



СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

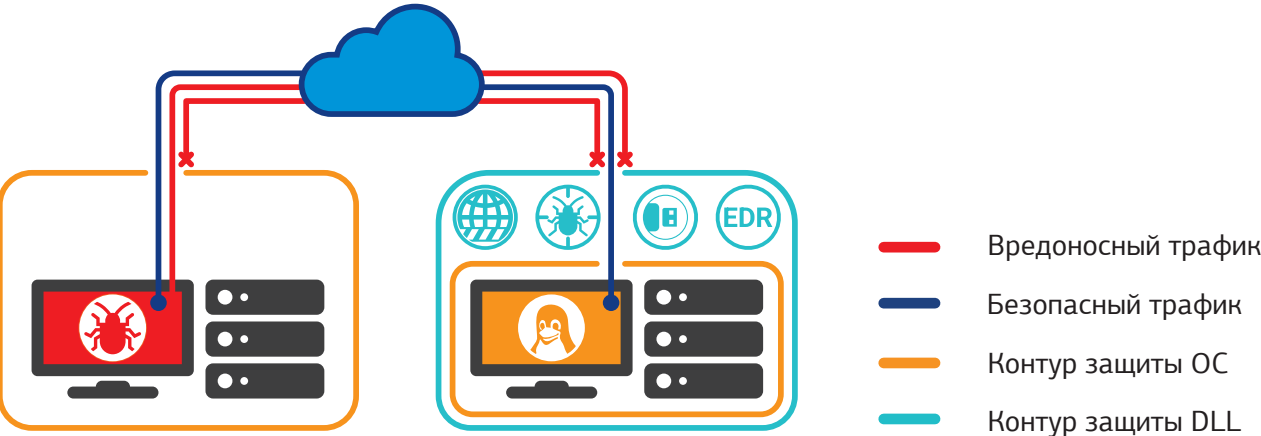
DALLAS LOCK LINUX

**РАСШИРЕНИЕ БЕЗОПАСНОСТИ
ОПЕРАЦИОННЫХ СИСТЕМ**

ОБЗОР



Сертифицированная операционная система (ОС) – обеспечивает фундамент безопасности, однако этого может быть недостаточно для необходимого уровня защиты. Атаки часто нацелены не только на каналы обмена данными, но и на конечные устройства. Требования регуляторов (ФСТЭК России, ЦБ РФ) предполагают комплексный подход к защите информации, который не может быть обеспечен средствами одной только ОС.



Сертифицированная СЗИ Dallas Lock Linux позволит обеспечить безопасность рабочих мест и серверов, дополняя меры защиты, реализованные в ОС, поддерживаемыми модулями:



Сертифицированный межсетевой экран Dallas Lock Linux (МЭ) для контроля сетевого трафика. Позволяет осуществлять контроль информационных потоков, блокировать передачу данных, контролировать приложения через создание черных и белых списков программ, предоставляет возможность индивидуальной и групповой работы с правилами фильтрации через единый интерфейс.



Сертифицированная система обнаружения вторжений Dallas Lock Linux (COB) для выявления атак в реальном времени. Позволяет анализировать сетевой трафик и события системы с применением эвристического анализа, применять гибкие сценарии реагирования на угрозы.



Сертифицированное средство контроля съемных машинных носителей информации Dallas Lock Linux (СКН) позволяет управлять списком разрешенных съемных накопителей, закреплять право подключения накопителей, осуществлять блокировку и разблокировку интерфейсов ввода-вывода, управлять подключением мобильных устройств к компьютеру.



Средство обнаружения и реагирования Dallas Lock Linux (COP) для оперативного выявления и реагирования на сложные атаки. Позволяет выявлять признаки взлома при помощи механизма обнаружения индикаторов компрометации (IoC), автоматически локализовать инциденты.



Централизованное управление при помощи Единого центра управления Dallas Lock (ЕЦУ) доступно для всех модулей Dallas Lock Linux.

СЗИ Dallas Lock Linux поддерживает широкий набор Linux-дистрибутивов, в их числе отечественные сертифицированные ОС:

-  Astra Linux Special Edition
-  Alt Linux 8 СП релиз 10
Рабочая станция, Сервер
-  РЕД ОС
-  МСВСфера АРМ, Сервер
и прочие ОС.

Благодаря технологическому партнерству с разработчиками операционных систем мы регулярно отслеживаем выход новых версий ОС и выпускаем обновления наших продуктов, что обеспечивает поддержку самых актуальных релизов ОС.

ВЫПОЛНЕНИЕ МЕР ЗАЩИТЫ ИНФОРМАЦИИ КОМБИНИРОВАННЫМ РЕШЕНИЕМ: СЕРТИФИЦИРОВАННАЯ ОС + СЗИ DALLAS LOCK LINUX

Сертифицированные ОС реализуют значительную часть мер по защите информации в соответствии с приказами ФСТЭК России, однако ряд мер требует применения дополнительных сертифицированных средств защиты. В таблице представлены меры защиты, выполнение которых обеспечивается только с использованием сертифицированных модулей СЗИ Dallas Lock Linux.

Меры по защите информации в соответствии с Приказами ФСТЭК России № 17, 21, 31, 239	СКН DLL	МЭ DLL	COB DLL
ЗНИ.1 Учет машинных носителей персональных данных (информации)	✓		
ЗНИ.5 Контроль использования интерфейсов ввода (вывода) информации на (съемные) машинные носители персональных данных (информации)	✓		
ЗНИ.7 Контроль подключения (съемных) машинных носителей персональных данных (информации)	✓		
АУД.5 Контроль и анализ сетевого трафика		✓	✓
АУД.7 Мониторинг безопасности		✓	✓
АУД.8 Реагирование на сбои при регистрации событий безопасности		✓	✓
АУД.9 Анализ действий (отдельных) пользователей			✓
COB.1 Обнаружение вторжений			✓
COB.2 Обновление базы решающих правил			✓
ЗИС.7 Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода		✓	
ЗИС.34 Защита от угроз отказа в обслуживании (DOS, DDOS-атак)			✓
ЗИС.35 Управление сетевыми соединениями		✓	
ИНЦ.3 Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами		✓	✓



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

<http://www.confident.ru/>
<http://www.dallaslock.ru/>
e-mail:

isc@confident.ru - коммерческие вопросы
helpdesk@confident.ru - техническая поддержка

Схема проезда:



www.confident.ru



www.dallaslock.ru



Telegram-канал

