Проект развития международного защищенного электронного документооборота в сегменте B2B

Лившиц Илья Иосифович, д.т.н., Университет ИТМО

Сессия 5 «PKI и ЭП в международной цифровой повестке»

17.09.2020, г. Санкт-Петербург

Нормативная база для ЭДО (1)

- С 08.04.2011 действует **Федеральный закон № 63-ФЗ "Об электронной подписи"**, который определяет порядок получения и использования электронной подписи и обязанности участников обмена электронными документами.
- Налоговым законодательством установлено, что если истребуемые у налогоплательщика документы составлены в электронной форме по установленным ФНС России форматам, то налогоплательщик вправе направить их в налоговый орган в электронном виде по телекоммуникационным каналам связи или через личный кабинет налогоплательщика (**п. 2 ст. 93 НК РФ**).
- С 15.01.2018 применятся приказ **ФНС России № ММВ-7-6/1096@** "О расширении электронного документооборота между налогоплательщиками и налоговыми органами в отношениях, регулируемых законодательством о налогах и сборах.
- С 02.09.2010 года действует норма налогового законодательства, предоставляющая налогоплательщикам возможность выставлять счета-фактуры в электронной форме по взаимному согласию сторон сделки и при наличии у указанных сторон совместимых технических средств и возможностей для приема и обработки этих счетов-фактур в соответствии с установленными форматами и порядком (**абз. 2 п. 1 ст. 169 НК РФ**).

Нормативная база для ЭДО (2)

Новый **ГОСТ Р 7.0.8-2013**. СИСТЕМА СТАНДАРТОВ ПО ИНФОРМАЦИИ, БИБЛИОТЕЧНОМУ И ИЗДАТЕЛЬСКОМУ ДЕЛУ. ДЕЛОПРОИЗВОДСТВО И АРХИВНОЕ ДЕЛО. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

- **Юридическая значимость документа**: Свойство документа выступать в качестве подтверждения деловой деятельности либо событий личного характера (п. 3.1 (14)).
- **Электронный документооборот:** Документооборот с использованием автоматизированной информационной системы (системы электронного документооборота). (п. 3.2.2. (74)).
- **Включение документа в СЭД:** Осуществление действий, обеспечивающих размещение сведений о документе и/или документа в системе электронного документооборота. (п. 3.2.2. (78)).

Подпись электронных документов

- В соответствии с нормами Федерального закона от 06.04.2011 **№ 63-ФЗ "Об электронной подписи"** электронные документы, подписанные **квалифицированной ЭП**, всегда признаются равнозначными документам, подписанным собственноручно и могут применяться в любых правоотношениях в соответствии с законодательством РФ.

- Электронные документы, подписанные **простой ЭП** или **неквалифицированной ЭП**, признаются равнозначными документам на бумажном носителе, подписанным собственноручно, если это установлено законодательством или соглашением между сторонами.

- Согласно п. 4 ч. 3 ст. 21 **Закона № 402-ФЗ** виды электронных подписей, используемых для подписания документов бухгалтерского учета, должны быть установлены соответствующим федеральным стандартом, который на настоящий момент отсутствует.

- **Налоговый кодекс РФ** признает только те электронные документы, которые подписаны **усиленной квалифицированной ЭП** (п. 7 ст. 23, п.п. 4, 6 ст. 78, п. 2 ст. 79, п. 1 ст. 80, п. 6 ст. 169, п. 6 ст. 176 НК РФ).

Новые требования к признанию иностранной электронной подписи (ФЗ-63 Ст.7 п.3)

Признание электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами

- Признание электронных подписей, созданных в соответствии с нормами права иностранного государства и международными стандартами, соответствующими признакам **усиленной электронной подписи**, и их применение в правоотношениях в соответствии с законодательством Российской Федерации осуществляются в случаях, установленных международными договорами Российской Федерации. Такие электронные подписи признаются **действительными** в случае подтверждения соответствия их требованиям указанных международных договоров аккредитованной доверенной третьей стороной, **аккредитованным удостоверяющим центром**, иным лицом, уполномоченными на это международным договором Российской Федерации, с учетом настоящего Федерального закона.

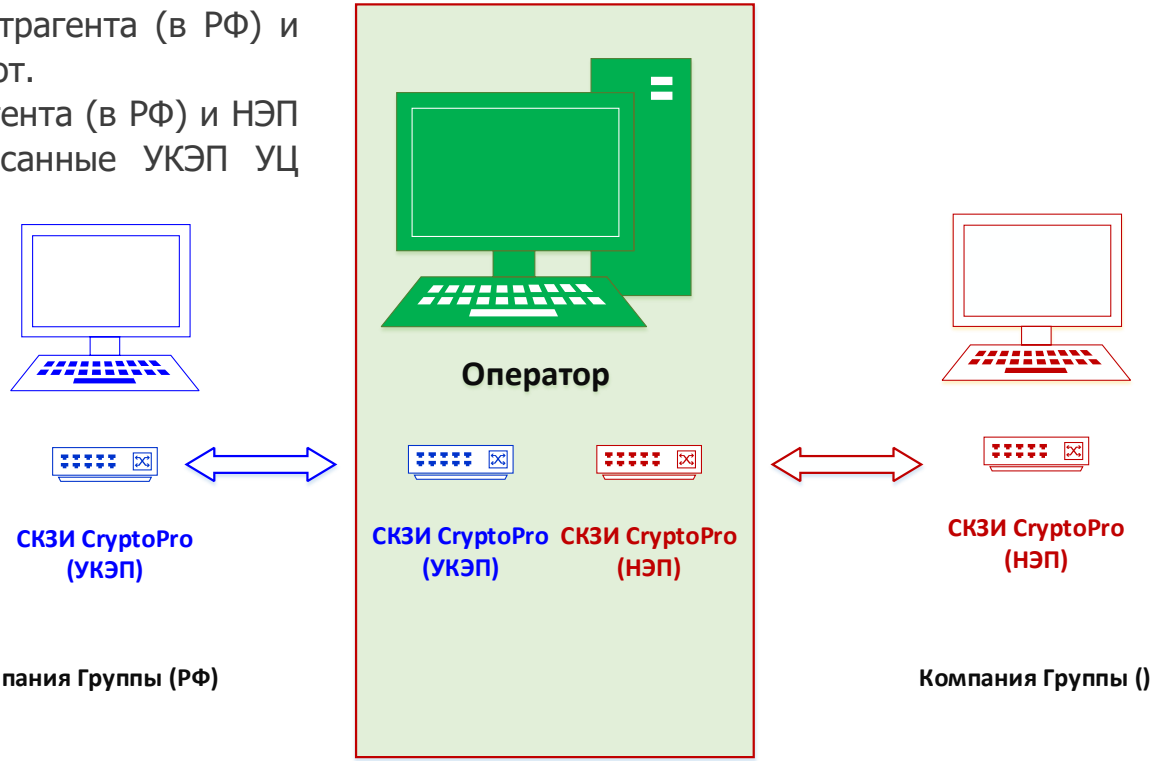
Решение ЭДО в России. Общий анализ

Всего доступно более 100 систем ЭДО, имеющих различный функционал.
Краткое сравнение 7 лучших (по степени интеграции с прикладным ПО)

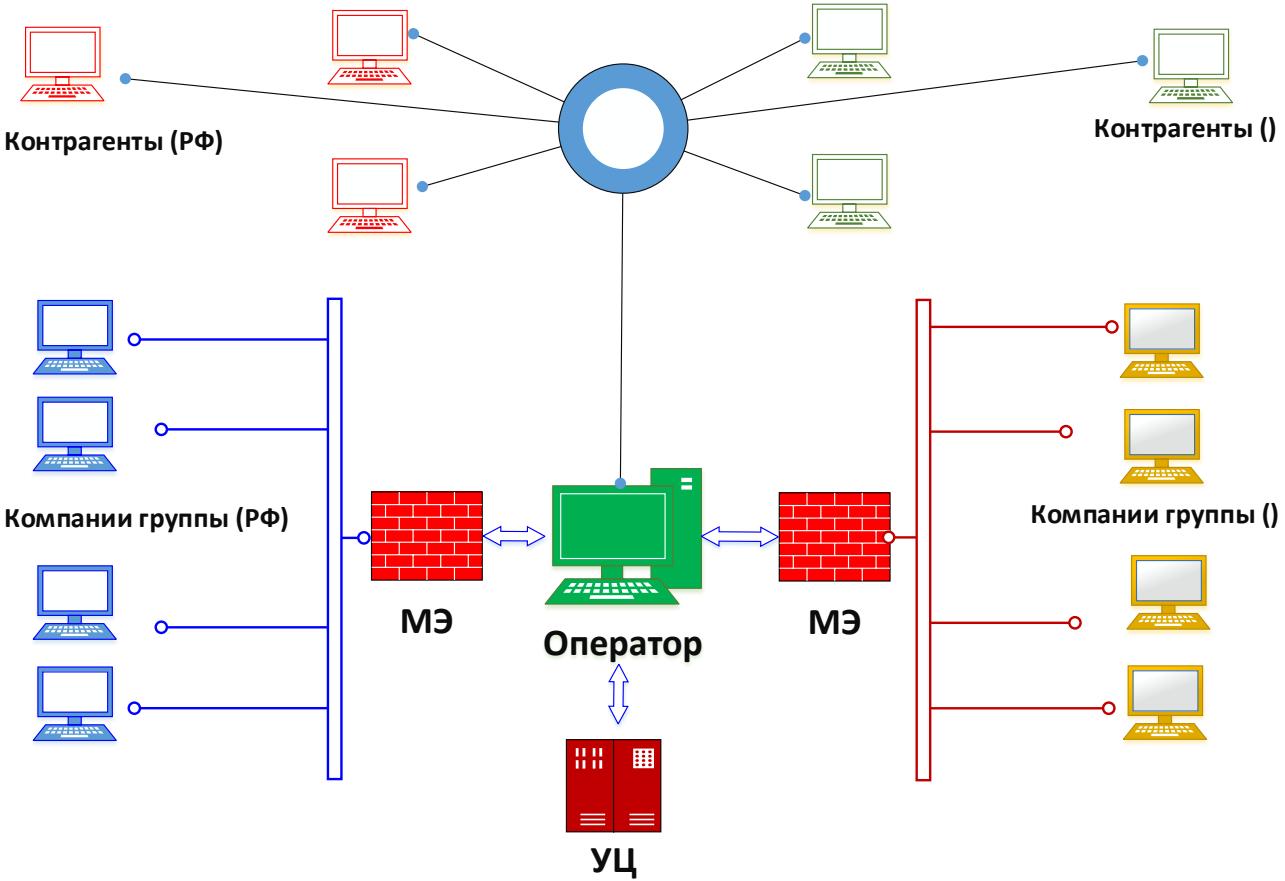
	Контур.Диадок	Taxcom	СБИС	Synerdocs	Калуга.Онлайн	Сфера Курьер	E-COM
SAP	+	+	+	+	−	+	+
Oracle	+	+	+ (API)	−	−	−	+
DIRECTUM	+	−	+ (API)	+	−	+	−
Открытый API	+	−	+	+	−	+	+
Универсальный инструмент/ коннектор для интеграции	+	+	+	+	−	+	+

Описание замысла задачи

- Сервер «Диадок» на двух интерфейсах (внутреннем и внешнем) имеет СКЗИ CryptoPro.
- Обеспечивается ЭП для ЭД от контрагента (в РФ) и контрагента (за рубежом) и наоборот.
- Обеспечиваются логи УКЭП контрагента (в РФ) и НЭП контрагента (за рубежом), подписанные УКЭП УЦ «Диадок».



Описание эскиза технической задачи



Варианты обеспечения НЭП для зарубежных компаний и контрагентов

Варианты обеспечения НЭП контрагента (за рубежом):

1. Поставить каждому контрагенту CryptoPro (в экспортном исполнении);
2. Принимать от каждого контрагента ЭД, подписанный ЭП на произвольном СКЗИ (RSA,…) и далее передавать на сервер «Диадок» все открытые ключи для проверки каждой ЭП.
3. Поставить 1 экз. CryptoPro на «хаб», который бы собирал все ЭП от иных контрагентов (за рубежом), вне зависимости от типа используемого СКЗИ.

Оценка вариантов:

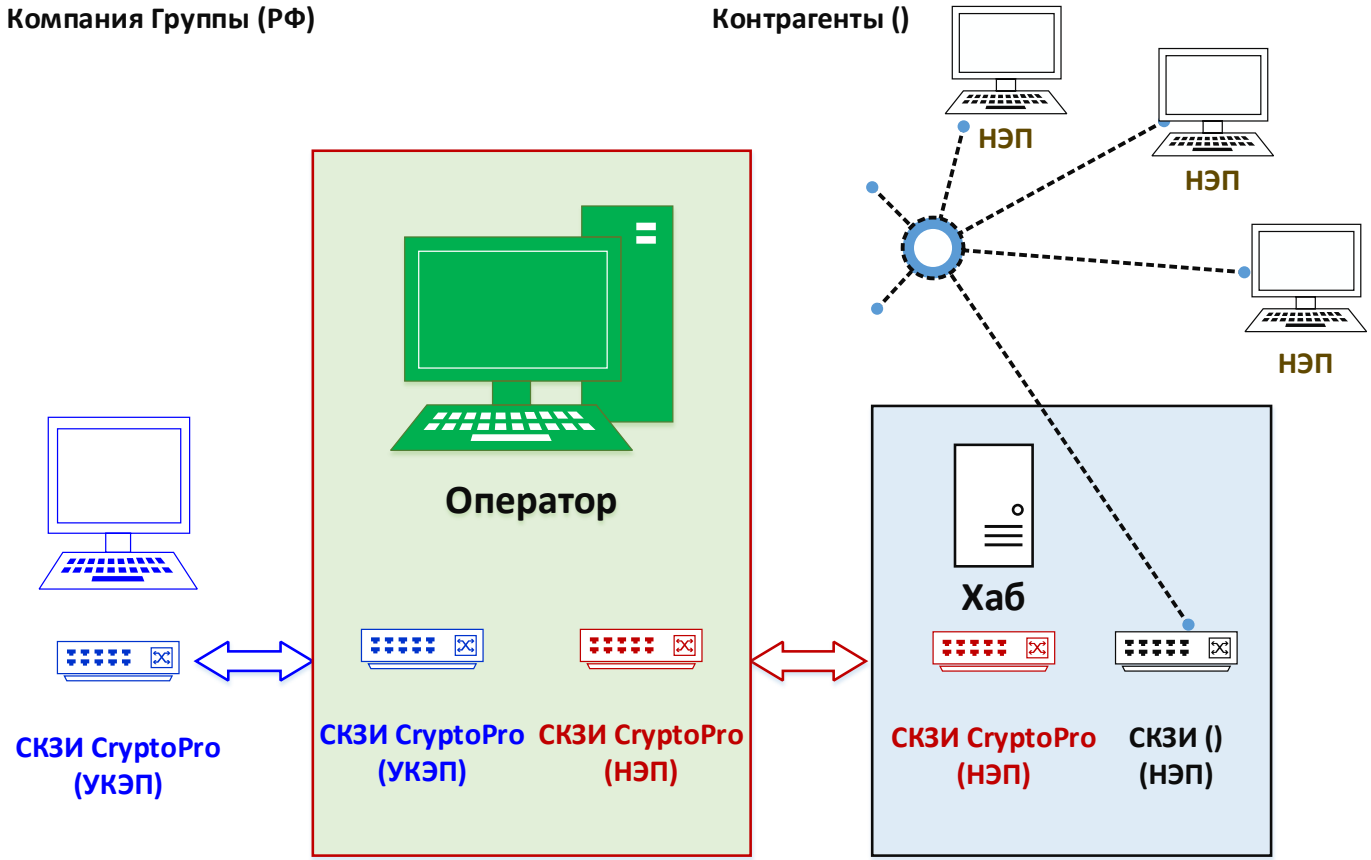
- вариант 1 – самый **дорогой**;
- вариант 2 – самый **сложный**;
- вариант 3 – самый **удобный**.

Описание эскиза пилотного проекта

Реализация пилотного проекта:

- Все контрагенты в своей системе используют свои форматы ЭП и передают на «хаб» только сам ЭД и данные по подтверждению его аутентичности;
- «Хаб» может быть в «облаке» или на стороне головного офиса или внутри корпоративной сети или…;
- «Хаб» транслирует ЭД, ЭП к нему и всю информацию о внутреннем согласовании внутри корпоративной сети;
- Эта информация передается на сервер «Диадока» под ЭП (CryptoPro);
- От «Хаба» идет один защищенный канал CryptoPro на сервер «Диадок»;
- Всем участникам МЭДО удобно работать.
- Подтверждение ЭП (НЭП), на стороне зарубежного партнера подтверждается УЦ «Диадок», физически на территории Российской Федерации;
- Подтверждение ЭП (УКЭП), на стороне российских контрагентов подтверждается УЦ «Диадок», физически на территории Российской Федерации.

Описание концепции технического решения для пилотного проекта



Преимущества проекта МЭДО

Основные преимущества проекта МЭДО:

- гибкая и бесшовная интеграция со всеми корпоративными ИТ-системами (1С);
- применение современных СКЗИ (CryptoPro);
- соблюдение требований импортозамещения и наличие необходимых сертификатов;
- способность обеспечивать безопасный обмен ЭД для всех Компаний и зарубежных контрагентов по установленным маршрутам.

В перспективе планируется завершить пилотирование и развернуть полномасштабный действующий рабочий проект в периметре всех Компаний, полностью соответствующих применимым национальным и международным нормативным требованиям в области информационной безопасности.

Благодарим за внимание!

Лившиц Илья Иосифович, д.т.н., Университет ИТМО

Livshitz.il@yandex.ru
+7 (921) 934-48-46

Проект развития корпоративной PKI-инфраструктуры, соответствующей методологии Zero Trust Architecture

Соколов Егор Олегович, Gazprom International

Сессия 5 «PKI и ЭП в международной цифровой повестке»

17.09.2020, г. Санкт-Петербург

Общие положения методологии Zero Trust Architecture (ZTA)

- ZTA внедряют везде, это просто товар или хорошая практика?
- ZTA помогает бороться с уязвимостями в прикладном и общесистемном ПО?
- ZTA позволяет контролировать подрядчиков, предоставляющих сервисы?
- ZTA позволяет решить большую проблему – безопасность персонала?

Принципы Zero Trust Architecture (ZTA)

- Модель Zero Trust, как и расширенная модель – Zero Trust eXtended (ZTX), является реализацией **принципа «Доверяй, но проверяй».**
- Модель предполагает, что к действиям пользователя, находящегося **внутри** периметра корпоративной ИТ-инфраструктуры, надо относиться так же подозрительно, как и к действиям контрагентов, запрашивающих доступ **извне**.
- Модель включает:
  - ✓ оценивание контекста для пользователей (**context** в нотации ISO),
  - ✓ **выявление угроз** и **оценка рисков** (в нотации ISO, NIST, Cobit) для PKI-инфраструктуры в периметре Компаний Группы,
  - ✓ **верификацию УЦ** (CA) в периметре Компаний Группы,
  - ✓ **валидацию конечных устройств** с установленными СЗИ и СКЗИ,
  - ✓ **авторизацию доступа** к PKI-сервисам в периметре Компаний Группы,
  - ✓ **восстановление устойчивости** (Resilience)

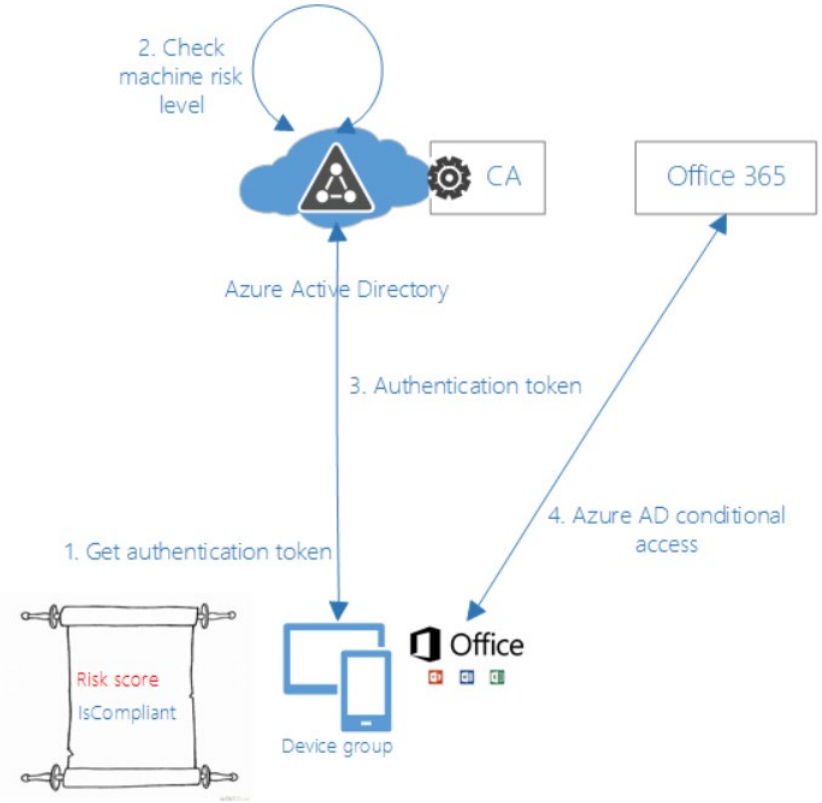
Примеры реализации Zero Trust Architecture (ZTA)

- **Building Zero Trust networks with Microsoft 365**

https://www.microsoft.com/security/blog/2018/06/14/building-zero-trust-networks-with-microsoft-365/

- **NIST Special Publication 800-207 «Zero Trust Architecture»**

https://doi.org/10.6028/NIST.SP.800-207-draft2



Основные требования к обеспечению безопасности корпоративной PKI-инфраструктуры

- Соответствие применимым требованиям **различных юрисдикций** в части ЭП;
- Защита «**одной степени прочности**» для внутренних и/или внешних интерфейсов;
- Ориентация на **отечественные** СЗИ и СКЗИ для формирования ЭП и/или шифрования;
- Обеспечение **мгновенного** и в равной степени **безопасного** обмена документами по установленным и резервным каналам связи;
- **Разделение функций безопасности и администратора** в периметре Компаний Группы;
- Обеспечение надежного и безопасного **длительного архивного хранения документов**.

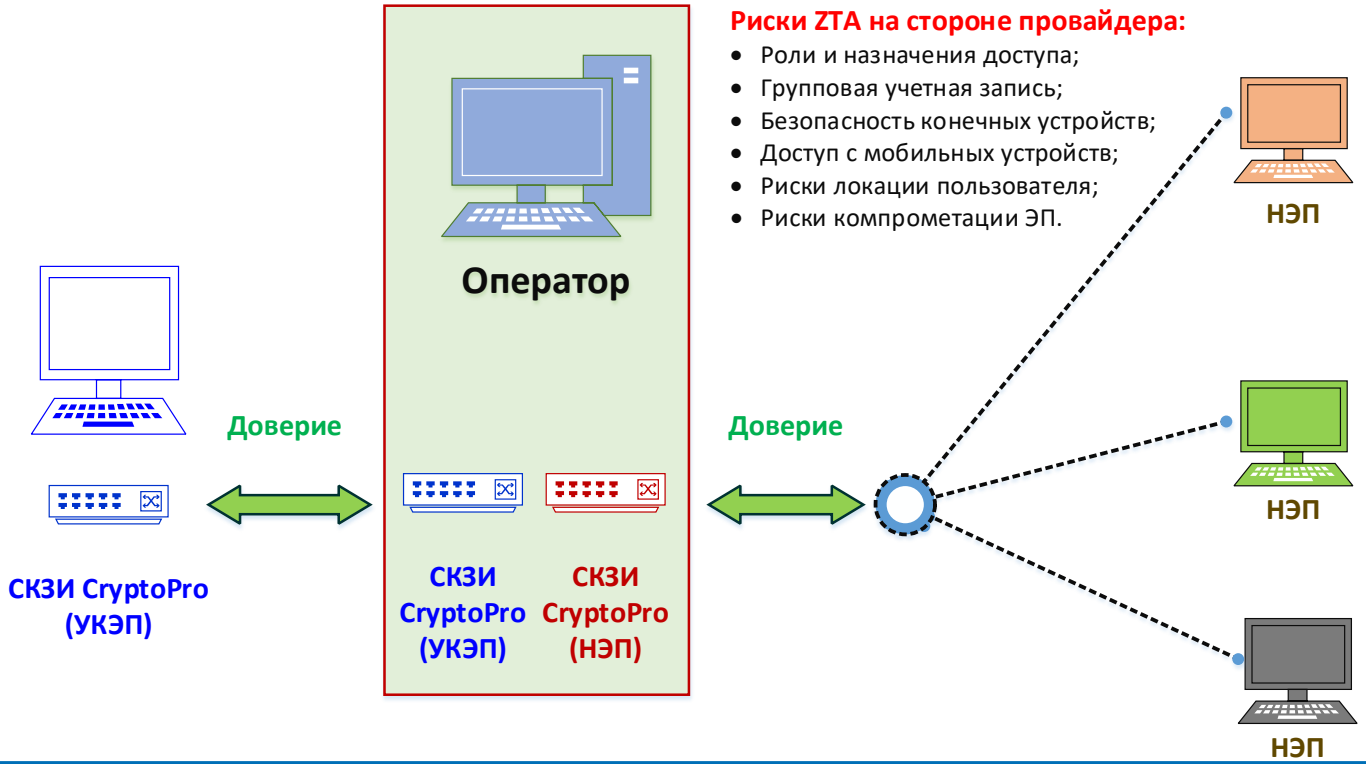
Реализация пилотного проекта для Компаний Группы

- Формирование **междисциплинарной** рабочей группы в периметре Компаний Группы.
- Определение **приоритетных бизнес-процессов** для цифровой трансформации.
- Формирование перечня **цифровых сервисов**, доступных на объектах Компании Группы.
- Определение **состава** и технических **характеристик** СЗИ и СКЗИ для формирования ЭП и/или шифрования в периметре Компаний Группы с учетом методологии ZTA.
- Заключение необходимых **сервисных контрактов** с учетом методологии ZTA

Описание концепции технического решения для пилотного проекта

Контрагенты (РФ)

Контрагенты (В мире)



Преимущества проекта развития корпоративной PKI-инфраструктуры

Основные преимущества проекта развития корпоративной PKI-инфраструктуры:

- интеграция современных технологий ЭДО и средств защиты – СЗИ и СКЗИ для шифрования и/или удостоверения ЭП внутренних и/или внешних документов, обращающихся во всех юрисдикциях в периметре Компаний Группы.
- Методология Zero Trust Architecture (ZTA) позволяет проектировать и управлять полным жизненным циклом цифровых сервисов исходя из равных предположений о доверенных соединениях внутри и извне по отношению к корпоративной ИТ-структуре.

В перспективе планируется завершить пилотирование и развернуть полномасштабный действующий рабочий проект в масштабе всех Компаний Группы, полностью соответствующих применимым национальным и международным нормативным требованиям в области информационной безопасности.

Благодарю за внимание!

Соколов Егор Олегович, Gazprom International
E.Sokolov@gazprom-international.com