РусКрипто

XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

РусКрипто

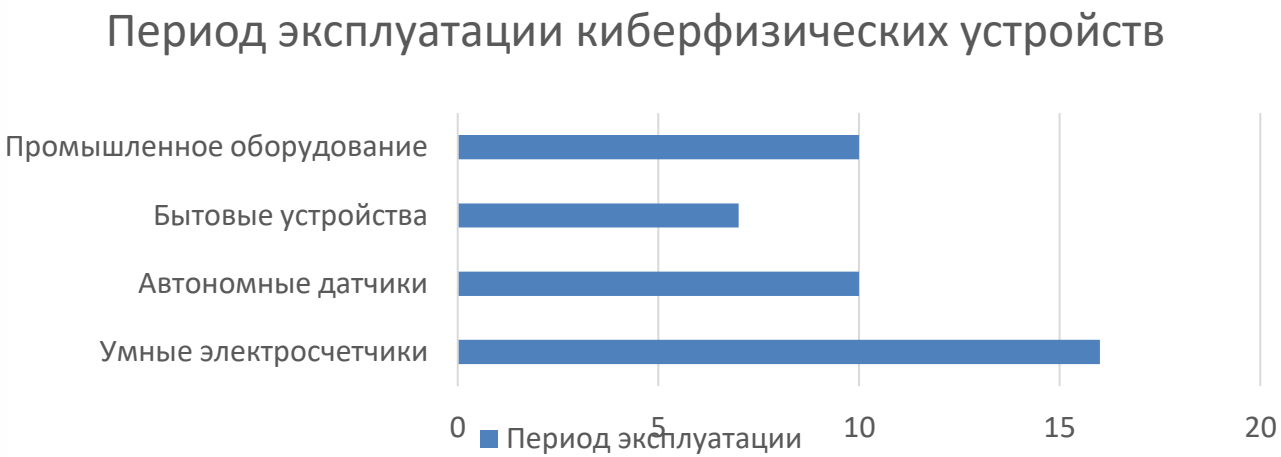
Проблема распределения криптографических ключей в Интернете вещей

К.Я. Мытник

АО «НИИМЭ»

Примеры киберфизических устройств

РусКрипто



Срок действия ключей: 1-3 года

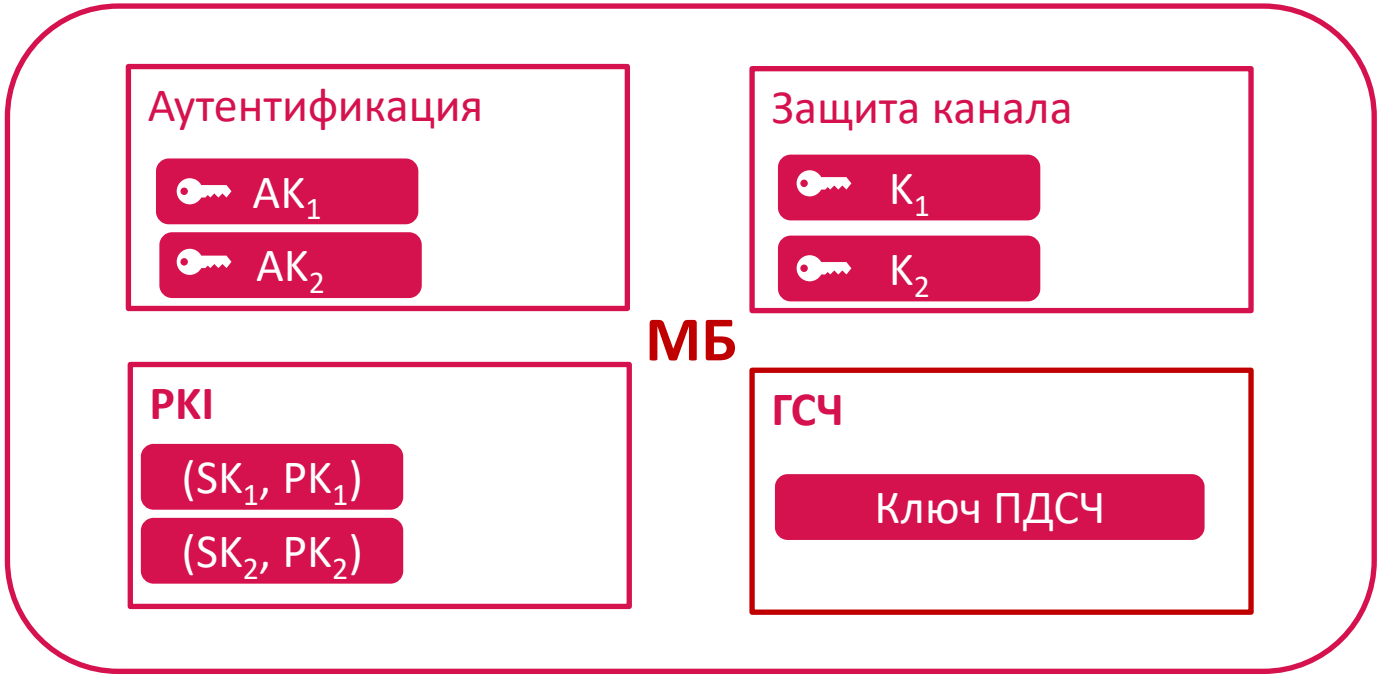
Как обеспечить замену ключей в киберфизических устройствах?

РусКрипто

- Сократить срок жизни устройства до срока действия ключа
- Сделать легкосъемные сменные модули безопасности
- Предусмотреть интерфейс подключения к устройству оборудования для замены ключа внутри модуля безопасности
- Усилить меры защиты в модуле безопасности для увеличения срока действия ключей до времени жизни устройства
- Хранить несколько версий ключей и последовательно вводить их в действие
- Использовать удаленную смену ключей

Ключевая система модуля безопасности киберфизического устройства

РусКрипто



Увеличение срока действия ключей

РусКрипто

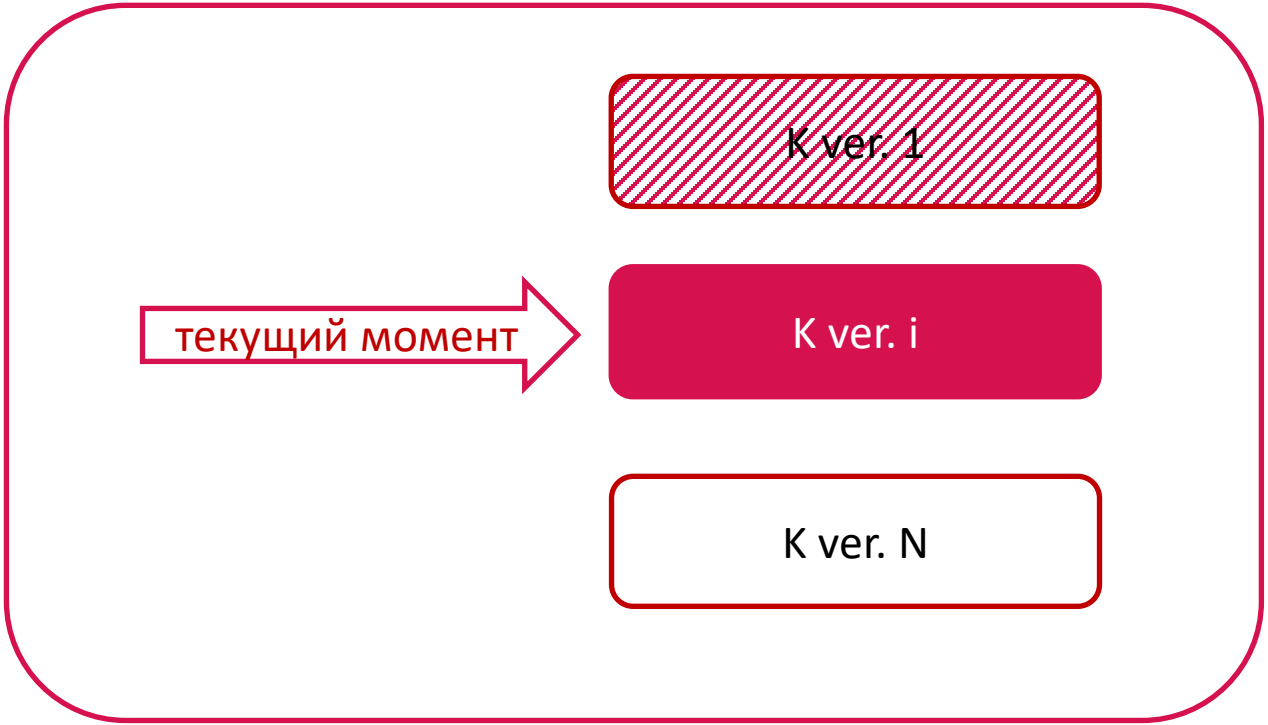
«Требования к СКЗИ, предназначенным для обеспечения некорректируемой регистрации информации»

СКЗИ - НР

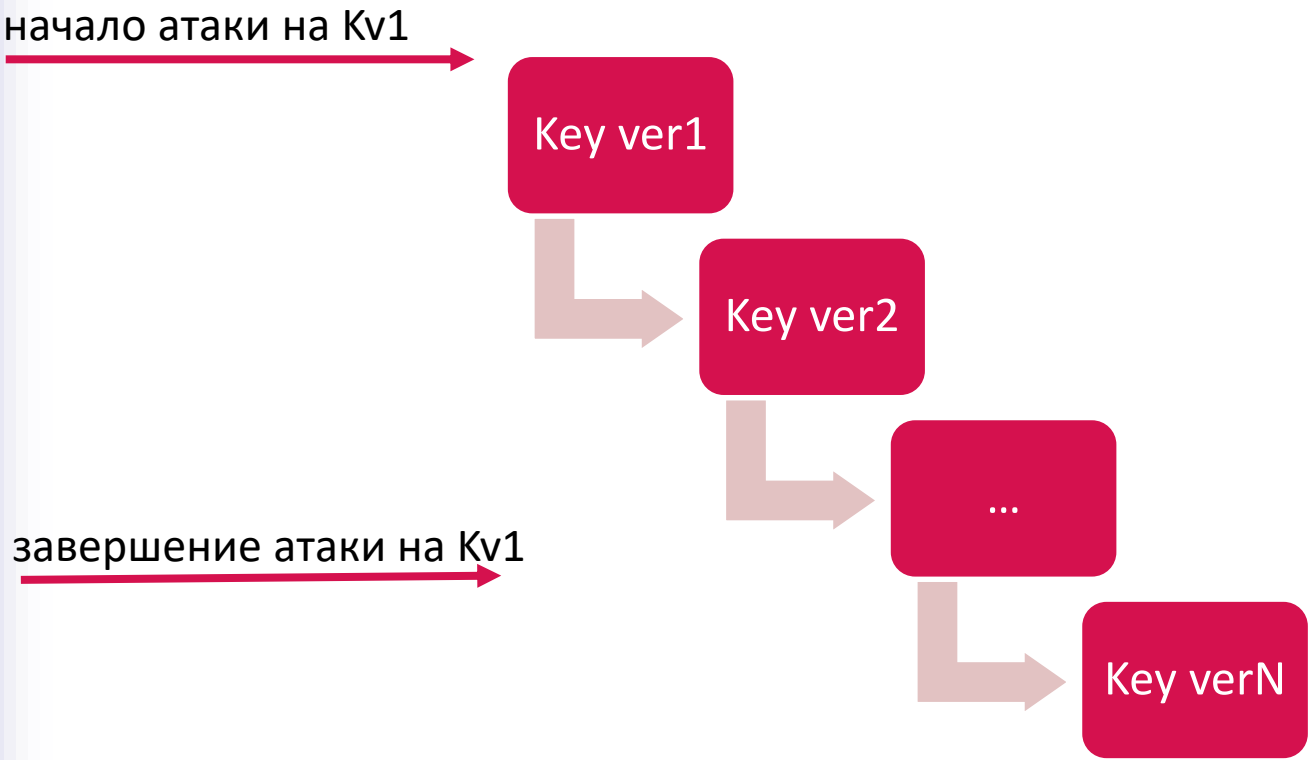
- активный защитный экран …
- система защиты по цепям питания …
- система поиска ошибок …
- датчик света …
- внутренний тактовый генератор с переменной частотой тактирования …
- …

Хранение секретных ключей

РусКрипто



Передача зашифрованных рабочих ключей



РусКрипто

Использование эфемерных ключей обмена

РусКрипто

МБ должен иметь **ФДСЧ** для выработки асимметричных ключей.

МБ и сервер вырабатывают эфемерную пару асимметричных ключей и обмениваются открытыми ключами

Подлинность открытых ключей обеспечиваются имитовставкой, вычисленной на **актуальных** симметричных ключах

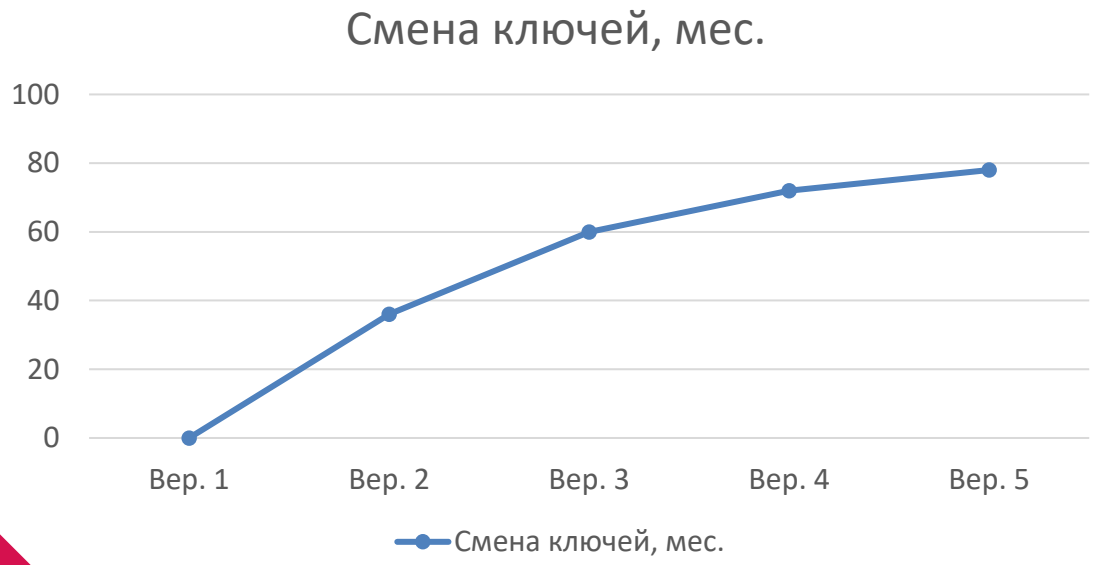
Вырабатывается сессионные ключи обмена по протоколу согласования ключей (VKO) на основе схемы DH (Р 50.1.113-2016).

На ключах обмена сервер формирует крипто-конверт с новыми симметричными ключами и передает его МБ.

МБ меняет ключи и удаляет все временные данные сессии, включая эфемерные ключи.

Потенциальные угрозы

РусКрипто



HDPA

Dual Laser

Ion Beam

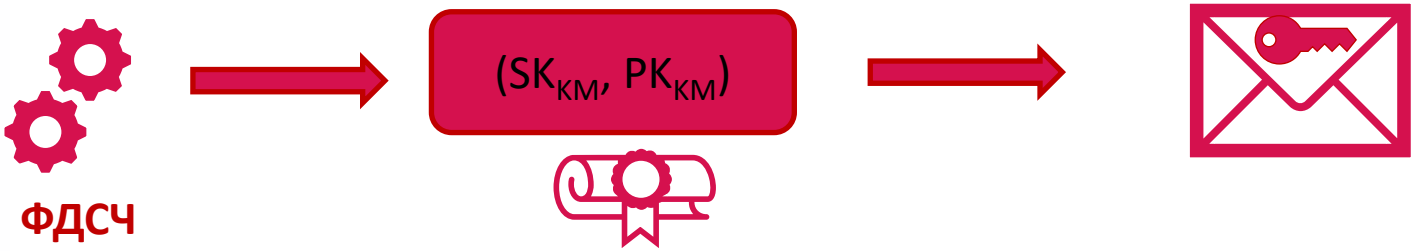
HDEMA

Quantum threat

DFA

Решение НИИМЭ

РусКрипто



РусКрипто

СПАСИБО
ЗА ВНИМАНИЕ