Защищенный машинный носитель информации

JaCarta SF/ГОСТ

- Доступ к данным на USB-Защищенный машинный носитель информации возможен только аутентифицированным пользователям и только на авторизованных компьютерах
- Защита от внутреннего, внешнего нарушителей, от администраторов
- Сертификат Минобороны России
- Выполняет требования Профиля ФСТЭК России к средствам отчуждения информации на съёмных носителях

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. Компоненты авторизации входят в комплект программного обеспечения.

Аудит действий пользователя служебного носителя
В журнале фиксируются операции со служебными носителями, в т.ч. факты подключения к неавторизованному компьютеру или попытки монтирования скрытых разделов с защищаемой информацией.

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, выведенные 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.
- USB-накопители могут быть подключены к любому современному средству вычислительной техники.
- 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

JaCarta SF/ГОСТ может использоваться в целях защиты информации в следующих системах

- В информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну до степени секретности СС включительно.
- В государственных информационных системах 3 класса защищённости в случае их взаимодействия с информационно-телекоммуникационными сетями международного информационного обмена, а также в государственных информационных системах 1 и 2 классов защищённости*.
- В информационных системах персональных данных при необходимости обеспечения 3 уровня защищённости персональных данных в случае актуальности угроз 2-го типа или взаимодействия этих систем с информационно-телекоммуникационными сетями международного информационного обмена, а также при необходимости обеспечения 1 и 2 уровня защищённости персональных данных*.
- В информационных системах общего пользования 2 класса*.
- В информационных системах критически важных объектов (КВО) информационно-коммуникационной инфраструктуры*.
- В автоматизированных системах управления технологическими процессами (АСУ ТП)*.

* После завершения сертификации во ФСТЭК России.

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 (сертифицированная российская криптография, неизвлекаемые ключи), подтверждённая неклонируемость и защита от взлома.
- Загрузка и последующий контроль целостности прошивки встроенного микроконтроллера смарт-карты.
- APDU-Firewall, работа только по "белым спискам" команд.
- Пыле-влагозащищенный корпус, соответствующий стандарту IP57.
- Устройство имеет повышенную защищённость от воздействия электромагнитных излучений и помех и соответствует требованиям ГОСТ Р 51318.22-99.
- Собственная операционная система реального времени для микроконтроллера, позволяющая осуществлять:
  - доверенную загрузку;
  - безопасное обновление прошивки микроконтроллера (подписана ЭП устройства);
  - безопасный обмен с ПО на хосте (защита команд и данных).
- Пыле-влагозащищенный корпус, соответствующий России.

Особенности поставки

- Возможный объём карты памяти — 8 ГБ (16 ГБ или 32 ГБ на заказ).
- При необходимости, по требованию заказчика, 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).
- Для предотвращения необнаруживаемого вскрытия корпуса используется специальная голографическая наклейка "СЗИ" со скрытым водяным знаком.

Сертификаты:

- сертификат Минобороны России № 4438 от 30 августа 2019 г. для работы с гостайной с грифами С/СС;
- сертификат ФСБ России № СФ-124/3502 (КС1, КС2) на используемые в составе изделия средства ЭП и СКЗИ.

Поддерживаемые ОС:

- Microsoft Windows 7 SP1, 8, 8.1, 10;
- Astra Linux 1.4, 1.5, 1.6;
- МС ВС 3.0, 5.0.

Аладдин

+7 (495) 223 00 01
aladdin@aladdin.ru
www.aladdin.ru

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.17
Лицензии ФСБ России № 12632Н от 20.12.12, № 30419 от 16.08.17
Лицензия Министерства обороны РФ № 1384 от 22.08.16
Система менеджмента качества компании сертифицирована в Системе добровольной сертификации услуг ГОСТ Р (РОСС RU.0001.03ГУ00) и соответствует требованиям стандарта ГОСТ Р ИСО 9001-2015 (ISO 9001:2015)
Сертификат соответствия - № РОСС RU.ФК14.К00011 от 20.07.18
Система менеджмента качества компании сертифицирована в Системе добровольной сертификации "Военный Регистр" (РОСС RU.И1975.04ГШ02) и соответствует требованиям стандарта ГОСТ Р ИСО 9001-2015 (ISO 9001:2015) и дополнительным требованиям ГОСТ РВ 0015-002-2012
Сертификат соответствия - № ВР 21.1.13537-2019 от 25.04.19