КРИПТОПРО

Ключевое слово
в защите информации

Эволюция технологии средств электронной подписи и способов её применения

конференция РусКрипто

Маслов
Юрий Геннадьевич
Коммерческий директор, эксперт РОСЭУ

Хронотоп развития технологий применения электронной подписи в России

Доисторический период

до принятия 1-ФЗ «Об ЭЦП» в 2001 году

начало 90-х

2001

Исторический период

до принятия 63-ФЗ «Об ЭП» в 2011 году

2011

Новая история

до вступления в силу норм 476-ФЗ, внёсшего поправки в 63-ФЗ «Об ЭП»

2021

Новейшая история

настоящее время

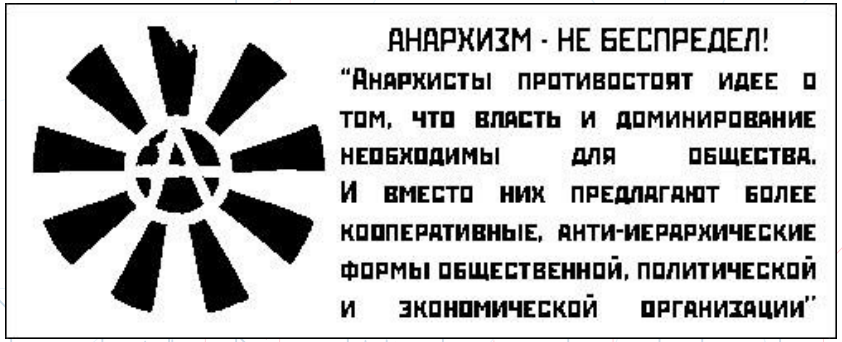
Эра анархии и раздробленности. Эра поисков и кристаллизации идей

Особенности эпохи:

- Несовместимость средств ЭП и форматов ЭП. Как следствие, разобщённость систем ЭДО
- Засилье реализаций иностранных криптоалгоритмов и местечковых криптоалгоритмов, отличных от ГОСТ
- Эпоха дискет и таблеток Touch Memory

Правовые основы:

- Лицензирование деятельности разработчиков
- Необязательная система сертификации
- Корпоративные регламенты и соглашения



Технология локальной подписи:

- создание ЭП производится непосредственно в памяти вычислительного устройства пользователя с использованием ключа создания ЭП, хранящегося у пользователя
- Средство ЭП реализовано в форме статических и динамических библиотек
- Использование предустановленных в MS Windows криптопровайдеров, реализующих импортные криптоалгоритмы

Технология серверной подписи:

- создание ЭП производится на сервере, где осуществляется хранение ключей создания ЭП пользователей и доступ к ним

Эра развития PKI в России с ГОСТом. Эра начала безбумажных технологий.

Особенности эпохи:

- Эра отечественных криптопровайдеров и совместимости СКЗИ
- Вытеснение иностранных криптоалгоритмов и местечковых криптоалгоритмов
- Эпоха защищённых носителей ключей – токенов
- Появление удостоверяющих центров

Правовые основы:

- Федеральный закон 1-ФЗ «Об ЭЦП»

Технологии локальной подписи:

- создание ЭП производится непосредственно в памяти вычислительного устройства пользователя с использованием ключа создания ЭП, хранящегося у пользователя
- Популярность приобретают СКЗИ в форме криптопровайдеров
- Совместимость применения ЭП между ЭДО за счёт использования одного криптопровайдера

Технологии серверной подписи :

- создание ЭП производится на терминальном сервере с удалённым RDP-доступом, с «пробросом» USB-токена

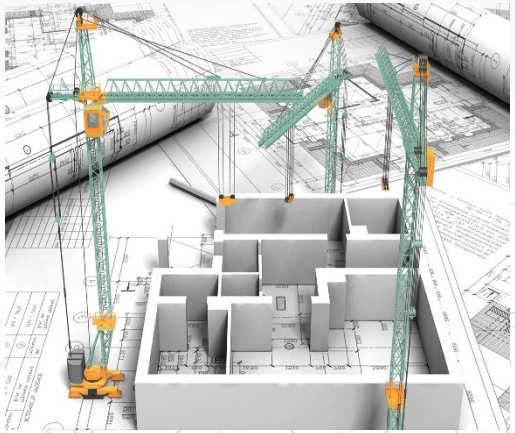
Эра становления рынка применения ЭП

Особенности эпохи:

- Девиз эпохи: удобнее, дешевле, технологичней
- Государство начало регулировать рынок
- Появление значительного числа сервисов с применением ЭП
- Бум развития ЭДО
- Ориентация на применение УКЭП

Правовые основы:

- Федеральный закон 63-ФЗ «Об ЭП»
- Обязательная система сертификации для применении УКЭП
- Система аккредитации удостоверяющих центров



Технологии локальной подписи:

- Появление функциональных ключевых носителей

Технологии удалённой (дистанционной) подписи:

- создание ЭП производится в специализированной информационной системы, где обеспечивается надёжное хранение ключей создания ЭП пользователей и строгая аутентификация этих пользователей

Технологии мобильной подписи подписи :

- создание ЭП производится на мобильном устройстве пользователя с использованием ключа создания ЭП, хранящегося в памяти мобильного устройства или на съёмном носителе

Государство вошло в рынок

Особенности эпохи:

- Изменение акцентов в применении ЭП (МЧД)
- Активное вмешательство государственных органов в структуру функционирования рынка деятельности удостоверяющих центров
- Государство стало демпинговым участником рынка применения ЭП

Правовые основы:

- Федеральный закон 63-ФЗ «Об ЭП» в новых редакциях
- Изменение системы аккредитации удостоверяющих центров
- Принятие локальных НПА, фиксирующие превалирование госсервисов

Технологии локальной подписи:

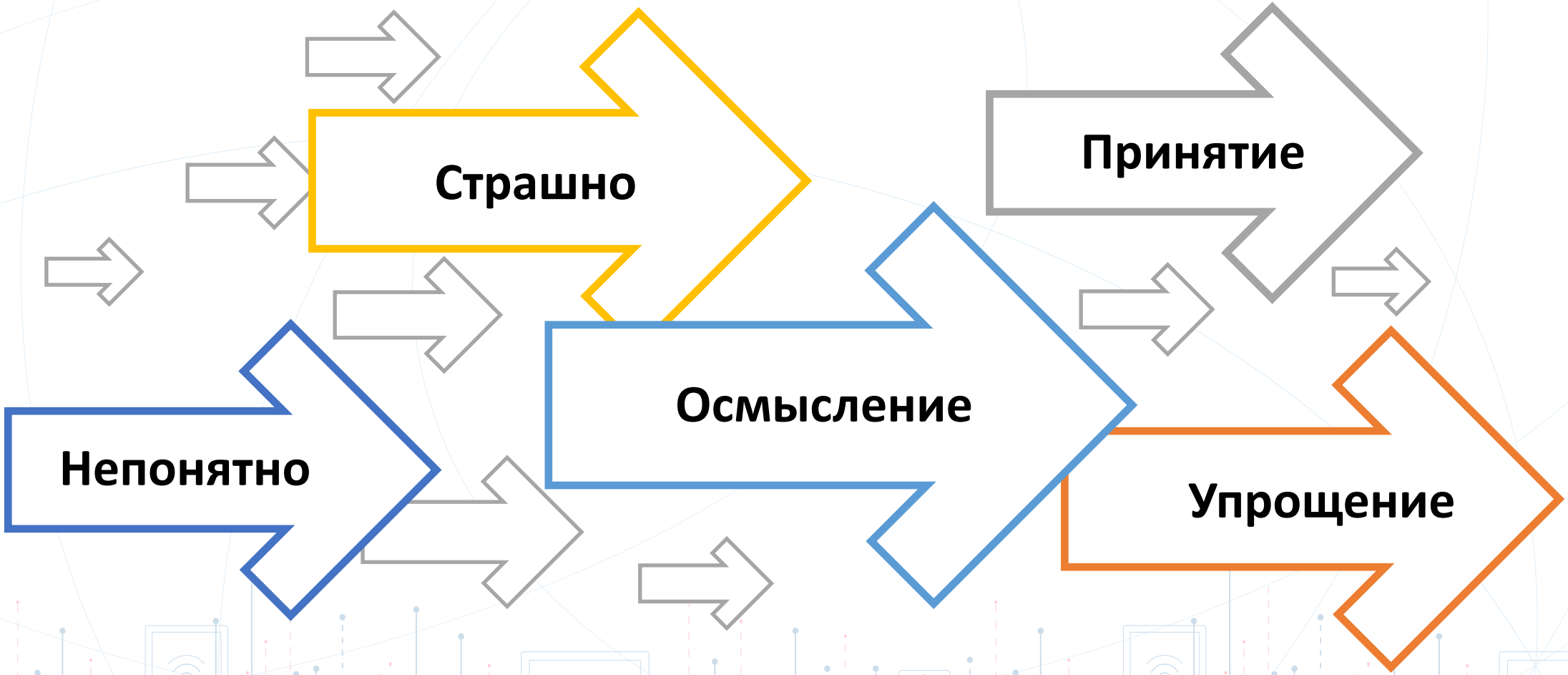
- Появление функциональных ключевых носителей

Технологии распределённой подписи:

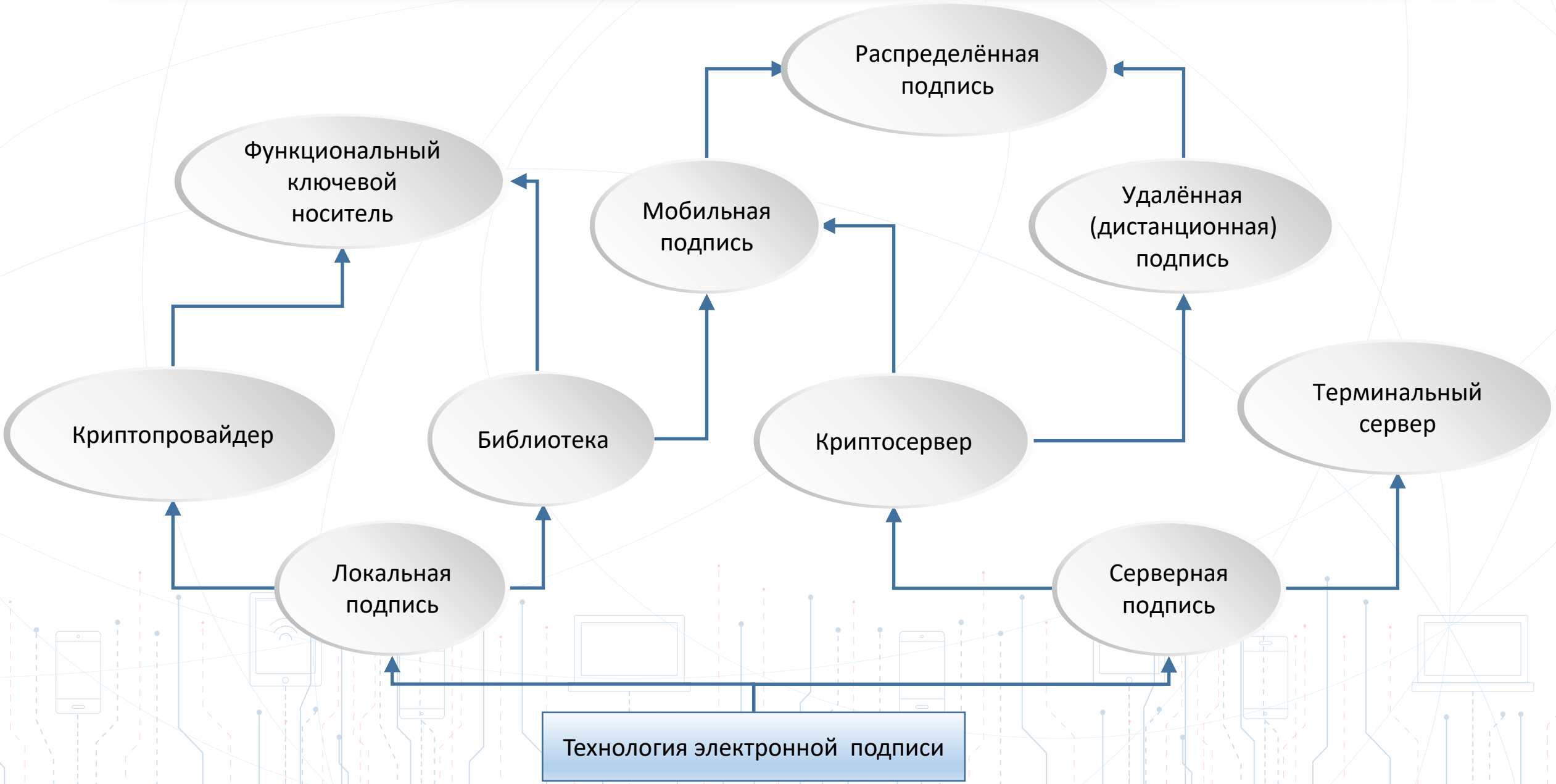
- создание ЭП производится в специализированной информационной системе
- разделение ключа создания ЭП пользователя и распределение компонент ключа по вычислительным устройствам
- ключ подписи никогда не собирается на одном устройстве

Технологии мобильной подписи подписи :

- создание ЭП производится на мобильном устройстве пользователя с использованием ключа создания ЭП, хранящегося в памяти мобильного устройства или на съёмном носителе


Страшно
Принятие
Непонятно
Осмысление
Упрощение

Эволюция технологий электронной подписи



Оценка с точки зрения пользователей

Почти всегда самостоятельно не могу установить и настроить. Так же огорчает, что нужно постоянно помнить про правила обращения с токенами и обеспечивать их доступность в нужный момент

Оценка с точки зрения ИБ

Радует, что риски, связанные с конфиденциальностью ключей, на стороне пользователей

Оценка с точки зрения оператора ЭДО и ИТ

Сложно с этими электронными подписями, ибо нужно как-то автоматизировать и упростить пользователям работу со средствами ЭП

Оценка с точки зрения пользователей

Привычная работа в смартфоне, но непривычно обращаться со смартфоном как с ключевым носителем. И это быстро забывается.

Оценка с точки зрения ИБ

Радует, что риски, связанные с конфиденциальностью ключей создания ЭП, всё там же, на стороне пользователей

Оценка с точки зрения Оператора ЭДО и ИТ

Удобно работать с такими подписями: интегрировался на стороне сервера ЭДО, а всё остальное уже средствами системы мобильной подписи

Оценка с точки зрения пользователей

Привычная работа в смартфоне, что не может не радовать

Оценка с точки зрения ИБ

Приходится напрягаться, ибо нужно защищаться от рисков , связанные с конфиденциальностью ключей создания ЭП, на нашей стороне

Оценка с точки зрения оператора ЭДО и ИТ

Удобно работать с такими подписями: интегрировался на стороне сервера ЭДО, а всё остальное уже средствами системы мобильной подписи. Но напрягает, что оператор отвечает за риски с этой подписью

Оценка с точки зрения пользователей

Привычная работа в смартфоне, что не может не радовать

Оценка с точки зрения ИБ

Радует, что отсутствую риски, связанные с конфиденциальностью ключей создания ЭП, ни у нас и ни на стороне пользователя

Оценка с точки зрения оператора ЭДО и ИТ

Удобно работать с такими подписями: интегрировался на стороне сервера ЭДО, а всё остальное уже средствами системы мобильной подписи. И тоже радует, что радует нет рисков компрометации ключей с нашей стороны

КРИПТОПРО

Ключевое слово
в защите информации

СПАСИБО ЗА ВНИМАНИЕ!

127018, г. Москва, ул. Сущевский Вал, д.18
Тел./факс: +7 (495) 995-48-20

https://cryptopro.ru

Общие вопросы: **info@cryptopro.ru**
Контрактный отдел: **kpo@cryptopro.ru**
Для дилеров: **dealer@cryptopro.ru**