

Операционная система Guardant OS

Guardant OS — это операционная система, поставляемая на специальных носителях.

Данная операционная система содержит функции лицензирования программных продуктов, защиты программного кода при помощи операций шифрования и подписи данных, а также организует управление данными (хранение, чтение, чтение по паролю, обновление, удаление) в памяти специального носителя.

В качестве носителей операционной системы Guardant OS используются [электронные ключи Guardant](#).

Набор функций Guardant OS зависит от модели носителя, на котором операционная система поставляется.

Носитель	Доступные функции Guardant OS
Guardant Sign	• Туннельное шифрование трафика протокола обмена. • Электронная подпись на эллиптических кривых ECC160 • Симметричное шифрование AES-128 и GSI164
Guardant Time	• Все функции Guardant Sign • Возможность ограничения времени работы криптографических алгоритмов для лицензирования защищаемого приложения по времени
Guardant Sign Micro	• Все функции Guardant Sign
Guardant Sign SD	• Все функции Guardant Sign
Guardant Code	• Электронная подпись на эллиптических кривых ECC160 • Симметричное шифрование AES-128 • Загрузка и исполнение до 20 000 строк кода в постоянной памяти Guardant OS • Поддержка Guardant Mobile API
Guardant Stealth II	• Симметричный алгоритм GSI164 с длиной носителя 128 или 256 бит • Алгоритмы шифрования Stealth 1: Autoprotect, Fast, Random
Guardant SD	• Поддержка Guardant Mobile API • Загрузка и исполнение апплетов на Java • Ассиметричное шифрование и подпись RSA • Симметричное шифрование AES-128 • Хэширование на базе SHA-1 и SHA-256

Встроенные механизмы:

- Туннельное шифрование трафика протокола обмена (эта функция вызывается автоматически в фоновом режиме).
- Чтение и запись произвольных бинарных данных в постоянную память по паролю.
- Чтение и запись произвольных данных в постоянную память.
- Запись произвольного программного кода на языке C или Java в постоянную память по паролю.
- Выполнение загруженного программного кода по паролю.
- Возможность обращаться к постоянной памяти из загруженного кода (GCA API).
- Запись и автоматический контроль количества одновременных соединений с внешними системами

Поддержка криптографических алгоритмов с возможностью записывать дескрипторы в постоянную память:

- Электронная подпись на эллиптических кривых ECC160 (генерация подписи и проверка подписи).

- Симметричное шифрование AES-128.
- Симметричное шифрование GSI164.

Возможность устанавливать ограничения на работу криптографических алгоритмов:

- Общее количество использований.
- Продолжительность работы в миллисекундах.
- Дата начала и окончания работы.

Информация, необходимая для эксплуатации программного обеспечения:

[Инструкция по использованию Guardant OS](#)

[Guardant_OS_документация_по_процессам.docx](#)

[Guardant_OS_документация_по_функциям.docx](#)

Для начала работы с Guardant OS необходимо установить Guardant SDK. Утилиты и библиотеки, входящие в состав SDK, позволяют построить защиту разного уровня сложности и стойкости — от защиты программы за несколько минут с помощью Мастера автозащиты до загрузки произвольного кода в ключи Guardant Code. Guardant SDK является основным средством работы с ключами Guardant, поставляемыми в составе Комплекта разработчика.

С помощью инструментов Guardant SDK решается ряд задач, среди которых:

- удаленное обновление ключей, находящихся у конечных пользователей,
- встраивание Guardant API в программы и библиотеки на платформах Windows и Linux,
- автоматическая привязка защищаемого приложения к ключу с помощью Мастера или с помощью ручной настройки любых параметров,
- загрузка и отладка произвольного пользовательского кода в Guardant Code,
- программирование и работа с сетевыми ключами.

Программное обеспечение Guardant постоянно совершенствуется и предоставляет все больше инструментов и новых возможностей. Скачать последнюю версию программного обеспечения и документацию Guardant можно в разделе [Центр загрузки](#).