НОВЫЕ ВОЗМОЖНОСТИ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПРИ ПОМОЩИ ЭЛЕКТРОННЫХ КЛЮЧЕЙ

Иванов Александр Александрович. МИФИ. Каф.41

Электронные ключи защиты

- Защита от копирования
- Шифрование
- Аппаратная защита
- Защита от эмуляции
- Интеграция
- Пользовательские алгоритмы

Guardant Stealth III Sign

- Аппаратная реализация алгоритма электронной цифровой подписи на основе эллиптических кривых (ECC);
- Аппаратная реализация алгоритма симметричного шифрования AES;
- Поддержка всех возможностей Guardant Stealth III:
  - Аппаратные алгоритмы **GSII64, HASH64 и RND64**;
  - Технология защищенных ячеек;
  - Trusted Remote Update (TRU) — безопасное удаленное обновление.
- Защита от анализа на уровне протокола обмена. Во время каждого сеанса происходит взаимная аутентификация между электронным ключом и Guardant API, выработка уникального сеансового ключа на каждой стороне и шифрование всех данных протокола;
- Возможность работать в ОС Windows без установки драйверов, как устройство типа HID (Human Interface Device);
- Поддержка GNU/Linux и Windows CE;
- Высокая скорость работы. За счет оптимизированного протокола обмена и благодаря новой аппаратной платформе Stealth III Sign выполняет основные операции в 10 раз быстрее Stealth III.

Guardant Stealth III Time

- Все новые возможности, реализованные в Stealth III Sign (ECC, HID, шифрование протокола и т.д.);
- Поддержка всех возможностей Guardant Stealth III;
- Часы реального времени RTC (real time clock) и литиевая батарейка со сроком службы около 4-5 лет;
- Возможность ограничения работы аппаратных алгоритмов по RTC (расширенные политики лицензирования по времени):
  - Блокировка аппаратного алгоритма в заданное время;
  - Задание промежутка времени, в течение которого алгоритм будет работоспособен
  - Разблокировка алгоритма в заданное время.
- Возможность ограничения работы защищенных ячеек по RTC;
- Аппаратная защита часов реального времени.