



## III Межбанковская конференция ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВ

# Нормативное обеспечение применения ЭЦП в банковской сфере

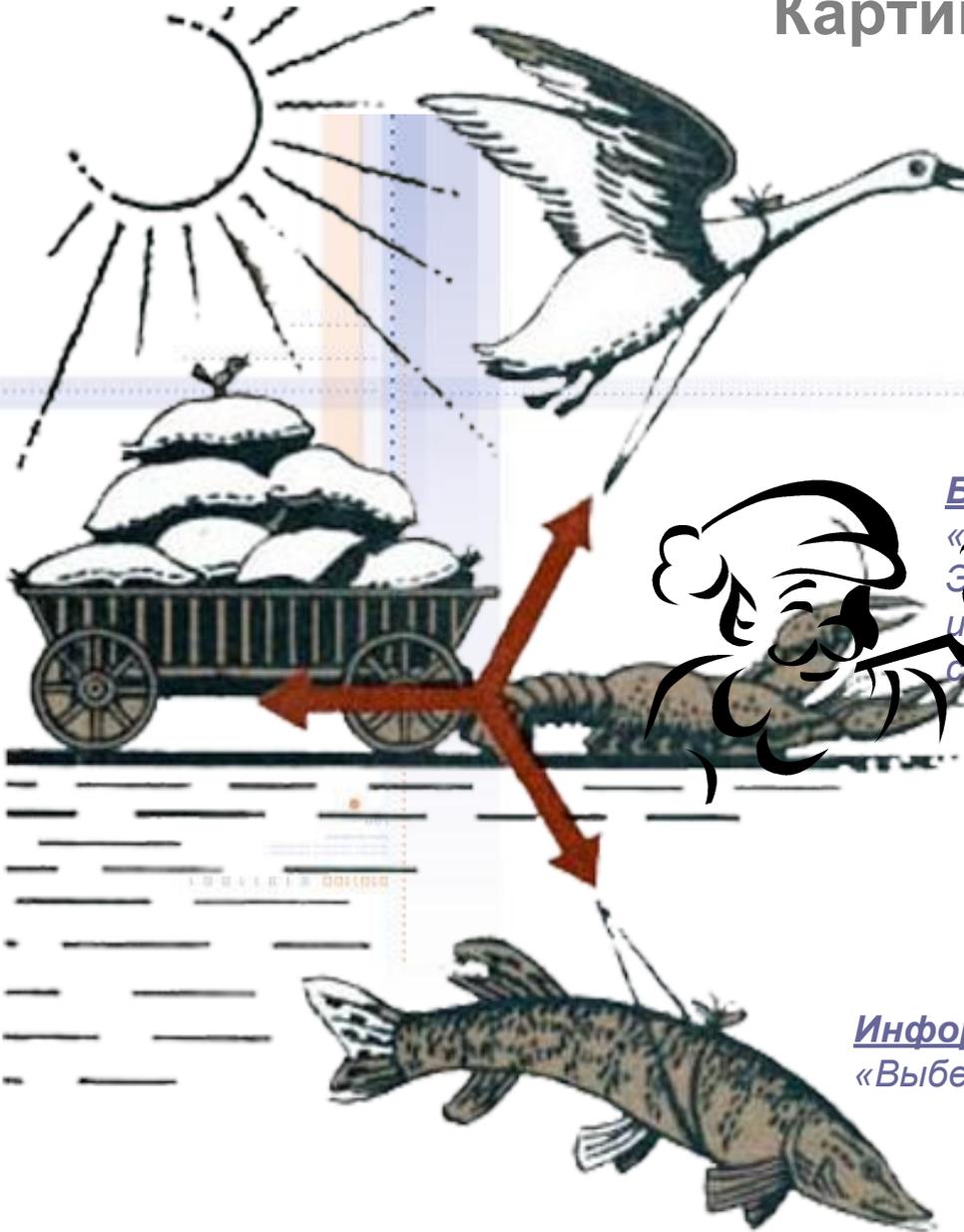
Маслов Юрий Геннадьевич

Коммерческий директор  
ООО «КРИПТО-ПРО»  
Эксперт НП «РОСЭУ»

КОМПАНИЯ КРИПТО-ПРО  
ключевое слово в защите информации

[www.cryptopro.ru](http://www.cryptopro.ru)

# Картина маслом



## Бизнес:

«В кратчайшие сроки и с меньшими затратами внедрим информационную систему!»

## Безопасность:

«Надо разобраться как применяется ЭЦП и обеспечивается защита информации в информационной системе...»

## Юристы:

«А мы не в теме...»

## Информатизаторы:

«Выберем готовую систему и внедрим!»

**КОМПАНИЯ КРИПТО-ПРО**  
ключевое слово в защите информации

[www.cryptopro.ru](http://www.cryptopro.ru)

# Общая схема реалии бытия:

Разработчик разрабатывает систему исходя из собственного понимания, как надо применять ЭЦП, средства ЭЦП и шифрования в этой системе



Банк получает от разработчика систему «в коробке»



Банк внедряет систему «из коробки»



Банк получает не оцененные и неуправляемые риски, связанные с применением ЭЦП

# Реалии бытия:

## Псевдо ЭЦП

Разработаны и достаточно широко используются банковские системы, в которых декларируется применение ЭЦП, но не в соответствии с 1-ФЗ «Об ЭЦП»

Цитата из примера договора:

Клиент при подписании электронного документа (ЭД) ЭЦП применяет свои секретные ключи подписи, а Банк при проверке ЭЦП ЭД — открытые ключи подписи Клиента, являющиеся действующими на момент подписания и передачи документа на обработку соответственно. Ключи электронной цифровой подписи (секретный и соответствующий ему открытый ключ) подписывающей Стороны становятся действующими только после завершения процедур регистрации открытых ключей и ввода в действие секретных ключей.

Риски банков применения псевдо ЭЦП не оценены. Ущерб от реализации данных рисков не минимизирован.

# Реалии бытия:

## Некорректные процедуры работы с ЭЦП

Во многих банковских системах:

- По умолчанию отключена проверка на отозванность сертификата ключа подписи при проверке ЭЦП;
- Отсутствуют проверки на отозванность сертификата ключа подписи при создании ЭЦП

Появляются риски банков и пользователей, связанных с исполнением документов, удостоверенных ЭЦП с отозванными (аннулированными) сертификатами

# Реалии бытия:

## Декларирование применения сертифицированных средств ЭЦП (СКЗИ)

- Применение сертифицированных библиотек или модулей на смарт-картах, предназначенных для создания СКЗИ;
- Передача средств ЭЦП по незащищенным каналам связи или по протоколам SSL с алгоритмами RSA, DES и т.д.

Появляются риски банков и пользователей, связанных с отказом от ЭЦП ввиду подтверждения экспертной организации о несертифицированном условии использования средства ЭЦП

# Реалии бытия:

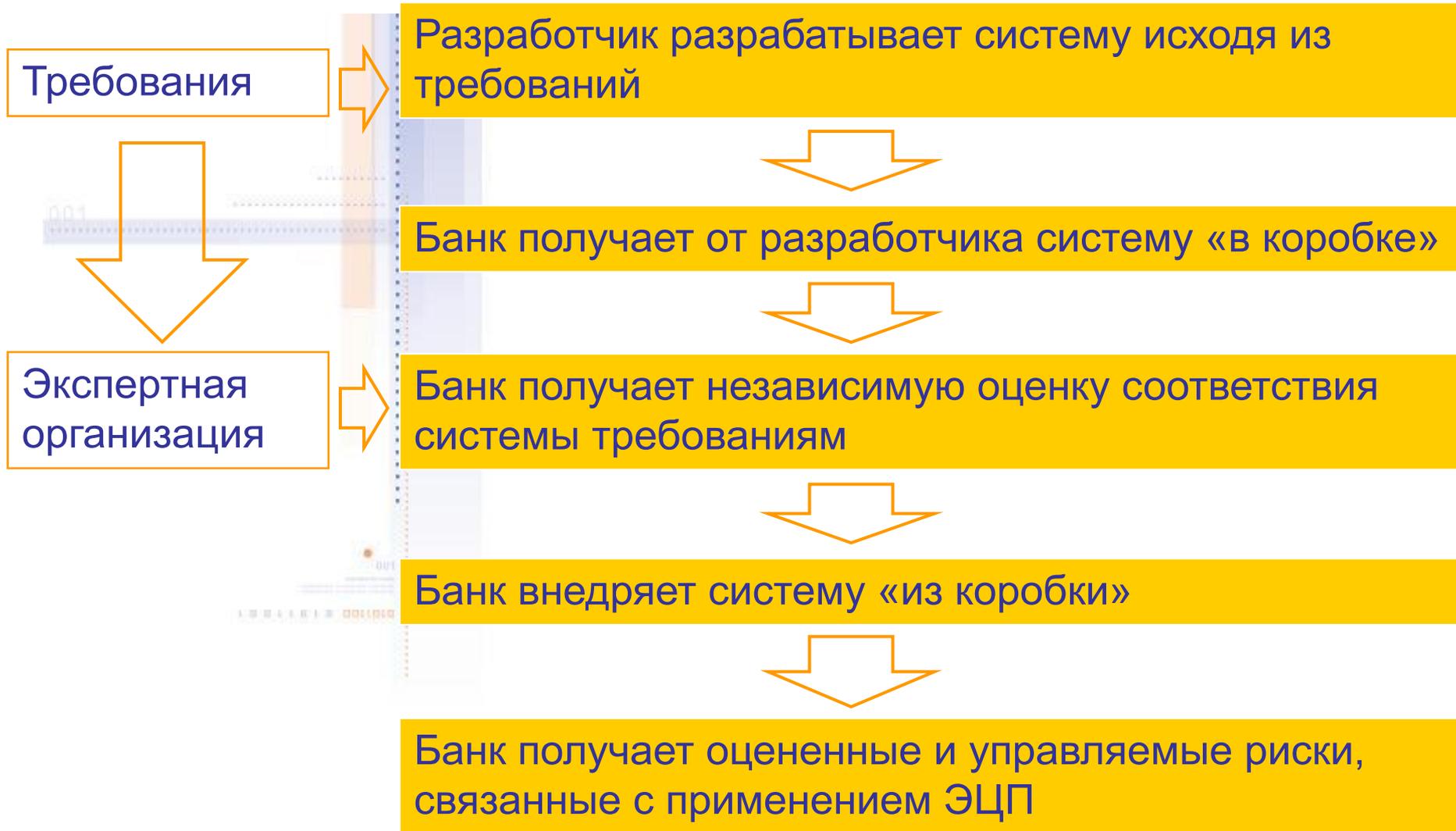
## Реальный уровень защиты ключей

- Применяются незащищённые ключевые носители (дискеты, флэшки), т.к. они по определению дешевле защищённых;
- Цитата из договора, описывающая ВСЕ меры защиты ключей:  
КЛИЕНТ обязан самостоятельно обеспечить сохранность своих секретных ключей и несет за это полную ответственность. КЛИЕНТ по возможности обязан содержать свои секретные ключи на съёмном электронном носителе информации, а данный носитель хранить в сейфовом шкафу или другом надёжном месте с ограниченным доступом.
- Отсутствуют понятные и выполнимые меры по обращению с ключами в конкретной системе
- Отсутствуют требования к среде функционирования средства ЭЦП в конкретной системе (особенно в части защиты от вирусов) и меры по контролю этой среды

Не говорим об уровне криптографической защиты системы!

Появляются риски банков и пользователей, связанных с действием третьих лиц

# Взгляд на идеальное бытие:



# Требования: о чём и в каком виде

## Общие положения о применении ЭЦП

Устанавливает единые нормы при взаимоотношениях лиц по исполнению или принятию к сведению документов, оформленных в виде электронного документа с ЭЦП:

- условия действительности ЭД, удостоверенного ЭЦП (детализированные условия равнозначности ЭЦП, условия действительности СКП участника системы, СКП уполномоченного лица)
- условия действительности ключей подписи
- общий порядок разрешения споров/конфликтов, связанных с применением ЭЦП.

Позволил бы защитить интересы как банков, так и клиентов банка в части исполнения электронных документов, удостоверенных ЭЦП.

Варианты оформления:

- Постановление Правительства РФ
- Приказ уполномоченного федерального органа власти с регистрацией в Минюсте
- Стандарт СРО

# Требования: о чём и в каком виде

## Технический регламент по применению ЭЦП

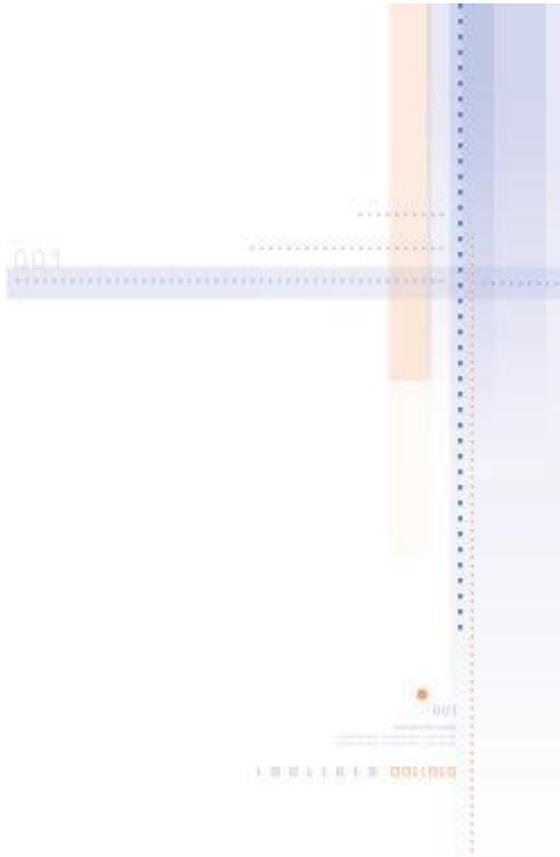
Устанавливает единые процедурные правила применения ЭЦП в части:

- применения средств ЭЦП (требований к ним и условий применения)
- распространения средств ЭЦП и обращения с ними
- формирования и проверки ЭЦП
- форматов ЭЦП
- определение статуса сертификата ключа подписи
- обращения с ключами ЭЦП
- описания реакции системы на состояния с ЭЦП и сертификатами
- содержания документации системы и особенно в пользовательской части.

Позволил бы обеспечить разработчиков банковских систем необходимыми нормативными документами для создания соответствующих комплексов, существенно снижающих риски применения ЭЦП и шифрования.

Варианты оформления:

- Приказ уполномоченного федерального органа власти с регистрацией в Минюсте
- ГОСТ
- Стандарт СРО



# ВОПРОСЫ?

Маслов Юрий  
[maslov@cryptopro.ru](mailto:maslov@cryptopro.ru)

КОМПАНИЯ КРИПТО-ПРО  
ключевое слово в защите информации

[www.cryptopro.ru](http://www.cryptopro.ru)