ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДА МОСКВЫ

ЭЛЕКТРОННАЯ ПОДПИСЬ В ГОСУДАРСТВЕННОМ СЕКТОРЕ

Вызовы, задачи, пути решения

Горбут Андрей
начальник отдела криптографической защиты информации
Департамент информационных технологий города Москвы

PKI-Форум 2023

Структура доклада

ДИТ

1 ПОЛУЧЕНИЕ СЕРТИФИКАТОВ

2 ПРИМЕНЕНИЕ СРЕДСТВ ЭП

3 ПРИМЕНЕНИЕ ДОВЕРЕННОСТЕЙ

4 ПРОВЕРКА ЭП ДОКУМЕНТОВ

PKI в инфраструктуре Правительства Москвы

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДА МОСКВЫ

1 334
Информационных ресурсов обеспечены защитой ГОСТ-TLS

50 187
сотрудников используют КЭП

106
Информационных систем используют КЭП

2 420
органов власти и учреждений

281 млн
Проверок КЭП, выполненных по запросам систем ДИТ Москвы

1 468
граждан получили комплексную услугу за 2023 г., в составе которой предоставляется КЭП

World Innovation Award 2023
Лауреат премии ООН в области развития цифровой экосистемы городской среды

>15,7 млн
зарегистрированных пользователей на mos.ru

>400
услуг и сервисов в электронном виде

1 ПОЛУЧЕНИЕ СЕРТИФИКАТОВ

Осознанное использование КЭП

ДИТ

Мероприятия, способствующие повышению эффективности использования усиленной электронной подписи

Обучение и информирование

Повышение уровня культуры использования СКЗИ (курсы обучения, каналы информирования)

Удобство получения сертификатов

Пользователи самостоятельно и осознанно выполняют действия с ключами

Адаптивный выбор СКЗИ

СКЗИ соответствует условиям работы пользователей

Контроль отзыва сертификатов

Наличие механизмов оперативного отзыва сертификатов ЭП и МЧД

Единые стандарты, решения и сервисы

Одинаковый подход к реализации технологии электронной подписи и криптозащиты в ИС

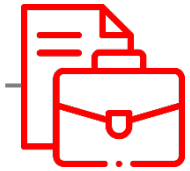
ОПЫТ МОСКВЫ

8 Централизованных сервисов по использованию СКЗИ и средств ЭП

Информационный канал и методическое обеспечение

Кадровый документооборот с ЭП

Кандидаты на трудоустройство



Оформление в ОИВ/учреждение

Получение КЭП

Удостоверяющий центр Федерального Казначейства

Трудоустроенные сотрудники

Подписание кадровых документов

Потребность в подписании ЭП кадровых документов возникает до момента трудоустройства

Использование НЭП/ КЭП физического лица

Привлечение доверенных лиц

ДИТ

Очная идентификация при получении КЭП должна быть удобной и доступной для пользователей

Открытые вопросы

Привлечение доверенных лиц к выдаче квалифицированных сертификатов в отдельных проектах и сферах деятельности (с сохранением мер контроля)

Расширение полномочий доверенных лиц, в том числе по подаче заявлений на отзыв сертификатов, выданных таким доверенным лицом

ОПЫТ МОСКВЫ

Соглашение с Федеральным казначейством

Постановление Правительства Москвы

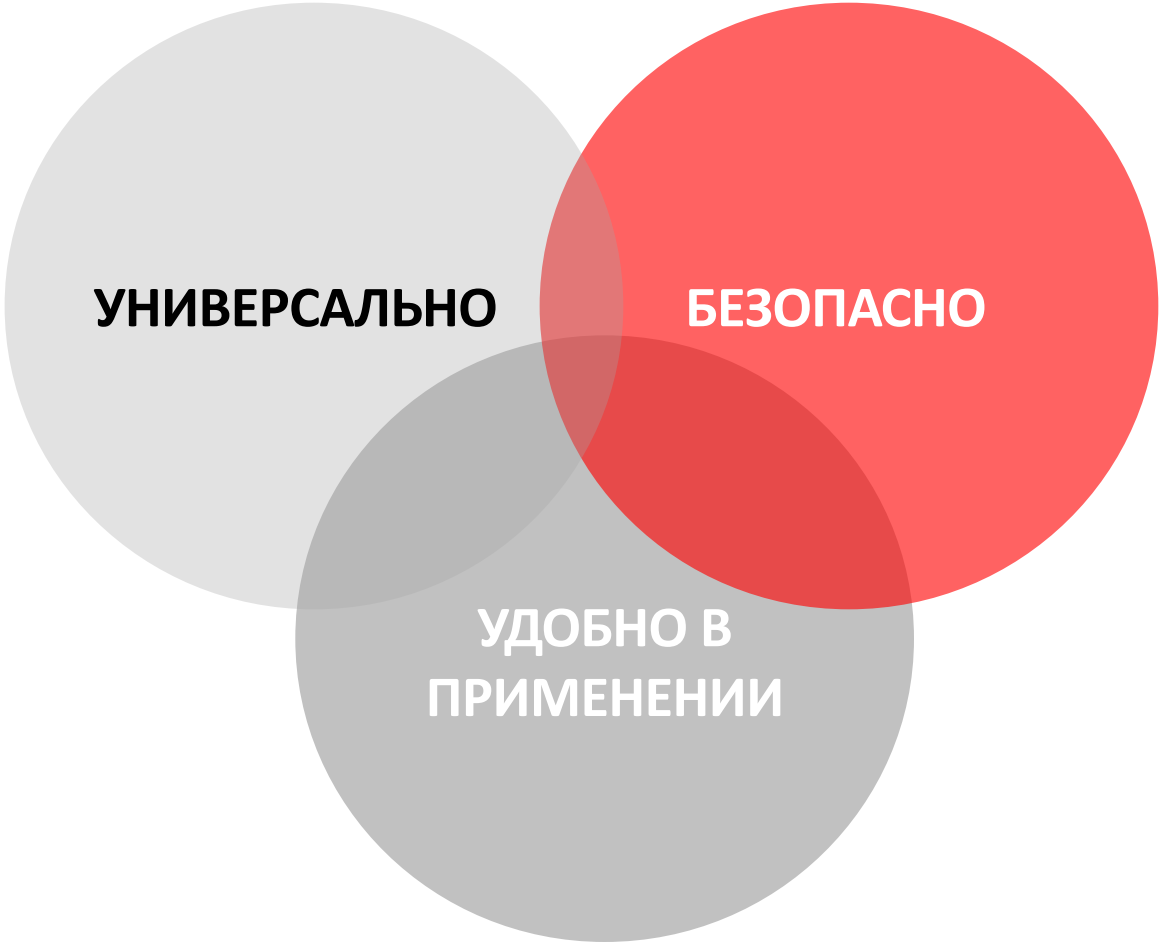
Представители доверенного лица в ОИВ

47 тысяч КЭП выдано за 2023 год

2 ПРИМЕНЕНИЕ СРЕДСТВ ЭП

Использование дистанционной/мобильной ЭП

ДИТ



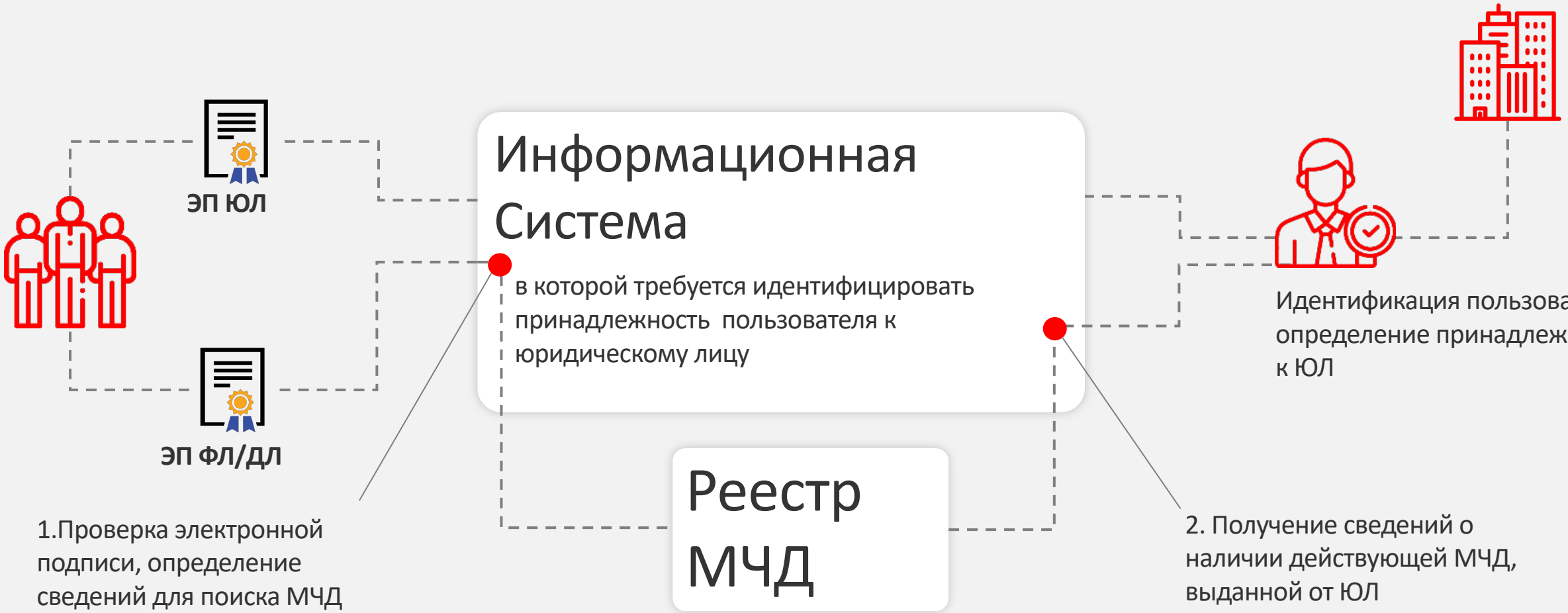
Рост потребности в применении усиленной квалифицированной электронной подписи

Облачная (дистанционная) электронная подпись – комплексное решение

Идентификация представителей ЮЛ

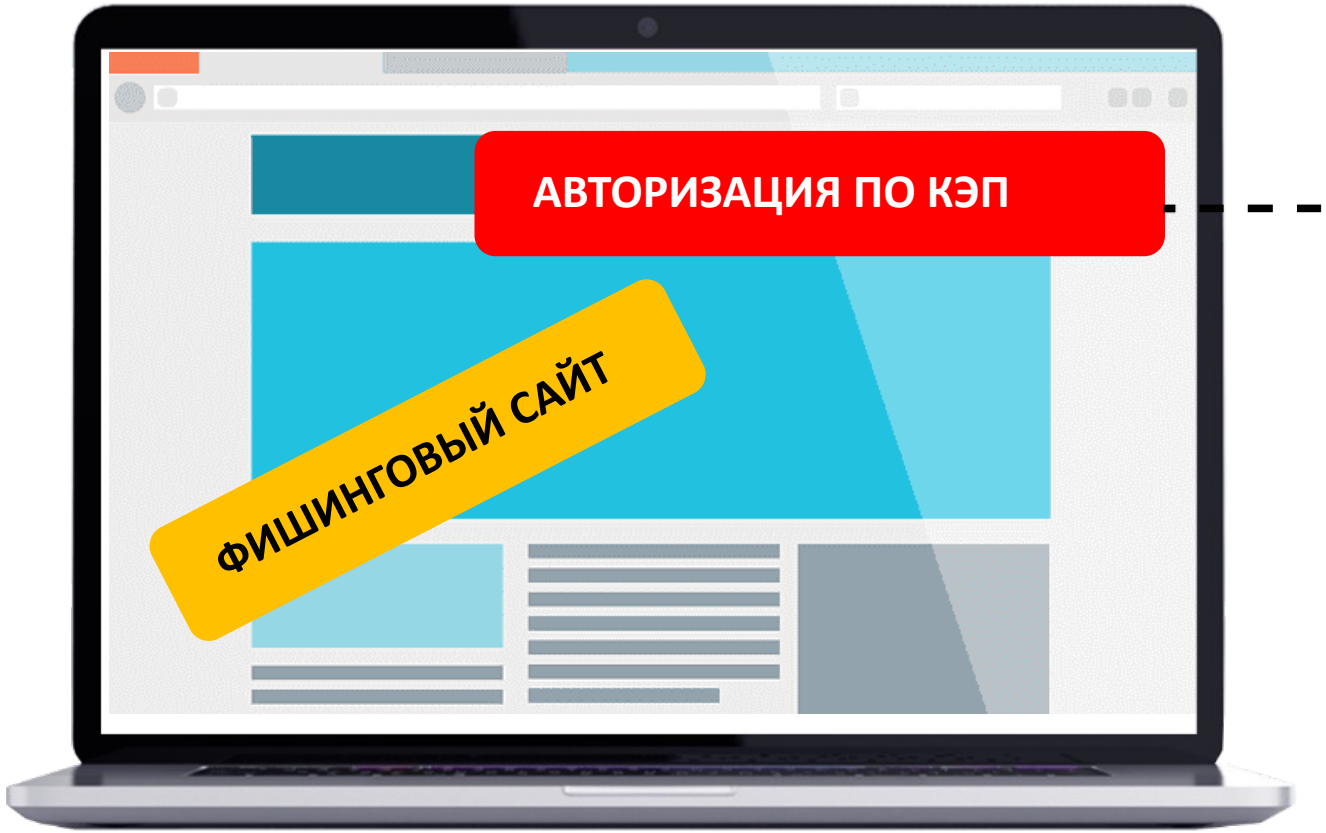
ДИТ

Необходим механизм подтверждения принадлежности физического лица к организации



Риски аутентификации по КЭП

Использование КЭП для аутентификации влечет потенциальные риски подмены подписи данных



» Использование НЭП в качестве инструмента для аутентификации

Подмена подписываемых данных

3 ПРИМЕНЕНИЕ ДОВЕРЕННОСТЕЙ

Полномочия в электронных доверенностях

Выбор полномочий в составе МЧД должен быть понятным для пользователей и исчерпывающим для информационных ресурсов

Классификатор полномочий

Сейчас

Полномочия определяются участниками электронного взаимодействия, дублируются по смыслу

Потребность

Полномочия выбираются из базового классификатора полномочий (с учетом ограничений), дополняются полномочиями, эксклюзивными для ИС

Реализация в системах

Полномочия сопоставляются с параметрами разграничения доступа в информационных системах для ограничения возможности просмотра сведений и подписания документов

Хранение МЧД

МЧД хранится
а) Головной УЦ;
б) Гос УЦ (ФНС, ФК, ЦБ);
в) АУЦ;
г) ДТС;
д) Специальные операторы связи;
е) ИС, в которой подписан и из которой направляется электронный документ, подписанный КЭП;
ж) ФОИВы, внебюджетные фонды

3) Информационная система, определенная решением субъекта Российской Федерации

Субъекты Российской Федерации не могут:

- Организовать централизованное хранение МЧД в региональной информационной системе

- Присоединиться к использованию распределенного реестра для хранения МЧД в том числе для проверки выданных МЧД

Рассмотреть возможность добавления дополнительных мест хранения МЧД

Особенности формата МЧД

ДИТ

Дополнение формата МЧД. Предложения к рассмотрению

Указание информации о системе, в которой выдана МЧД

В поле сведений указывается произвольное наименование системы или ссылка

```
<СвДов ВидДовер="1" ПрПередов="1" ВнНомДовер="125"
  <СведСист>https://m4d.nalog.gov.ru/</СведСист>
</СвДов>
```

Определить формат добавления ссылки с возможностью простановки сведений, необходимых для проверки основных параметров МЧД (по ссылке)

Указание даты выдачи и срока действия МЧД в абсолютном формате

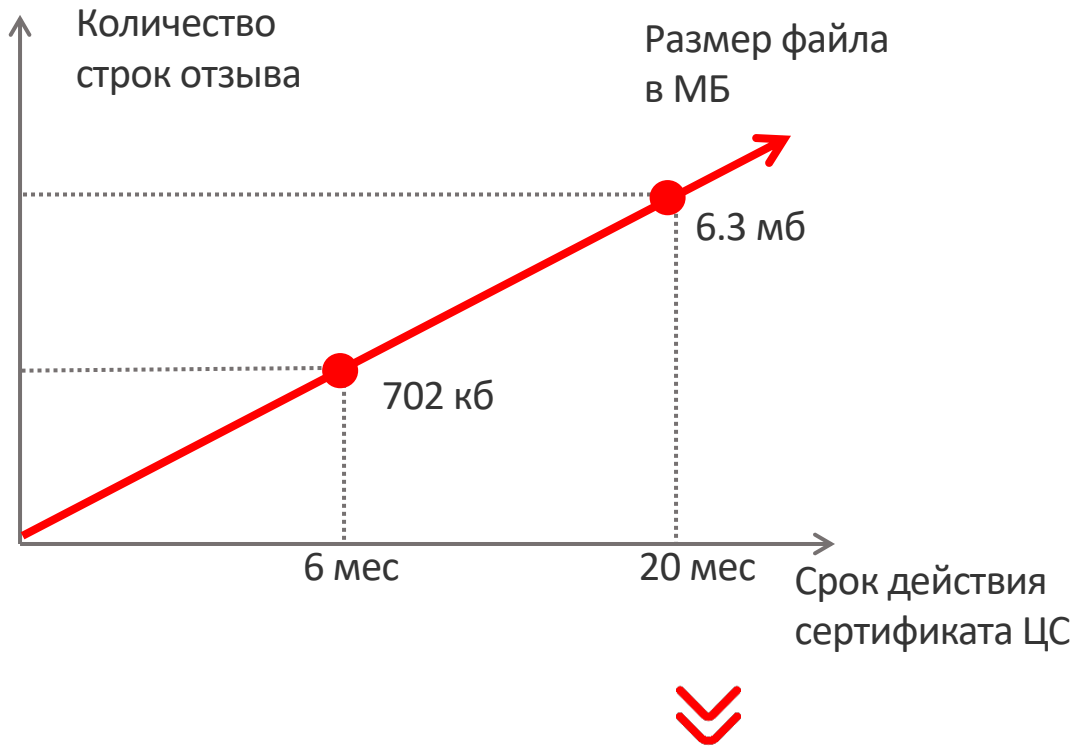
Время начала и окончания доверенности не уточняется

```
ДатаВыдДовер="2023-09-04" СрокДейст="2024-09-04">
```

Цифровые действия обычно предполагают точность с указанием времени. В некоторых случаях это может быть неудобным, однако при автоматизированной проверке МЧД является верным

4 ПРОВЕРКА ЭП ДОКУМЕНТОВ

Проверка отзыва сертификатов по CRL



Размер файла CRL центра сертификации зависит от количества записей об отозванных сертификатах

Количество записей об отозванных сертификатах в CRL будет увеличиваться при переходе на сертификаты длительного срока действия

Рассмотреть возможность более частого обновления сертификатов центров сертификации для снижения размеров файлов CRL

ОПЫТ МОСКВЫ

Перевыпуск сертификатов, используемых для автоматизированного подписания и аутентификации серверов по мере смены промежуточного сертификата УЦ

Использование механизмов OCSP

ДИТ

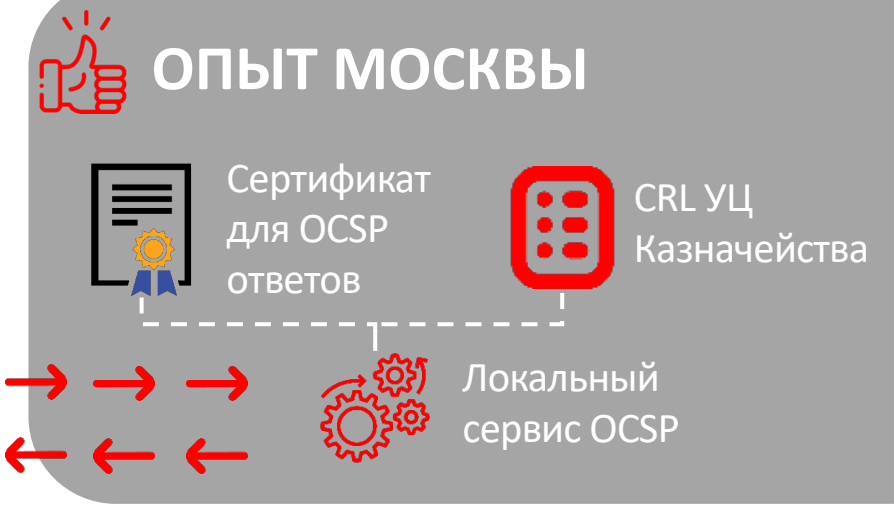
В настоящее время в сертификатах большинства аккредитованных удостоверяющих центров отсутствует указание на OCSP. Сервис не предоставляется

⚠ Форматы длительного хранения электронной подписи предполагают наличие атрибута ответа OCSP сервера.

⚠ Адрес службы OCSP должен указываться в составе квалифицированного сертификата

1. Необходимо рассмотреть возможность организации OCSP сервисов в центрах сертификации на обязательной основе
2. Закрепить порядок получения сертификатов для подписания OCSP ответов операторами локальных сервисов, работающим по сведениям из CRL

ОПЫТ МОСКВЫ



Дальнейшее развитие отрасли

ДИТ

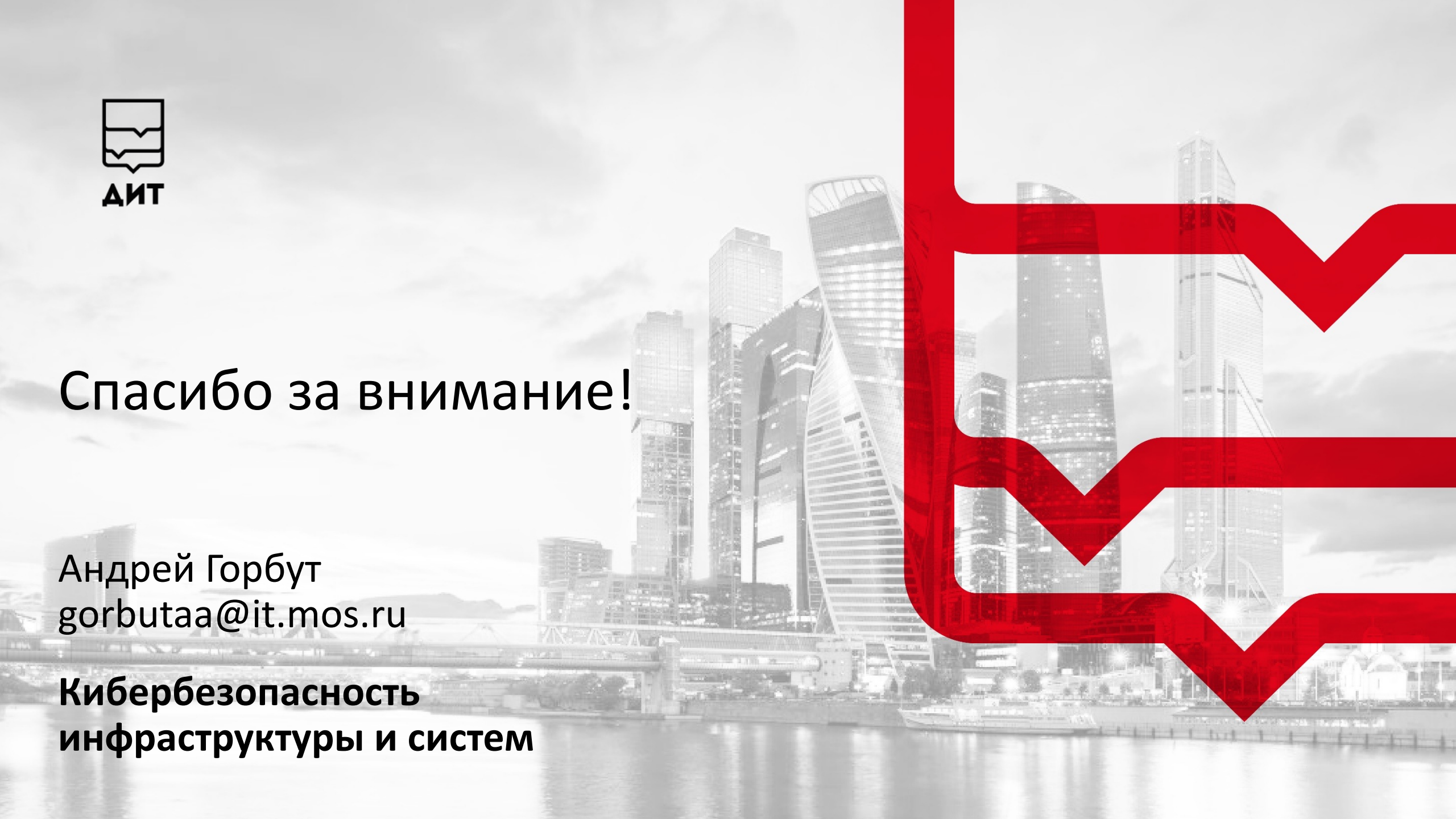
Экспертное мнение с учетом актуальных задач и потребностей

Направления, которые зададут вектор развития в ближайшую перспективу

- Кадровый документооборот в электронном виде
- Криптографическое усиление существующих мер защиты информации
- В условиях импортозамещения развитие клиентских сервисов, используемых в западных продуктах

Сферы, требующие разработки стандартов и дополнительного регулирования

- Технология дистанционной (облачной) электронной подписи
- Долгосрочное хранение документов с ЭП
- Проверка МЧД и хранение результата проверки МЧД



ДИТ

Спасибо за внимание!

Андрей Горбут
gorbutaa@it.mos.ru

Кибербезопасность инфраструктуры и систем