



# РусКрипто

## XXVIII

НАУЧНО-ПРАКТИЧЕСКАЯ  
КОНФЕРЕНЦИЯ

### **Модуль безопасности российского банкомата.**

Евтушенко Владимир. АО "СмартКард-Сервис" Управляющий партнер



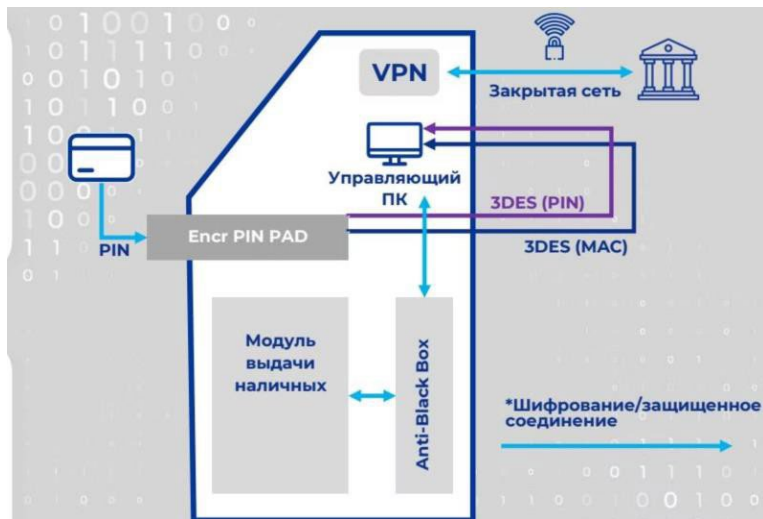
## Сети банкоматов – социальный объект и объект атак

- Инфраструктура кассовых центров, касс предприятий и других традиционных институтов доставки наличных населению по факту заменена на сети банкоматов..
- “Обратный” поток наличных в виде возврата кредитов, платежей и переводов также выполняется в банкоматах. До 50% операций в банкоматах с рециркуляцией наличных составляют операции вноса.
- Своевременное и бесперебойное обслуживание наличного оборота является важной социальной функцией государства, одной из основ общественной стабильности, и, как следствие, – объектом атак.

*\* Исторически Регуляторы в Российской Федерации не регламентировали функционирование сетей самообслуживания банков в аспекте информационной безопасности. Защита сетей осуществлялась на основе **западных стандартов**, и по усмотрению банков-субъектов, с **использованием западных средств защиты информации**.*



## Актуальные методы криптографической защиты в Индустрии.



### 3DES/DEA

Стандарт производителя  
ATM

### 3DES (MD5)

Финансовое сообщение

### VPN

Выбор банка, вне стандарта

### Anti-BlackBox

Стандарт производителя  
ATM

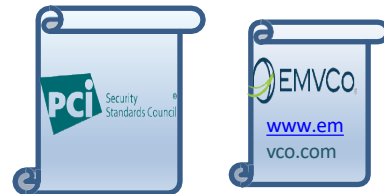
Криптографические подсистемы независимы, в комплексе не стандартизованы, и находятся в компетенции трёх субъектов: производителя ATM/EPP, поставщика VPN и банка-владельца ATM.





## Действующие требования к аппаратным средствам. Алгоритмы шифрования.

- Применяемые алгоритмы: 3DES, RSA 2048/4096, MD5,
- Криптографические процедуры: RKL TR.31, TR.34,
- Требования **МПС** к шифрующим клавиатурам ЕРР: **PCI, EMV L1**.
- Ключевая компонента безопасности – шифрующая клавиатура **Encrypting Pin Pad**.
  - Специальный контроллер для хранения ключей,
  - Требования по физической безопасности: вскрытие, давление, температура...
  - Логическая безопасность: “шум” в канале, “прямой” ввод ключей шифрования,...



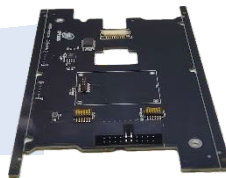
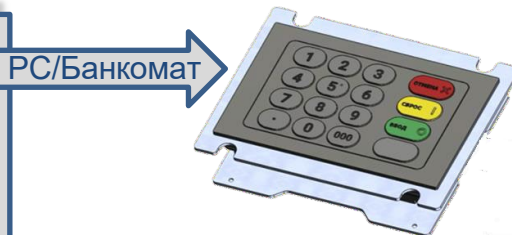
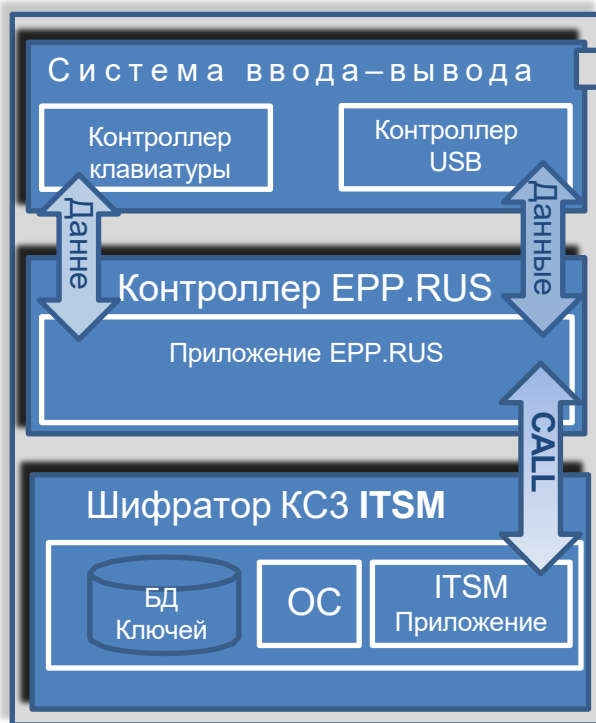


## Почему российская ЕРР нужна ?

- **2022 г.** Западные *поставщики банкоматов* прекратили деятельность в России.
  - ✓ Прекращена поддержка прикладного, системного ПО банкоматов и *шаблонов наличных*.
  - ✓ Закрыта возможность получения Ключей и Сертификатов PKI, и предзагруженных ЕРР-клавиатур.
  - ✓ Затруднены ремонт, диагностика и поставки комплектующих. Исключена возможность загрузки корневых ключей PKI (RKL) – замены ЕРР-клавиатур.
- **2022 г.** EMVCo официально известило о “временном прекращении транзакций” с компаниями РФ.
  - ✓ Закрыта возможность сертификации ПО и оборудования.
  - ✓ Сертификация по “альтернативным каналам” существенно затруднена.
- Обеспечение реальной безопасности финансовых институтов на основе российских процедур сертификации решений на базе отечественных СКЗИ.
- Поддержка Программы импортозамещения Правительства РФ.
- **2030 г.** переход на отечественную криптографию в НСПК МИР.



## Как устроен модуль безопасности EPP.RUS



**Средство криптографической  
защиты информации (СКЗИ)  
«IT SM» версии 1.0, исполнение 2.**

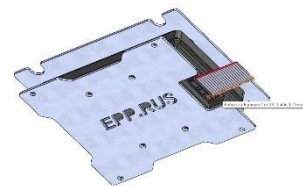
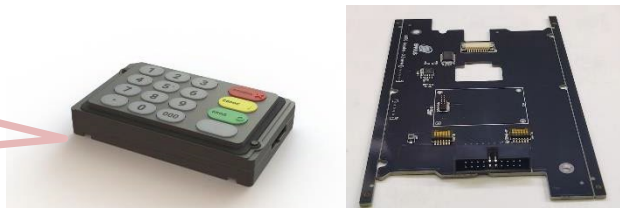
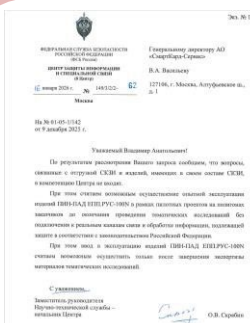




## Сделано в России.

- Разработана схемотехника и технология производства.
- Получен патент на полезную модель RU 240290.
- Изготовлена опытная партия.
- Проводится опытная эксплуатация.

Получено Заключение 8-го Центра ФСБ России по оценке влияния.





# Новая регуляторика в Индустрии платежных карт.

На сайте ЦБ РФ опубликованы:

*Требования к техническим средствам и программному обеспечению, реализующим криптографические механизмы информационной инфраструктуры значимой платежной системы, используемых при осуществлении переводов денежных средств по карточным счетам.*

[https://www.cbr.ru/Content/Document/File/186801/req\\_hardware\\_and\\_software.pdf](https://www.cbr.ru/Content/Document/File/186801/req_hardware_and_software.pdf)

Благодаря усилиям ЦБ РФ, сформулированы “Требования к техническим средствам...” Индустрия ожидает, что произведенные в России устройства – модули и компоненты безопасности, - соответствующие Требованиям, будут разрешены к использованию в НСПК и рекомендованы банкам для применения. До 2030-го года это создаст технические предпосылки к полному переходу в Индустрии на российскую криптографию.





# Спасибо за внимание!

**Евтушенко Владимир**

АО “СмартКард-Сервис”, Управляющий партнер

[evtushenko@scserv.ru](mailto:evtushenko@scserv.ru) +7(981)017 6709