DOI: 10.25728/avtprom.2021.06.08

# Общие технические решения для безопасного документооборота

**И.И. Лившиц (Университет ИТМО)**

*Показано, что электронный документооборот (ЭДО) предоставляет предприятиям такие преимущества, как достоверность, простоту, скорость и неотказуемость при работе с документами. Приведены примеры известных проектов, реализованных в России. Указаны проблемы, связанные с использованием ЭДО, и рассмотрены экономические аспекты реализации таких решений. Приведен подход к оценкам рисков внедрения ЭДО. Рассмотрен проект международного ЭДО в транснациональной компании.*

*Ключевые слова: документ, документооборот, простая электронная подпись, усиленная квалифицированная электронная подпись, информационная безопасность, риски.*

## Введение

Актуальность применения современных решений для обмена документами в электронном виде (электронный документооборот, ЭДО) не вызывает возражений. ЭДО необходим как дополнительный гибкий, эффективный и безопасный инструмент, предоставляющий всем участникам информационного взаимодействия ранее недоступные преимущества – достоверность, простоту, скорость и неотказуемость при работе с электронными документами. Но при этом встают вопросы технической реализации, информационной безопасности (ИБ) и удобства для пользователей все еще являются известной проблемой. Для решения этой проблемы применяются программные продукты на базе Microsoft, Oracle, SAP, также известны десятки реализаций на базе отечественных ИТ-компонентов (например, 1С). Причем проекты на базе 1С занимают до 53% рынка, а на долю SAP и Oracle приходится только 22% и 3% соответственно[1].Каждая компания решает, какие именно ИТ-компоненты нужно применять, но наличие простой и эффективной корпоративной платформы (например, 1С) позволяет снизить стоимость таких решений до приемлемого уровня.

С учетом особенностей национального законодательства применяется несколько видов электронных подписей (ЭП), например: простая (ПЭП) и усиленная квалифицированная (УКЭП). Характерной особенностью является преимущество использования национальной криптографии (например, Крипто-Про).

## Известная практика проектов ЭДО

На сегодняшний день многие компании заявили о выполнении проектов «цифровой» трансформации, в том числе проектов ЭДО (Сбербанк, ПАО «Ростелеком», X5, «Газпром нефть» и пр.) [1 – 4]. Проводится эксперимент с переводом кадрового ЭДО в электронную форму в соответствии с ФЗ "О проведении эксперимента по использованию электронных документов, связанных с работой" от 24.04.2020 N122-ФЗ. Примечательно, что участники эксперимента ориентируются на использование простой электронной подписи (ПЭП), данные которой загружают через шлюзы Единой системы идентификации и аутентификации (ЕСИА)[2].

Известно, что ПЭП не содержит криптографических функций, в отличие от УКЭП, и не может быть проверена специальными сервисами безопасности, например, удостоверяющими центрами (УЦ). Конечно, риски использования только ПЭП весьма значимы [5 – 6], но многие разработчики ЭДО разрабатывают собственные решения в области криптографии (СКЗИ – средства криптографической защиты информации) и оформляют на них специальные патенты. ФЗ-122 требует усиленную квалифицированную подпись (УКЭП) только для трех типов документов: трудовые договоры, договоры материальной ответственности и ученические договоры, так что применение УЦ и УКЭП не является обязательным. Пока нельзя заявить, что все документы будут «оцифрованы» даже в крупных компаниях, например, в ПАО «Ростелеком» установлено всего 23 типа электронных документов, и доля всех кадровых документов в электронном виде не превышает 58%.

Приведем статистику использования разных видов ЭП[3]: лидирует ПЭП – до 79% и УКЭП – 58% (допускалось несколько вариантов ответов).

Необходимо обращать внимание на объемы использования ЭП, например, представители компании ПИК сообщали, что за 6 мес. выдали своим сотрудникам 2605 УКЭП и подписали только 2880 электронных документов. Возможно, такой порядок обеспечения ИБ соответствует принятой концепции в конкретной компании, но следует помнить об удобстве пользователей и о стоимости данного решения.

## Известные проблемы проектов ЭДО

На основании данных из открытых источников сформулируем основные проблемы, возникающие при реализации проектов ЭДО.

1. Работники не всегда видят, кому должен передаваться электронный документ, и какой ЭП подписан конкретный тип документа (привычка видеть «визы» на бумажной копии).

[1] https://www2.deloitte.com/ru/ru/pages/tax/articles/2021/hr-edf-survey-2020.html
[2] https://msbevents.com/docs/9th-annual-kedo/
[3] https://www2.deloitte.com/ru/ru/pages/tax/articles/2021/hr-edf-survey-2020.html

2. Ориентация на сервис проверки ПЭП на сайте Минтруда, что может привести к рискам корректной идентификации работника, подписавшего конкретный тип документа, поскольку ПЭП не предполагает использования доверенной инфраструктуры УЦ.

3. Работники не смогут более подписывать электронные документы «задним числом», что для многих организаций означает серьезные риски ЭДО.

4. Проблемы выполнения кадровых функций для работников, которые не приходят в офис, не имеют или не используют ПЭП (УКЭП), не выполняют установленные технические регламенты.

### Экономические аспекты создания ЭДО

Остановимся на оценивании проекта внедрения ЭДО по критерию экономической эффективности.

1.Группа компаний «Прауд» оказывает услуги по реализации ЭДО на платформе 1С (https://business.pra.ru/primery_proektov). Проект ЭДО может занять по длительности до 1 года. Примечательно, что приводится многокритериальный анализ ускорения обработки документов с использованием ЭДО – по времени (до 5 раз). Стоимость проекта, ориентировочно, не менее 1 млн. руб.

2. Проект группы «Тезис» (https://www.tezis-doc.ru/buy) по стоимости составляет свыше 920 тыс. руб. из расчета на 100 рабочих мест.

3.Компания «Контур – Диадок» (https:// www.diadoc.ru/price) предлагает сервисную модель ЭДО при стоимости примерно 6 руб. за 1 документ при 6 тыс. исходящих документов. Кроме того, дополнительно нужно учесть консультационные услуги (внедрение, настройка) - минимально 2600 час.

4. Компания «Директум» (https://www.directum.ru) предлагает за 2 млн. руб. пакет 200 базовых лицензий, и отдельно – управление договорам – 12 тыс. руб., финансовый архив – 260 тыс. руб., web-доступ к системе ЭДО – 125 тыс. руб.

5.Решение компании «Атлас-Софт» (https:// www.atlas-soft.ru) предусматривает серверную лицензию – 85 тыс. руб., но нет точных данных по клиентским рабочим местам.

6.Предложение компании Энсол (https:// endocs.ru) отличается большой вариативность: серверная лицензия – 200 тыс. руб., отдельная лицензия на систему хранения – 600 тыс. руб., отдельно поддержка ЭП – 200 тыс. руб., пакет 150 пользовательских лицензий – 350 тыс. руб.

Подводя итоги, оценим полный проект ЭДО, выполненный сторонней компанией, по минимальным параметрам: длительность от 1 года и стоимость от 1 млн. руб. только в отношении базовых компонентов ПО. В том случае, если требуется консалтинг, услуги внедрения, сопровождения, приобретения сертификатов УКЭП (НЭП), то стои-мость проекта ЭДО «под ключ» может превысить 3 млн. руб.

### Оценка рисков проекта ЭДО

До начала любого проекта высшее руководство желает получить четкие оценки всех выгод и негативных последствий, иначе говоря, необходимо выполнить оценку рисков. Технологии ЭДО не являются исключением, и как любая новая технология сулят немалые преимущества, но и таят весьма значимые риски. На основании доступных материалов (например, 9-й практической конференции «Электронный документооборот», https://msbevents.com/review/9th-hr-docflow) и собственной экспертизы оценим негативные воздействия на бизнес-процессы компании для проекта кадрового ЭДО. В табл. 1 представлен фрагмент основных рисков ЭДО. В предоставленном примере видно, что наиболее значимым риском может быть потеря (умышленная или случайная) ключа ЭП, особенно, если носитель не был защищен паролем и был утерян (скомпрометирован) УКЭП руководителя, имеющего право подписи финансовых документов. Обработка рисков ЭДО выполняется по авторской методике в соответствии с требованиями стандартов ISO 31000, IEC 31010 и ISO/IEC 27005.

Пример таблиц для определения рангов вероятности наступления рисков и их последствий представлены в табл. 2 и табл. 3 соответственно. Матрица для определения значений риска по известным значениям вероятности и последствий представлена в табл. 4. Упомянутые выше таблицы для оценки рисков можно взять как типовые в указанных выше стандартах или адаптировать для каждого предприятия, исходя из собственных оценочных суждений о возможной вероятности и допустимом ущербе при наступлении события риска. Преимуществом использования именно данных таблиц является возможность оперировать и качественным (столбец 3 в табл.2 и табл. 3) и количественными оценками (столбец 2) соответственно. Для определения значения риска по табл. 4 нужно перемножить соответствующие ранги (столбец 1) табл.2 и табл. 3 и получить числовое значение. Например, для события с вероятностью не чаще 1 раз в год (ранг 2 по табл. 2) и максимальным ущербом до 1 млн. руб. (ранг 4 по табл. 3) получим значение риска 8 (табл. 4), что соответствует уровню приемлемого риска. Конечно, при необходимости каждое предприятие может установить свои собственные шкалы и правила оценивания рисков исходя из принятых корпоративных регламентов.

### Сценарии применения сервисов ЭДО

До начала проектирования, разработки и внедрения полномасштабного проекта необходимо предложить высшему руководству технологические варианты реализации ЭДО, выбрать подходящие ИТ-компоненты, типы СКЗИ, типы ЭП и основные технологические операции. Соответственно для проекта ЭДО предлагаются три готовые сценария, основные параметры которых представлены в табл. 5. Предполагается использования СКЗИ «Крипто-Про»

*Таблица 1. Основные риски кадрового ЭДО (фрагмент)*

| № | Риск | Риск (ранг) | | | Существующие меры контроля | Кр | Обработка риска | Дополнительные меры | Остаточный риск | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | В | П | З | | | | | В | П | З |
| 1. | Отказ работника от подписи документа | 1 | 1 | 1 | - Технические (СКЗИ, уникальность УКЭП/НЭП, защита носителя), - Организационные (Регламенты, Политики, Инструкции) | 2 | Риск приемлем | | | | |
| 2. | Потеря ключевого носителя работником | 3 | 1 | 3 | - Технические (СКЗИ, уникальность УКЭП/НЭП, защита носителя), - Организационные (Регламенты, Политики, Инструкции) | 2 | Требуется обработка! | - Аудит ИБ, - Организационные меры (Расписки, инструктажи, тесты) | 2 | 1 | 2 |
| 3. | Фальсификация работником электронного документа | 1 | 1 | 1 | - Технические (СКЗИ, уникальность УКЭП/НЭП, защита носителя), - Организационные (Регламенты, Политики, Инструкции) | 2 | Риск приемлем | | | | |
| 4. | Повтор (исправление) работником | 1 | 1 | 1 | - Технические (СКЗИ, уникальность УКЭП/НЭП, защита носителя), - Организационные (Регламенты, Политики, Инструкции) | 2 | Риск приемлем | | | | |
| 5. | Обращение работника в суд с требованием признать / не признавать подписанный НЭП / УКЭП | 1 | 1 | 1 | - Технические (СКЗИ, уникальность УКЭП/НЭП, защита носителя), - Организационные (Регламенты, Политики, Инструкции) | 2 | Риск приемлем | | | | |

*В – вероятность риска, П – последствия риска, З – значение риска, Кр – критерий принятия риска*

*Таблица 2. Ранговые оценки для вероятности рисков*

| Ранговая оценка | Период времени | Описание вероятности |
|---|---|---|
| 0 | Не чаще 1 раза в 10 лет | Риск реализуется с крайне низкой вероятностью |
| 1 | Чаще 1 раза в 10 лет, не чаще 1 раза в 5 лет | Риск реализуется с минимальной вероятностью |
| 2 | Чаще 1 раза в 5 лет, не чаще 1 раза в 1 год | Риск реализуется с малой вероятностью |
| 3 | Чаще 1 раза в год, не чаще 1 раза в 6 мес. | Риск реализуется с вероятностью ниже средней |
| 4 | Чаще 1 раза в 6 мес., не чаще 1 раза в 1 мес. | Риск реализуется со средней вероятностью |
| 5 | Чаще 1 раза в 1 мес., не чаще 1 раза в неделю | Риск реализуется с достаточной вероятностью |
| 6 | Чаще 1 раза в неделю, не чаще 1 раза в день | Риск реализуется с большой вероятностью |
| 7 | Чаще 1 раза в день | Риск реализуется с высокой вероятностью |

*Таблица 3. Ранговые оценки для последствий рисков*

| Ранговая оценка | Значение последствий | Описание последствий |
|---|---|---|
| 0 | Негативные последствия практически отсутствуют | Негативные последствия крайне незначительны |
| 1 | Негативные последствия менее 100 тыс.руб. | Негативные последствия минимальны |
| 2 | Негативные последствия более 100 тыс. руб., менее 250 тыс. руб. | Негативные последствия малозначительны |
| 3 | Негативные последствия более 250 тыс. руб., менее 500 тыс. руб. | Негативные последствия ниже среднего |
| 4 | Негативные последствия более 500 тыс. руб., менее 1 млн. руб. | Негативные последствия средние |
| 5 | Негативные последствия более 1 млн. руб., менее 5 млн. руб. | Негативные последствия значительны |
| 6 | Негативные последствия более 5 млн. руб., менее 15 млн. руб. | Негативные последствия существенны |
| 7 | Негативные последствия более 15 млн. руб. | Негативные последствия критические |

*Таблица 4. Определение значения риска*

| Ранговая оценка последствий | Ранговая оценка вероятностей | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 | 0 | 2 | 4 | 6 | 8 | 10 | 12 | 14 |
| 3 | 0 | 3 | 6 | 9 | 12 | 15 | 18 | 21 |
| 4 | 0 | 4 | 8 | 12 | 16 | 20 | 24 | 28 |
| 5 | 0 | 5 | 10 | 15 | 20 | 25 | 30 | 35 |
| 6 | 0 | 6 | 12 | 18 | 24 | 30 | 36 | 42 |
| 7 | 0 | 7 | 14 | 21 | 28 | 35 | 42 | 49 |

*Риск приемлем, обработка не требуется*
*Риск значимый, постоянный мониторинг, обработка по плану*
*Риск неприемлемый, приоритетная обработка*
*Риск критический, немедленная обработка*

с алгоритмами ГОСТ (РФ) и RSA (зарубежный). Обязательно применяется сервис УЦ для проверки (валидации) УКЭП (РФ) и/или НЭП (зарубежный).

### Предложения по созданию международного значимого ЭДО

На основании подготовленных сценариев (табл. 5) в 2018 г. стартовал проект по созданию международного значимого ЭДО (МЭДО), целью которого было значительно ускорить передачу электронных документов в компании при обеспечении заданных требований по ИБ. Проект предусматривал

*Афоризмы пропускают подробности и выделяют главное: Это превосходная документация высокого уровня.*
Алан Перлис

постепенное вовлечение всех филиалов, в том числе и тех, которые находятся в иностранной юрисдикции, в единую защищенную корпоративную информационную систему ЭДО.

Первый этап этого проекта затрагивал создание ИТ-инфраструктуры на базе корпоративного решения 1С. Общая схема этого этапа создания МЭДО представлена на рис. 1. Краткое описание проекта: оператор обеспечивает внешние сервисы ЭДО на базе УКЭП (валидация через УЦ). Применяется только УКЭП на базе Крипто-про по алгоритмам ГОСТ. Внутренние сервисы ЭДО обеспечиваются на базе корпоративного решения 1С. Коричневым пунктиром показан путь для проверки (валидации) УКЭП, так называемые «цепочки доверия» - от пользователей до УЦ и далее до аккредитующего центра (Минкомсвязи в РФ). Отметим, что в РФ необходимо соответствовать требованиям ФЗ-476 от 27.12.2019, которые содержит значительные поправки в ФЗ-63 от 06.04.2011 «Об электронной подписи».

На втором этапе проекта МЭДО, который стартовал в ноябре 2020 г., создан полнофункциональный продукт корпоративного уровня. В развитие

*Таблица 5. Основные сценарии применения сервисов ЭДО*

| № | Локация контрагентов | Тип сертификата | Крипто-провайдер | УЦ | Описание технологических операций |
|---|---|---|---|---|---|
| 1 | Россия / Россия | УКЭП | CryptoPro CSP ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 | Аккредитованный УЦ в России (Минкомсвязь) | Подписание / шифрование документа. Используется УКЭП (ГОСТ). Используется Крипто-Про. Выполняется валидация УКЭП / УКЭП. |
| 2 | Россия / Мир Мир / Россия | УКЭП / НЭП | CryptoPro CSP ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 | Аккредитованный УЦ в России (Минкомсвязь) | Подписание / шифрование документа. Для обмена данными используется УКЭП, выданный аккредитованным УЦ в России (ГОСТ), Выполняется валидация УКЭП / НЭП. |
| 3 | Мир / Мир | НЭП / НЭП | CryptoPro CSP (экспортный вариант) или Microsoft CSP | Аккредитованный УЦ в России (Минкомсвязь) или Доверенный УЦ в периметре Компании в иной юрисдикции | Подписание / шифрование документа. Для обмена данными используется НЭП, выданный доверенным УЦ (RSA). У контрагента используется НЭП (RSA) и Microsoft CSP. Выполняется валидация НЭП (ГОСТ) / НЭП (RSA) |

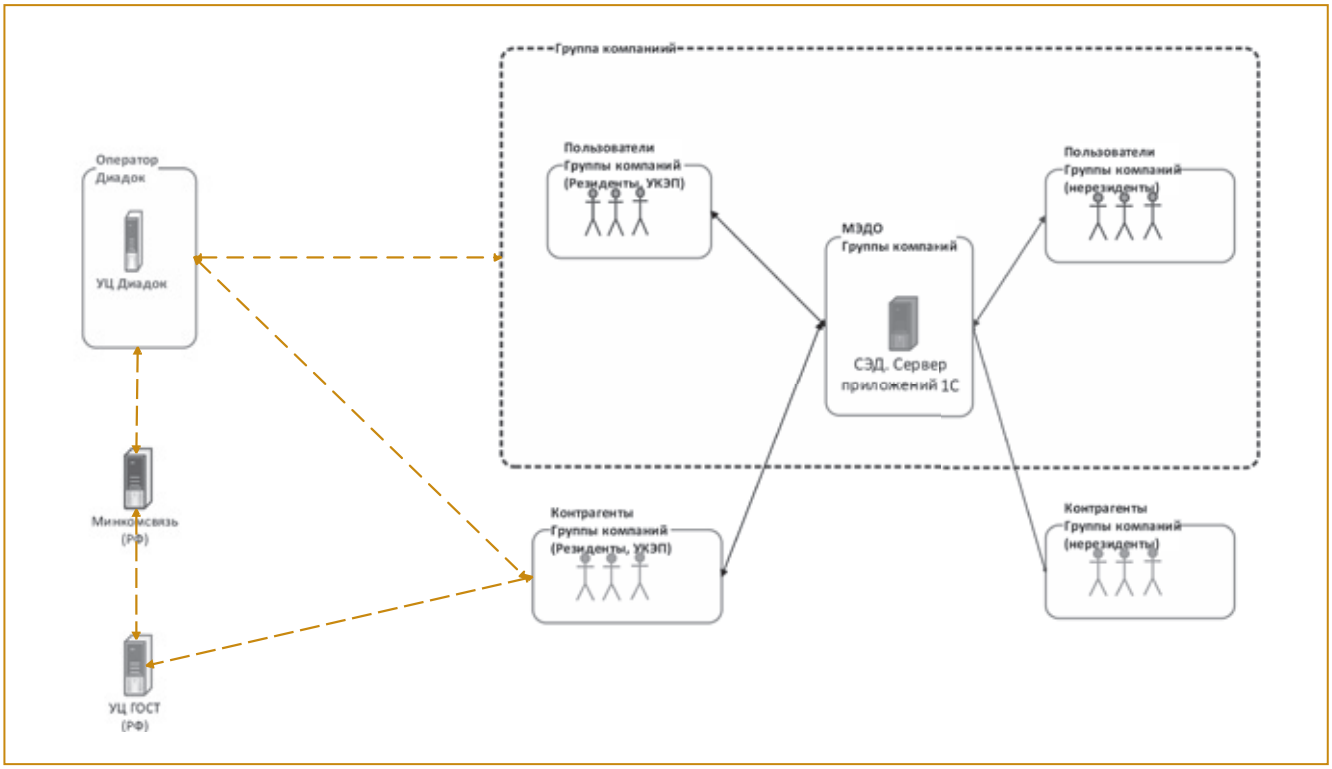


*Рис. 1. Схема первого этапа реализации МЭДО*

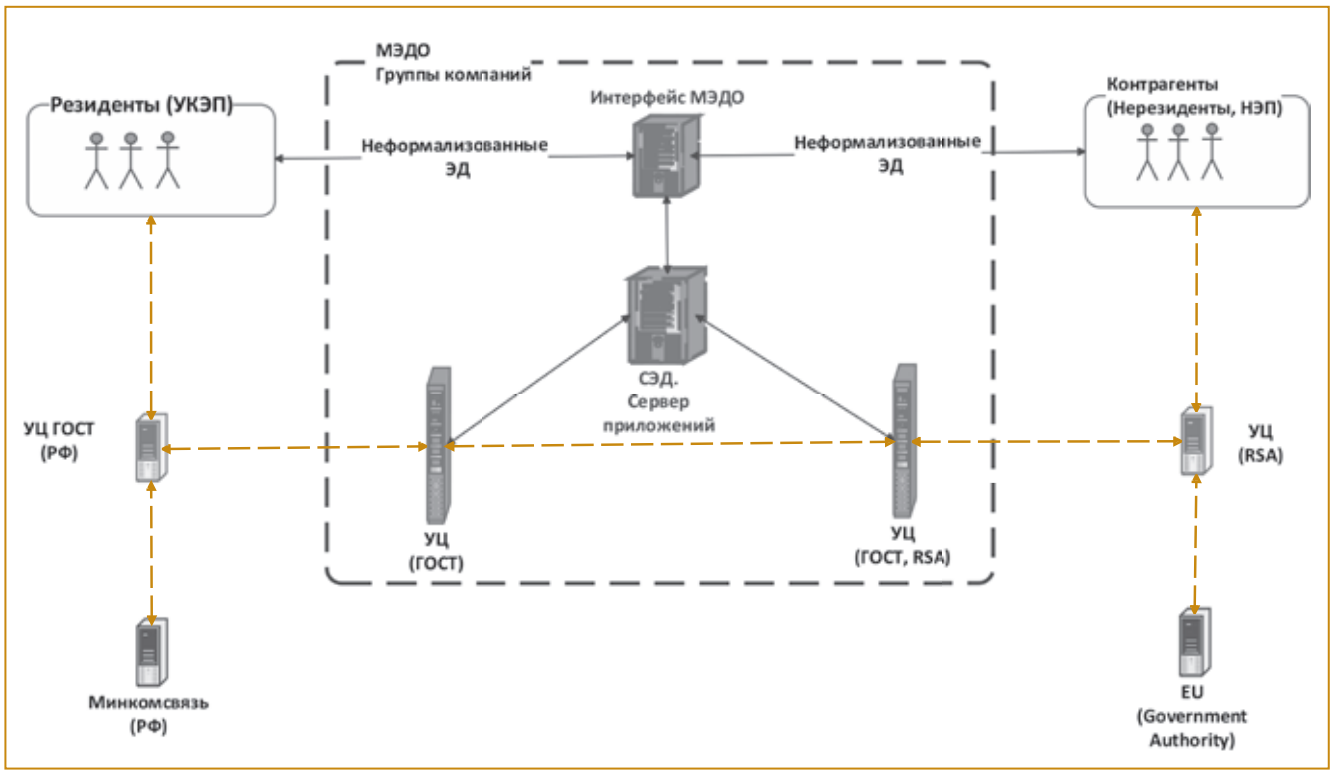


*Рис. 2. Схема второго этапа реализации МЭДО*

предыдущей схемы были реализованы сертификаты УКЭП и НЭП, несколько типов криптографических алгоритмов (ГОСТ и RSA), заложена реализация сервисов нескольких УЦ, имеющих соответствующую аккредитацию в РФ / в мире, разработаны механизмы устойчивости собственной ИТ-инфраструктуры сервисов МЭДО. Общая схема второго этапа МЭДО представлена на рис. 2.

На втором этапе проекта было принято решение не использовать ПЭП и сервисы ЕСИА. «Цепочки доверия» также показаны коричневым пунктиром, соответственно, обеспечивается валидация от УЦ

до аккредитующих центров (РФ и международного) с соответствующими юридическими полномочиями. Для практической апробации проекта МЭДО был выполнен полный цикл идентификации, оценивания и обработки рисков. Применялась методика, рассмотренная выше. Наиболее значимыми рисками МЭДО признаны потеря (умышленная или случайная) ключа ЭП, а также действия органов государственное власти – как прямое вмешательство, так и изменение локального законодательства. Два последних риска требуют постоянного контроля со стороны юристов, экспертов ИТ и служб ИБ.

Проблема обеспечения защиты корпоративных данных имеет важное значение в системе МЭДО, поскольку необходимо выполнять требования регламентов ИБ в разных юрисдикциях. Известно, что возможна ситуация, при которой сумма ущерба может значительно превосходить затраты на создание (модернизацию) корпоративной системы защиты информации (КСЗИ) [7, 8]. В ходе выполнения проекта МЭДО проводились оценки «степени зрелости» КСЗИ [9, 10].

### Результаты практической апробации МЭДО

Первый этап проекта МЭДО на базе «1С: Документооборот 8» признан проектом 2020 г. в Центральной и Восточной Европе по итогам 4-го международного конкурса партнерской сети «1С» (https://eawards.1c.ru/winners). Важным преимуществом является адаптация интерфейса для пользователей на английском и русском языках. Также была доработана функция мониторинга финансовых показателей, что позволяет отслеживать отклонения от плана в системе 1С.

Методика выполнения внутреннего аудита ИБ получила в 2019 г. диплом лауреата первой премии на Международном конкурсе научных, научно-технических и инновационных разработок, направленных на развитие топливно-энергетической и добывающей отраслей (https://www.technodevelop.ru/tek). На практике это позволило улучшить методы аудита ИБ, минимизировать потери при возникновении риска, а также повысить степень соответствия законодательным требованиям [11, 12].

### Заключение

В работе предложена новая схема обеспечения юридически значимого ЭДО, которая обладает рядом значительных преимуществ, прежде всего: современные риск-ориентированные стандарты, единая интеграционная платформа 1С, равнопрочная система «цепочек доверий» УЦ и ориентация на УКЭП/НЭП. Кроме того, важно отметить, что все этапы проекта юридически значимого МЭДО должную практическую апробацию. Представленные результаты могут быть востребованы в российских и международных компаниях, для которых реализация защищённого и безопасного ЭДО является не данью моде «цифровизации», а насущной технологической необходимостью.

### Список литературы


1. *Кильдеева С.С., Катасёв А.С., Талипов Н.Г.* Модели и методы прогнозирования и распределения заданий по исполнителям в системах электронного документооборота // Вестник Технологического университета. 2021. Т. 24. № 1. С. 79-85.
2. *Чарыева К.А., Байрамбердиев К.Б.* Важность электронного документооборота // Интернаука. 2021. № 5-1 (181). С. 17-18.
3. *Грудинина Е.А., Мкоян Г.В.* Оптимизация электронного документооборота на примере компании «Связьтранзит» // Бизнес-образование в экономике знаний. 2021. 1 (18). С. 32-35.
4. *Коробейникова К.В.* Защита конфиденциальной информации в ЭДО и архивном хранении // Защита информации. Инсайд. 2019. № 4 (88). С. 4-7.
5. *Сосина А.В., Шишина Ю.А.* Электронный документооборот и его безопасность // В сборнике: НАУКА И НАУЧНЫЙ ПОТЕНЦИАЛ - ОСНОВА УСТОЙЧИВОГО РАЗВИТИЯ ОБЩЕСТВА. Сборник статей Международной научно-практической конференции. 2018. С. 98-103.
6. *Власов А.Ю., Дмитричев А.С., Иванов А.С., Смирнов В.А., Турунов С.А., Чат Е.А.* Бифит ЭДО контрагенты. Свидетельство о регистрации программы для ЭВМ RU 2018617864, 03.07.2018. Заявка № 2018615043 от 18.05.2018.
7. *Брюховецкий К.А., Лившиц И.И.* Анализ влияния регламента General Data Protection Regulation на деятельность предприятий топливно-энергетического комплекса // Энергобезопасность и энергосбережение. 2020. № 5. С. 55-63.
8. *Лившиц И.И.* Оценка степени влияния General Data Protection Regulation на безопасность предприятий в Российской Федерации // Вопросы кибербезопасности. 2020. № 4 (38). С. 66-75
9. *Лившиц И.И.* Менеджмент рисков в области безопасности в топливно-энергетических компаниях // Стандарты и качество. – 2021. - № 1. – С. 42-48
10. *Лившиц И.И.* Аудит информационной безопасности объектов топливно-энергетического комплекса // Энергобезопасность и энергосбережение. – 2021. – № 1. – С. 5-12.
11. *Лившиц И.И., Соколов Е.О.* Проектирование международного значимого электронного документооборота для компаний холдингового типа // Вопросы кибербезопасности. 2020. № 5 (39). С. 61-68.
12. *Басырова А.А., Лившиц И.И.* Анализ методики аудита информационной безопасности предприятия с помощью аутсорсинговых компаний // Автоматизация в промышленности. 2020. № 7. С. 6-9.


***Лившиц Илья Иосифович*** *– д-р техн. наук, проф. практики, Университет ИТМО.*
*E-mail: livshitz.il@yandex.ru*