



СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

DALLAS LOCK LINUX

СЕРТИФИЦИРОВАННЫЕ МОДУЛИ

СКН, МЭ, СОВ

ОБЗОР



СОДЕРЖАНИЕ

1. О продукте.....

2. Подключаемые модули.....

2.1 Средство контроля подключения съемных носителей информации (СКН)

2.2 Межсетевой экран (МЭ)

2.3 Система обнаружения и предотвращения вторжений (COB)

2.4. Возможности EDR в новом модуле Средство обнаружения и реагирования.....

1

1

2

2

2

3



Размещаемая в данном документе информация предназначена для свободного ознакомления. Центр защиты информации ООО «Конфидент» оставляет за собой право вносить без уведомления любые изменения в данный документ, а также в ПО, которое описано в документе.

1. О ПРОДУКТЕ

Dallas Lock Linux — сертифицированная система защиты информации накладного типа, предназначенная для автономных персональных компьютеров и компьютеров в составе локально-вычислительной сети.

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



Изделие имеет сертификат соответствия ФСТЭК России № 3594 от 4 июля 2016 г. на соответствие:

- 4 уровню доверия. «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»;
- 5 классу защищенности СВТ от НСД. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;
- 4 классу защиты СКН. «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты» ИТ.СКН.П4.ПЗ;
- 4 классу защиты МЭ. «Профиль защиты межсетевых экранов типа «В» четвертого класса защиты» ИТ.МЭ.В4.ПЗ;
- 4 классу защиты СОВ. «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты» ИТ.СОВ.У4.ПЗ.



Сведения о включении в государственные реестры:

- Приказом Минкомсвязи России № 426 от 06.09.2016 г. Dallas Lock Linux включен в единый реестр российских программ для ЭВМ и БД под номером № 1285 от 05.09.2016 г.

2. ПОДКЛЮЧАЕМЫЕ МОДУЛИ

В состав Dallas Lock Linux входят сертифицированные ФСТЭК России функциональные модули:

- Средство контроля подключения съемных носителей информации (ИТ.СКН.П4.ПЗ);
- Межсетевой экран (ИТ.МЭ.В4.ПЗ);
- Система обнаружения и предотвращения вторжений (ИТ.СОВ.У4.ПЗ).



2.1 СЕРТИФИЦИРОВАННОЕ СРЕДСТВО КОНТРОЛЯ ПОДКЛЮЧЕНИЯ СЪЕМНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ (СКН)

Позволяет администратору информационной безопасности:

- Управлять списком разрешенных съемных накопителей для рабочей станции.
- Закреплять право подключения накопителей к компьютеру за определенными пользователями и гибко настраивать права доступа.
- Осуществлять блокировку и разблокировку интерфейсов ввода-вывода.
- Управлять подключением мобильных устройств к компьютеру.

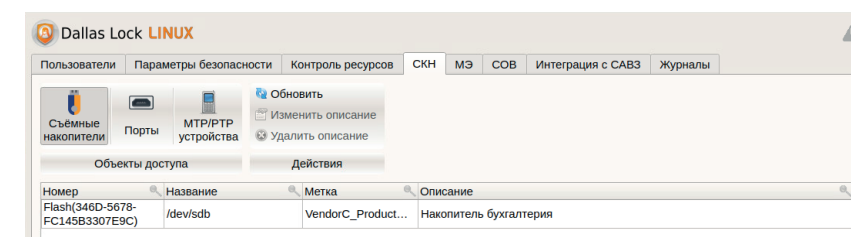


Рисунок 1 – Вкладка СКН в графическом интерфейсе Dallas Lock Linux



2.2 СЕРТИФИЦИРОВАННЫЙ МЕЖСЕТЕВОЙ ЭКРАН (МЭ)

МЭ интегрирован в Dallas Lock Linux и обеспечивает:

- Контроль информационных потоков — фильтрацию, маршрутизацию, контроль соединений и однонаправленную передачу данных.
- Блокировку передачи данных — настройку ограничений по протоколам и защиту от нежелательного трафика.
- Контроль приложений — возможность создания черных и белых списков программ.
- Гибкость настроек — индивидуальную и групповую работу с правилами фильтрации через единый интерфейс.

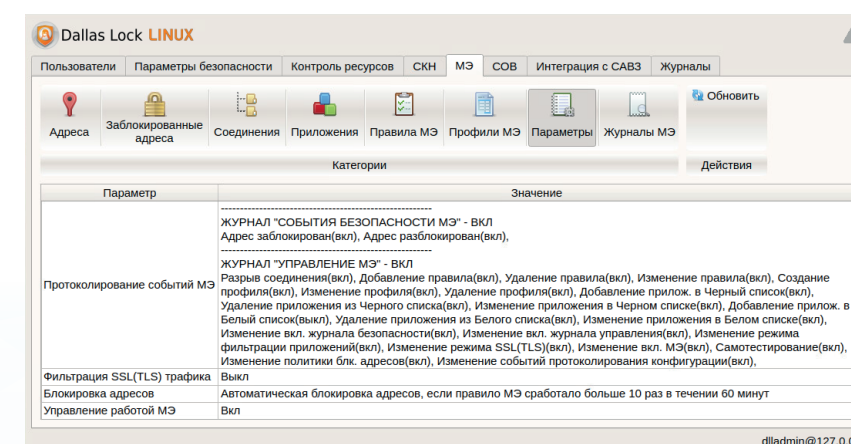


Рисунок 2 – Параметры МЭ в графическом интерфейсе Dallas Lock Linux



2.3 СЕРТИФИЦИРОВАННАЯ СИСТЕМА ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ (СОВ)

Высокая эффективность защиты — интеграция защитных механизмов СОВ в Dallas Lock Linux создает мощный инструмент для противодействия кибератакам, с возможностью централизованного управления через Единый центр управления (ЕЦУ) Dallas Lock.

Анализ сетевого трафика и событий системы — сигнатурный и эвристический анализ сетевого трафика, журналов ОС и приложений позволяет выявлять нештатные ситуации, попытки вторжений и аномалии в поведении пользователей.

Гибкие сценарии реагирования на угрозы — система поддерживает автоматическое реагирование на инциденты, включая блокировку компьютера, ограничение доступа или изоляцию вредоносной активности, обеспечивая проактивную защиту инфраструктуры.



Рисунок 3 – Информация о COB в графическом интерфейсе Dallas Lock Linux

EDR

2.4. ВОЗМОЖНОСТИ EDR В НОВОМ МОДУЛЕ
СРЕДСТВО ОБНАРУЖЕНИЯ И РЕАГИРОВАНИЯ¹

Модуль обеспечивает быструю и своевременную защиту от сложных атак. Помогает находить признаки взлома, анализировать угрозы и автоматически реагировать на инциденты.



- Выявление признаков взлома.**
Механизм обнаружения в системе индикаторов компрометации (IoC) — цифровых артефактов, свидетельствующих о несанкционированном доступе.
- Сканирование системы по запросу, по расписанию или централизованно через ЕЦУ Dallas Lock.
 - Управление базой IoC с возможностью добавления пользовательских индикаторов.
 - Регулярное обновление базы индикаторов.
- Автоматическая локализация инцидента.**
Механизм принятия решений с помощью правил автоматического реагирования.
- Централизованное управление.**
Модуль тесно интегрирован с ЕЦУ Dallas Lock, что обеспечивает настройку и управление из единой Консоли и для всего домена безопасности.

1. Функциональная возможность реализована и уже доступна для бета-тестирования, а также будет включена в следующие сертифицированные версии продуктов.



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

