошел процедуру испытаний ФСТЭК России в составе СЗИ Dallas Lock 8.0 редакций «К» и «С» (сборка 8.0.761.0) и СЗИ НСД Dallas Lock Linux (сборка 3.25.21).

Единый центр управления (сборка 48) сертифицирован в составе СЗИ от НСД Dallas Lock 8.0 редакции «К» (сборка 710) по линии ФСТЭК России.

Единый центр управления (сборка 48) сертифицирован в составе СДЗ Dallas Lock (сборка 348.1) по линии Минобороны России.

Приказом Минкомсвязи России № 768 от 27.07.2021 г. ЕЦУ Dallas Lock включен в единый реестр российских программ для ЭВМ и БД.

Номер записи реестра — № 11185 от 29.07.2021 г.

Ссылка: <https://reestr.digital.gov.ru/reestr/384672/?sphrase_id=2327134>

Цифровые копии сертификатов вы можете скачать в личном кабинете на сайте dallaslock.ru или получить по электронной почте, отправив запрос в коммерческий департамент: [isc@confident.ru](mailto:isc@confident.ru)

Ссылка на страницу продукта на сайте вендора

ЕЦУ Dallas Lock: <https://dallaslock.ru/products/edinyy-tsentr-upravleniya/>

# Общее описание «О компании» ЦЗИ ООО «Конфидент»

## Графические материалы

Ссылка на графические материалы:

<https://dallaslock.ru/upload/dallasdocs/konfident.zip>

Логотип



## Описание компании

**Малое (до 20 слов)**

Центр защиты информации компании «Конфидент» — российский разработчик линейки сертифицированных средств защиты информации Dallas Lock.

**Среднее (до 35 слов)**

Центр защиты информации компании «Конфидент» — российский разработчик линейки сертифицированных средств защиты информации. Продукты компании применяются для защиты конфиденциальной информации, и сведений, составляющих государственную тайну до уровня «совершенно секретно» включительно.

**Большое (до 70 слов)**

Компания «Конфидент» с 1992 года работает на российском рынке услуг в области информационной безопасности.

Центр защиты информации компании «Конфидент» — российский разработчик линейки сертифицированных средств защиты информации. Продукты компании применяются для защиты конфиденциальной информации, в том числе содержащейся в ГИС и ИСПДн, АСУ ТП, КИИ, и сведений, составляющих государственную тайну до уровня «совершенно секретно» включительно.

Решения компании «Конфидент» регулярно проходят инспекционный контроль, подтверждая надежность и качество новых функциональных возможностей. Они одинаково эффективны для защиты как малых сетей, так и масштабных сетевых инфраструктур.

# Описание «О компании» Группы компаний «Конфидент»

## Графические материалы

Ссылка на графические материалы:

<https://dallaslock.ru/upload/dallasdocs/konfident.zip>

Логотип



## Описание компании

**Малое**

Группа компаний «Конфидент» — одна из первых негосударственных организаций на российском рынке, предложивших услуги в области защиты информации.

**Среднее**

Группа компаний «Конфидент» — одна из первых негосударственных организаций на российском рынке, предложивших услуги в области защиты информации. Она включает в себя Центр защиты информации, ООО «Конфидент-Дистрибуция», ООО «Конфидент-Интеграция», Инженерный центр, Сервисный центр.

**Большое**

Группа компаний «Конфидент» — одна из первых негосударственных организаций на российском рынке, предложивших услуги в области защиты информации.

Сегодня ГК «Конфидент» работает по нескольким направлениям: комплексные проекты по созданию систем информационной безопасности заказчиков (органов государственной власти, бизнеса), разработка сертифицированных средств защиты информации, проектирование и монтаж систем инженерного обеспечения зданий, эксплуатация и техобслуживание инженерных систем.