Защищённый служебный носитель информации

JaCarta SF/ГОСТ

- Доступ к данным на USB-диске возможен только аутентифицированным пользователям и только на авторизованных компьютерах
- Защита от внутреннего, внешнего нарушителей, от администраторов
- Средство для безопасного хранения и переноса информации

Аладдин

Средство контроля отчуждения (переноса) информации со съёмных машинных носителей информации

Назначение

JaCarta SF/ГОСТ предназначен для безопасного хранения и транспортировки информации ограниченного доступа (ДСП, гостайна).

JaCarta SF/ГОСТ состоит из:

- аппаратного средства, выполненного в форм-факторе USB-токена;
- ПО для ввода в эксплуатацию, управления и администрирования.

Решаемые задачи

Безопасное хранение и отчуждение (перенос) информации ограниченного доступа
Доступ к информации может получить только авторизованный пользователь на авторизованном компьютере.

Аудит действий пользователя служебного носителя
В журнале фиксируются операции с ЗМНИ, в т.ч. факты подключения к неавторизованному компьютеру или попытки монтирования скрытых разделов с защищаемой информацией. Доступ к журналу аудита имеется только у администратора.

Предотвращение утечек
Реализуется с помощью комплекса средств JaCarta SF/ГОСТ и Secret Disk LX (сертифицирован Минобороны России и может использоваться в системах, обрабатывающих информацию, относящуюся к гостайне с грифами С/СС). При этом решение ограничивает несанкционированное копирование информации на съёмные машинные носители информации. Например, можно запретить копирование информации с компьютера на все съёмные носители, кроме авторизованных JaCarta SF/ГОСТ.

Защита от подмены компонентов служебного USB-носителя (атаки типа BadUSB)
В JaCarta SF/ГОСТ контролируется целостность компонентов служебного носителя: невозможно несанкционированно осуществить смену карты памяти или встроенного программного обеспечения (прошивки).

Работа с электронной подписью
Устройство JaCarta SF/ГОСТ является персональным средством электронной подписи (ЭП), аппаратно поддерживает как "старые" криптоалгоритмы ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001, выводимые из использования с 2019 г., так и новые — ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012. Устройство может использоваться для хранения ключевых криптоконтейнеров программных СКЗИ (КриптоПро CSP).

Главная цель
Обеспечение защиты информации ограниченного доступа от внутреннего (недобросовестный сотрудник) и внешнего (злоумышленник) нарушителей.

Угрозы "обычных" USB-накопителей

BadUSB — класс хакерских атак, основанных на уязвимости USB-устройств.

Проблема

— недостаточная защищённость прошивки USB-устройств.

Цель атак

— перехват и подмена команд и данных.

Методология

— злоумышленник меняет прошивку USB-устройства, что позволяет внедрить и исполнить вредоносный код.

Перепрошитый микроконтроллер USB-устройства может имитировать клавиатуру, сетевую карту, создать скрытый диск. При этом общепринятые инструменты защиты (виртуализация, антивирусное ПО, DLP-системы и пр.) не обеспечивают должной безопасности, т.к. ограничивают доступ к сменным носителям частично, например, разрешая активацию по "белому списку", или защищают только от одного класса атак, в частности от устройств, имитирующих клавиатуру.

Возникают следующие риски

- USB-устройство может заразить компьютер, а компьютер — все подключаемые USB- устройства и другие компьютеры в сети.
- USB-устройство может иметь скрытые разделы, на которые может быть записана копия перехваченной информации.
- Невозможно выявить нарушения или попытки нарушений — не ведётся журнал аудита.

Согласно "Требованиям по технической защите информации, содержащей сведения, составляющие государственную тайну", утверждённым приказом ФСТЭК России от 20.10.2016 № 025, вступившим в силу 1 декабря 2017 года, необходимо обеспечивать защиту съёмных носителей.

Области применения

В информационных системах, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну до степени секретности СС включительно.

Ключевые особенности продукта

- Архитектура и аппаратный дизайн JaCarta SF/ГОСТ разработаны российской компанией "Аладдин Р.Д.".
- Заказной (ASIC) микроконтроллер на базе процессорного ядра ARM Cortex-M3.
- Secure Element на базе смарт-карточного чипа с сертифицированной российской криптографией, неизвлекаемыми ключами и механизмами защиты от взлома или клонирования
- Загрузка и последующий контроль целостности прошивки встроенного микроконтроллера смарт-карты.
- APDU-Firewall, работа только по "белым спискам" команд.
- Пыле-влагозащищенный корпус, соответствующий стандарту IP57.
- Повышенная защищённость от воздействия электромагнитных излучений и помех.
- Собственная операционная система реального времени для микроконтроллера, позволяющая осуществлять:
  - доверенную загрузку микропрограммного обеспечения (далее МПО);
  - безопасное обновление МПО (подписана ЭП);
  - безопасный обмен с ПО на компьютере (защита команд и данных).
- Производство в России

Особенности поставки

- Возможный объём карты памяти — 16 ГБ или 32 ГБ на заказ.
- При необходимости проводятся спецпроверки (СП) и специсследования (СИ) в испытательной лаборатории, аккредитованной ФСБ России.
- Возможна поставка служебных носителей в пенале со специальным креплением и спецпломбой (контроль неотделимости USB-токена от пенала).

Сертификаты:

- сертификат Минобороны России для работы с гостайной с грифами С/СС;
- сертификат ФСБ России № СФ-124/4641 (КС1, КС2) на используемые в составе изделия средства ЭП и СКЗИ.

Поддерживаемые ОС:

- Microsoft Windows XP SP3, 7 SP1, 8, 8.1, 10;
- Windows Server 2003, 2008, 2008 R2, 2012;
- МСВС 3.0, 5.0;
- Astra Linux 1.2 - 1.6, 8.1;
- Альт 8 СП 64;
- ОС РОСА "Никель";
- ОС "Эльбрус-Д".

Аладдин

+7 (495) 223 00 01
www.aladdin.ru
aladdin@aladdin.ru
129226, Москва, ул. Докукина, 16с1

Аладдин — ведущий российский вендор-разработчик и производитель ключевых компонентов для построения доверенной безопасной ИТ-инфраструктуры

https://t.me/aladdinrd
https://vk.com/aladdinrd

LAP 21/06/2024