ПРОЕКТИРОВАНИЕ МЕЖДУНАРОДНОГО ЗНАЧИМОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ДЛЯ КОМПАНИЙ ХОЛДИНГОВОГО ТИПА

Лившиц И.И.[1], Соколов Е.О.[2]

Аннотация

Цель статьи: *изучение теоретических подходов и практических схем реализации международного значимого электронного документооборота и формирование предложений для проектирования таких сервисов для компаний холдингового типа.*

Метод исследования: *системный анализ современных подходов и практических схем реализации международного значимого электронного документооборота, в том числе, методов обеспечения доверия для компаний холдингового типа, действующих в различных юрисдикциях.*

Полученный результат.

Предложен эскиз схемы обеспечения международного значимого электронного документооборота для компаний холдингового типа, действующих в различных юрисдикциях. Показаны варианты обеспечения доверия к электронным сервисам, предоставляемых в различных локациях. Выявлены наиболее значимые риски информационной безопасности и предложены меры их снижения. Полученный результат может быть применим на практике для обеспечения юридической значимости электронных документов для трансграничного информационного обмена, в том числе для компаний, действующих в различных юрисдикциях.

Ключевые слова: *электронные сервисы, электронная подпись, удостоверяющий центр, компания холдингового типа, юрисдикция.*

DOI:10.21681/2311-3456-2020-05-61-68

Введение

В статье рассмотрены общие теоретические подходы реализации международного значимого электронного документооборота (далее – МЭДО), а также существующие доступные схемы реализации электронных сервисов МЭДО в Российской Федерации и в мире. С учетом существующих и перспективных потребностей для компаний холдингового типа, действующих в различных юрисдикциях, определены значимые риски информационной безопасности (далее – ИБ) и предложены меры для их снижения. В статье кратко изложены новации в законодательстве Российской Федерации об электронной подписи (далее – ЭП). С учетом существующих схем и юридических требований предложен эскиз схемы обеспечения МЭДО для компаний холдингового типа, действующих в различных юрисдикциях. Показаны варианты обеспечения доверия к электронным сервисам, предоставляемых в различных локациях. Полученный результат может быть применим на практике для обеспечения юридической значимости электронных документов для трансграничного информационного обмена, в том числе для компаний, действующих в различных юрисдикциях.

Нормативная база

Нормативная база для МЭДО, кратко может быть определена следующей основной совокупностью:

Федеральный закон № 63-ФЗ «Об электронной подписи», который определяет порядок получения и использования ЭП и обязанности участников обмена электронными документами (далее – ЭД);

Приказ ФНС России № ММВ-7-6/1096@ «О расширении электронного документооборота между налогоплательщиками и налоговыми органами в отношениях, регулируемых законодательством о налогах и сборах»;

Налоговый кодекс Российской Федерации, согласно которому налогоплательщик вправе направить документы в электронном виде в налоговый орган по телекоммуникационным каналам связи или через личный кабинет налогоплательщика (п. 2 ст. 93 НК РФ) и вправе выставлять счета-фактуры в электронной форме по взаимному согласию сторон сделки и возможностей для приема и обработки этих счетов-фактур в соответствии с установленным порядком (абзац 2 п. 1 ст. 169 НК РФ).

Юридическая значимость документа в нормативной базе Российской Федерации определяется по ГОСТ Р 7.0.8-2013 «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения». В частности, определены термины:

- юридическая значимость документа: свойство документа выступать в качестве подтверждения

1 Лившиц Илья Иосифович, доктор технических наук, доцент университета ИТМО, г. Санкт-Петербург, Россия. E-mail: Livshitz.il@yandex.ru

2 Соколов Егор Олегович, главный специалист отдела АСУ Gazprom International, г. Санкт-Петербург, Россия. E-mail: E.Sokolov@gazprom-international.com

деловой деятельности либо событий личного характера (п. 3.1 (14));
- электронный документооборот: документооборот с использованием автоматизированной информационной системы. (п. 3.2.2. (74));
- включение документа в систему электронного документооборота: Осуществление действий, обеспечивающих размещение сведений о документе и/или документа в системе электронного документооборота. (п. 3.2.2. (78)).

Следует принять во внимание, помимо Федерального закона № 63 в Российской Федерации принят Федеральный закон от 27.12.2019 N 476-ФЗ, который ввел новые термины. Для целей данной публикации отметим основные новации:
- доверенная третья сторона (далее – ДТС) – юридическое лицо, осуществляющее деятельность по проверке ЭП в ЭД в конкретный момент времени в отношении лица, подписавшего ЭД, для обеспечения доверия при обмене данными и ЭД и иные функции;
- метка доверенного времени – достоверная информация в электронной форме о дате и времени подписания ЭД ЭП, создаваемая и проверяемая ДТС, УЦ или оператором информационной системы и полученная в момент подписания ЭД ЭП в установленном уполномоченным федеральным органом порядке с использованием программных и (или) аппаратных средств, прошедших процедуру подтверждения соответствия требованиям.

Для целей МЭДО важно определить основные правила применения ЭП:
- в соответствии Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» ЭД, подписанные квалифицированной ЭП, всегда признаются равнозначными документам, подписанным собственноручно и могут применяться в любых правоотношениях в соответствии с законодательством Российской Федерации;
- ЭД, 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 ЭП, используемых для подписания документов бухгалтерского учета, должны быть установлены соответствующим федеральным стандартом, который на настоящий момент отсутствует;

Налоговый кодекс Российской Федерации признает только те ЭД, 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).

Кроме того, важной новацией в отношении признания иностранной ЭП Федеральным законом 27.12.2019 N 476-ФЗ определено:

ЭП, созданные в соответствии с нормами права иностранного государства и международными стандартами, признаются соответствующими признакам усиленной ЭП, и их применение в правоотношениях в соответствии с законодательством Российской Федерации осуществляется в случаях, установленных международными договорами Российской Федерации, при условии подтверждения их действительности аккредитованными ДТС, УЦ или иным лицом, уполномоченным на это международным договором Российской Федерации.

Решение ЭДО в России. Общий анализ

В настоящее время в Российской Федерации доступно значительное количество систем ЭДО, имеющих различный функционал [1 – 5]. За основу была взята реализованная ранее система ЭДО, а подготовительным этапом проекта была апробация ЭДО для российских компаний холдинга в 2019 году. Проект планировался с учетом развития под МЭДО и уже на начальной стадии позволял производить обмен ЭД в рамках единой информационной системы во всех странах присутствия подразделений компании холдингового типа. Данный проект ЭДО стал победителем конкурса «1С: Проект года» в номинации «Лучший региональный проект в Центральной и Восточной Европе» [6]. В дальнейшем реализованный ранее проект перед началом реализации дополнительного функционала и значительного развертывания в различных юрисдикциях прошел серьезную экспертизу по сравнению с имеющимися аналогами.

На первом этапе проекта МЭДО исходная совокупность существующих система прошла первую фильтрацию по системе критериев:
- систематизация работы с ЭД;
- подготовка документов по унифицированным (стандартным) формам;
- автоматическая классификация по различным параметрам;
- автоматизация поиска;
- осуществление рассылки и ознакомление с опубликованными ЭД;
- коллективный доступ к ЭД;
- использование централизованного хранилища для хранения ЭД и метаданных;
- формирование отчетов, в том чисел статистики;
- работа со списком персональных поручений.

После первого фильтра оставшаяся совокупность прошла финальное оценивания по следующим критериям:
- по степени интеграции с прикладным ПО;
- стоимость владения в пересчете на 1 документ в минимальном тарифе;
- режим работы службы техподдержки;
- минимальная стоимость интеграции с 1С в год;
- возможно работать с ЭП, выданной любым аккредитованным в Минкомсвязи УЦ.

В итоге среди лучших остались системы: Контур.Диадок, Taxcom, СБИС, Synerdocs, Калуга.Онлайн, Сфера. Курьер и eCom. В дальнейшем при выполнении эскизного проектирования МЭДО была выбрана одна из крупнейших систем, обладающая наилучшими показателями по всем критериям и предоставляющая требуемый список сервисов ЭП (в дальнейшем – Оператор). Необходимо отметить дополнительно, что при формиро-

вании финального решения по выбору Оператора были учтены риски, которые были подготовлены представителями службы безопасности, службы документооборота, а также юридического и технического департаментов. Детали формирования критерия оценки рисков основаны на «классических» стандарта ISO серии 31000 и ISO серии 27005 и не рассматриваются подробно в данной публикации.

Формирование технической задачи

Для компаний холдингового типа, действующих в различных юрисдикциях [7 – 8], реализация сервисов МЭДО должна поддерживаться серьезной технической инфраструктурой, в том числе с учетом перспективных технологий [9 – 13] и ограничений вычислительной мощности имеющейся серверной ИТ-инфраструктуры [14 – 16]. Также были подробно рассмотрены, в частности, специфические требования таможенного законодательства [17 – 18], электронного нотариата [19 – 20] и приложений e-Commerce [21 – 24]. Были сформированы основные требования для технической задачи Оператору, например:

- сервер Оператора имеет два интерфейса (внутренний и внешний), которые обеспечивают сервисы МЭДО для резидентов (Российской Федерации) и не резидентов (мир) на единой базе СКЗИ CryptoPro;
- сервисы МЭДО Оператора обеспечивают ЭП для произвольных типов ЭД от контрагентов (резидентов) до контрагентов (нерезидентов) и в обратном направлении;
- сервисы МЭДО Оператора обеспечивают логи по итогам анализа УКЭП от контрагентов (резидентов) и НЭП контрагентов (нерезидентов), подписанные УКЭП Оператора;
- интеграция внутренней ИТ-инфраструктуры и сервисов МЭДО Оператора должна быть максимально «бесшовной», ориентироваться на существующие корпоративные решения документооборота, бухгалтерии, финансовых приложений, средств защиты информации;
- реализация проекта должна обеспечивать максимальную возможность расширения функционала внутренней ИТ-инфраструктуры без критических взаимосвязей (взаимозависимостей) с сервисами МЭДО Оператора;
- реализация проекта должна в наибольшей степени сохранять реализованный нормативно-методический базис бухгалтерских (финансовых) приложений, учетную политику, внутренние регламенты ИБ;
- реализация проекта должна учитывать платформо-независимость и максимальную степень импортозамещения.

Общая схема построения МЭДО в соответствии со сформированной технической задачей представлена, обобщенно, на рис. 1.

На схеме не показан УЦ, подразумевается, что он включен в защищенную ИТ-инфраструктуру Оператора. Вопросы резервирования элементов критической ИТ-инфраструктуры Оператора и офисов компаний холдингового типа, действующих в различных юрисдикциях, не показаны. Предполагается обеспечение равной степени доверия для любого офиса компании холдингового типа в любой юрисдикции.

Эскизное проектирование

После формирования технической задачи на этапе эскизного проектирования были рассмотрены несколько вариантов реализации сервисов МЭДО с участием Оператора. Финальное обсуждение для компаний холдингового типа, действующих в различных юрисдикциях, проходили следующие варианты:

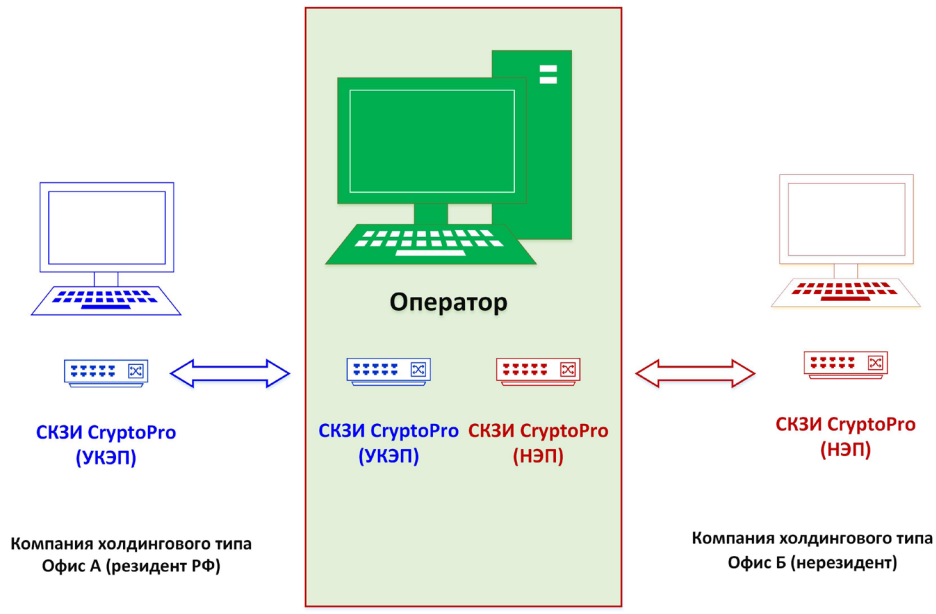

Рис. 1. Общая схема построения МЭДО

DOI:10.21681/2311-3456-2020-05-61-68

Вариант 1. Каждый контрагент оснащается СКЗИ CryptoPro (закупка через Оператора для резидентов – обычной версии, для нерезидентов – в экспортном исполнении). Информационный обмен протекает по единому технологическому режиму: СКЗИ CryptoPro и алгоритмы ЭП и/или шифрования – ГОСТ. «Цепочка доверия» устанавливается УЦ Оператора.

Вариант 2. Каждый контрагент (резидент) оснащается СКЗИ CryptoPro (закупка через Оператора), а для нерезидентов рекомендуется перечень СКЗИ, которые поддерживают зарубежные алгоритмы ЭП и/или шифрования (RSA, ECDSA). Информационный обмен протекает по комбинированному технологическому режиму: СКЗИ CryptoPro от резидентов до Оператора (ГОСТ) и от нерезидента до Оператора (RSA, ECDSA). Оператор играет роль ДТС, удостоверяя и УКЭП (ГОСТ) и НЭП (RSA, ECDSA). «Цепочка доверия» устанавливается УЦ Оператора.

Вариант 3. Каждый контрагент (резидент) оснащается СКЗИ CryptoPro (закупка через Оператора), а для нерезидентов рекомендуется перечень СКЗИ, которые поддерживают зарубежные алгоритмы ЭП и/или шифрования (RSA, ECDSA), дополнительно реализуется посредник «крипто-хаб», который оснащается СКЗИ CryptoPro (закупка через Оператора для нерезидентов – в экспортном исполнении). Информационный обмен протекает по комбинированному технологическому режиму: СКЗИ CryptoPro от резидентов до Оператора (ГОСТ), далее от Оператора до «крипто-хаба» и далее – от нерезидентов до Оператора (RSA, ECDSA). Теперь «крипто-хаб» играет роль ДТС, удостоверяя НЭП (ГОСТ) и НЭП (RSA, ECDSA). «Цепочка доверия» устанавливается от УЦ Оператора до «крипто-хаба», ЭП которого прослеживается до признаваемых мировых поставщиков (например, DigiCert, Sectigo и пр.).

Общая схема построения МЭДО для компаний холдингового типа на стадии эскизного проектирования представлена, обобщенно, на рис. 2.

На стадии эскизного проектирования дополнительно были изучены следующие аспекты:

- соответствие применимым требованиям различных юрисдикций в части ЭП;
- защита «одной степени прочности» для внутренних и/или внешних интерфейсов;
- ориентация на отечественные СКЗИ для формирования ЭП и/или шифрования;
- обеспечение мгновенного и безопасного обмена ЭД по установленным (резервным) каналам связи для всех офисов компании холдингового типа;
- разделение функций безопасности и администратора в периметре компании холдингового типа;
- обеспечение надежного и безопасного длительного архивного хранения ЭД (ДАХ).

Дополнительно следует отметить, что внимание к сервисам ДАХ в настоящий момент значительно возросло, поскольку сервисы МЭДО все больше получают практическое применение, при этом количество обрабатываемых ЭД может исчисляться миллионами. Исходя из результатов эскизного проектирования можно рекомендовать для построения систем ДАХ руководствоваться следующими нормативными документами:

- ISO 19005:1-2005 Document management — Electronic document file format for long-term preservation — Part 1: Use of PDF 1.4 (PDF/A-1) (на стадии пересмотра);
- ISO 11799:2015 Information and documentation — Document storage requirements for archive and library materials;
- ISO/TR 18492:2005 Long-term preservation of electronic document-based information (пересмотрен в 2013 и признан актуальным);
- ISO 15489-1:2016 Information and documentation — Records management — Part 1: Concepts and principles (пересмотрен в 2016 г.)

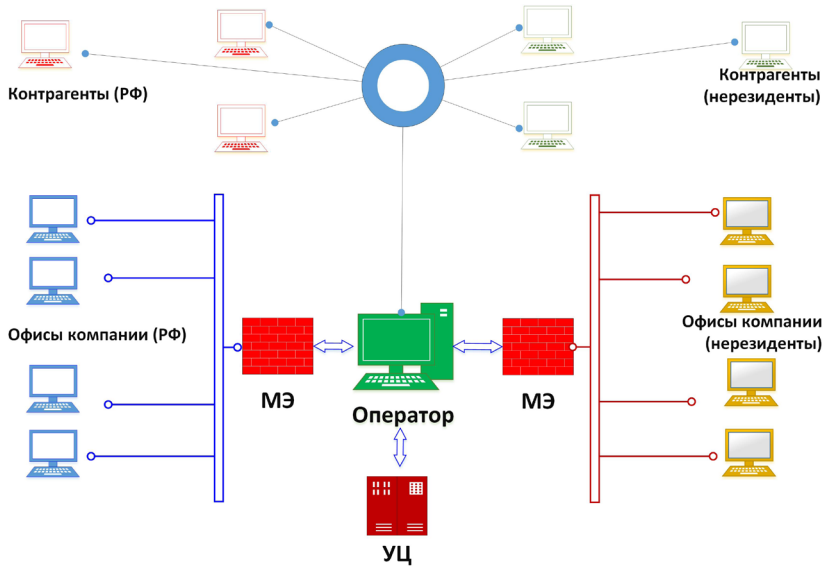

Рис. 2. Общая схема построения МЭДО для компаний холдингового типа

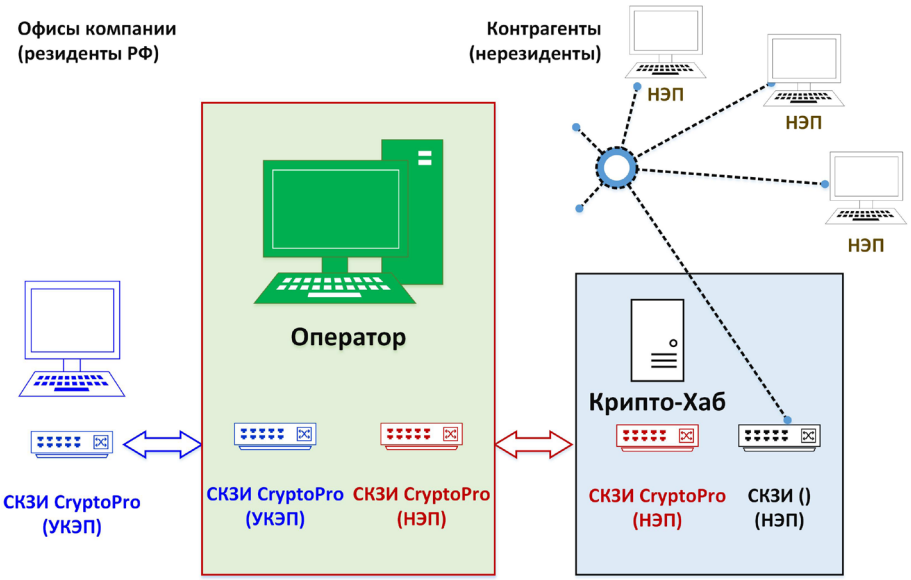

Рис. 3. Общая схема построения МЭДО для компаний холдингового типа с «крипто-хабом»

На этапе эскизного моделирования были идентифицированы, проанализированы и признаны значимыми следующие риски:

- корректное оценивание контекста ЭД для пользователей в разных юрисдикциях («*context*» подразумевается в нотации ISO как совокупность социальных, культурных, политических, правовых, регуляционных, финансовых, технологических, экономических и иных факторов на международном, национальном, региональном или местном уровнях);
- выявление актуальных угроз и количественная оценка рисков (в нотациях ISO, NIST, Cobit) для ИТ-инфраструктуры в периметре компании холдингового типа;
- полная и достоверная валидация оконечных устройств (установленное системное и прикладное ПО, средства защиты, двухфакторная аутентификация, СКЗИ и пр.);
- авторизацию доступа к сервисам МЭДО в периметре компании холдингового типа;
- обеспечение и восстановление устойчивости (*Resilience*).

Общая схема построения МЭДО для компаний холдингового типа на стадии эскизного проектирования в Варианте 1 с «крипто-хабом» представлена, обобщенно, на рис. 3.

Апробация

Апробация эскизного проекта прошла на XVIII международной конференции по проблематике инфраструктуры открытых ключей и электронной подписи PKI-Форум (https://ib-bank.ru/pki-forum/materials2020) в 2020 г. в рамках двух самостоятельных докладов, представленных авторами. В процессе дискуссии были обсуждены научные и научно-практические особенности проведённого эскизного этапа проекта и, в целом, получено одобрение сообщества ведущих экспертов в данной области.

Заключение

В данной работе проведен анализ правовых, организационных и технических аспектов обеспечения международного значимого электронного документооборота для компаний холдингового типа, действующих в различных юрисдикциях. Показаны варианты обеспечения доверия к электронным сервисам, предоставляемых в различных локациях. Выявлены наиболее значимые риски информационной безопасности и предложены меры их снижения.

Наиболее перспективной представляется схема по варианту № 3 с отдельным «крипто-хабом», которая обладает рядом важных преимуществ: гибкая и бесшовная интеграция со всеми корпоративными ИТ-системами, применением отечественных средств автоматизации, в том числе платформы 1С, и эффективных средств криптографической защиты информации, способных обеспечивать безопасный обмен документами в компании холдингового типа.

Полученный результат может быть применим на практике для обеспечения юридической значимости электронных документов для трансграничного информационного обмена, в том числе для компаний, действующих в различных юрисдикциях.

DOI:10.21681/2311-3456-2020-05-61-68

Литература

1. Корниенко А.А., Кустов В.Н., Станкевич Т.Л. Повышение эффективности службы доверенной третьей стороны // Защита информации. Инсайд. 2018. № 1 (79). С. 49-54.
2. Кустов В.Н., Станкевич Т.Л. Проблема операторов электронного документооборота // Защита информации. Инсайд. 2017. № 4 (76). С. 20-24.
3. Лившиц И.И. К вопросу оценки соответствия сервисов ДТС требованиям информационной безопасности на основе ISO 27001 // Оборонный комплекс - научно-техническому прогрессу России. 2016. № 1 (129). С. 7-14.
4. Лившиц И.И. К вопросу оценки соответствия электронных сервисов требованиям информационной безопасности на основе стандарта ISO 27001 в таможенном союзе / Лонцих П.А., Лившиц И.И. // Вестник Иркутского государственного технического университета. 2015. № 11 (106). С. 229-234.
5. Лившиц И.И. К вопросу оценки результативности при внедрении систем менеджмента информационной безопасности // Оборонный комплекс - научно-техническому прогрессу России. 2015. № 2 (126). С. 3-9.
6. Лучший региональный проект в Центральной и Восточной Европе. 1С:Проект года https://eawards.1c.ru/projects/vnedrenie-sistemy-elektronnogo-dokumentooborota-sed-na-baze-1s-dokumentooborot-8-v-gazprom-ep-international-bv-82950.
7. Лобанова А.М. Юридическая сила и юридическая значимость документа. Методологические аспекты нормативности и системности понятий // Вестник ВНИИДАД. 2020. № 3. С. 41-57.
8. Кузнецов А.К. Изменение законодательства об электронной подписи: Основные положения // Право и практика. 2020. № 2. С. 188-193.
9. Конарев Д.И. Вопросы доверия в отсутствии третьей стороны в технологии блокчейн // В сборнике: Исторические, философские, методологические проблемы современной науки. Сборник статей 1-й Международной научной конференции молодых ученых. Ответственный редактор А.А. Горохов. 2018. С. 118-122.
10. Веселицкая П.Д., Кротова Е.Л. Применение технологии блокчейн в инфраструктуре открытых ключей // Инновационные технологии: теория, инструменты, практика. 2017. Т. 1. С. 227-229.
11. Tawfik A.M., Sabbeh S.F., EL-Shishtawy T.A. Secure multiparty computation for privacy preserving range queries on medical records for star exchange topology. International Journal of Computer Network and Information Security. 2018. Т. 10. № 3. С. 8-16.
12. Mubarakali A., Elsier O., Bose S.C., Srinivasan K., Elsir A. Design a secure and efficient health record transaction utilizing block chain algorithm. Journal of Ambient Intelligence and Humanized Computing. 2019.
13. Maslov D.V., Kiryanov A.E., Arefyeva I.E., Badalov A.B. ATD Internet marketing: the management for participants of the flight of a butterfly project. Навигатор в мире науки и образования. 2017. № 2 (35). С. 153.
14. Wang W., Li S., Du R., Dou J. Privacy-Preserving mixed set operations. Information Sciences. 2020. Т. 525. С. 67-81.
15. Tonyali S., Munoz R., Akkaya K., Ozgur U. A realistic performance evaluation of Privacy-Preserving protocols for SMART grid AMI networks. Journal of Network and Computer Applications. 2018. Т. 119. С. 24-41.
16. Giang Do.H., Keong Ng.W. Mult-Dimensional range query on outsourced Database with strong privacy guarantee. International Journal of Computer Network and Information Security. 2017. Т. 9. № 10. С. 13-23.
17. Романов К.О. Применение механизма доверенной третьей стороны при использовании электронной подписи в международном таможенном электронном документообороте // В сборнике: Актуальные проблемы развития таможенного дела в условиях современных глобальных изменений. Сборник материалов IX Международной научно-практической конференции. 2017. С. 167-170.
18. Вологдина Е.С. Интеграция информационных ресурсов как инструмент взаимодействия таможенных органов государств-членов ЕАЭС // Вестник Академии права и управления. 2019. № 3 (56). С. 16-20.
19. Кочкина О.В., Тябина Ю.А. Зарубежный опыт становления и функционирования электронного нотариата // Нотариус. 2020. № 5. С. 42-44.
20. Костина О.В., Костин А.А. Развитие нотариата в Евразийском экономическом союзе: проблемы и перспективы // Нотариус. 2017. № 1. С. 40-43.
21. Song B., Yan W., Zhang T. Cross-border e-Commerce commodity risk assessment using text mining and fuzzy rue-based reasoning. Advanced Engineering Informatics. 2019. Т. 40. С. 69-80.
22. Wei K., Li Y., Zha Y., Ma J. Trust, risk and transaction intention in consumer-to-consumer e-marketplace: an empirical comparison between buyer' and sellers' perspectives. Industrial Management & Data Systems. 2019. Т. 119. № 2. С. 331-350.
23. Sahid G.T., Mahendra R., Budi I. E-commerce merchant classification using website information. В сборнике: ACM International Conference Proceeding Series. 9. Сер. "Proceedings of the 9th International Conference on Web Intelligence, Mining and Semantics, WIMS 2019" 2019.
24. Aliev T.T., Bit-Shabo I.V. Legal regulation of e-Commerce and other entrepreneurial activities conducted with digital technologies. Advances in Intelligent Systems and Computing. 2020. Т. 1100 AISC. С. 807-813.

DESIGNING AN INTERNATIONALLY SIGNIFICANT ELECTRONIC DOCUMENT FLOW FOR HOLDING COMPANIES

Livshitz I.[3], Sokolov E.[4]

Abstract

The purpose of the article: *study theoretical approaches and practical schemes for implementing international significant electronic document flow and making proposals for designing any electronic services for holding companies.*

Research method: *Systematic analysis of modern approaches and practical schemes for implementing international significant electronic document flow, including methods for ensuring trust for holding companies operating in various jurisdictions.*

The result obtained: *the scheme for ensuring an internationally significant electronic document flow for holding companies operating in various jurisdictions is proposed. Options for ensuring trust in electronic services provided in various locations are shown. The most significant information security risks are identified and countermeasures to reduce them are proposed. This result can be applied in practice to ensure the legal significance of electronic documents for safety cross-border information exchange, including for companies operating in different jurisdictions.*

Keywords

international significant electronic document flow, electronic services, electronic signature, certification center, holding company, jurisdiction

References

1. Kornienko A.A., Kustov V.N., Stankevich T.L. Improving the efficiency of the trusted third party service // information Protection. Insider. 2018. No. 1 (79). Pp. 49-54.
2. Kustov V. N., Stankevich T. L. The Problem of electronic document flow operators // information Protection. Insider. 2017. No. 4 (76). Pp. 20-24.
3. Livshits I. I. On the issue of assessing the compliance of DTS services with information security requirements based on ISO 27001 // Defense complex - scientific and technical progress of Russia. 2016. No. 1 (129). Pp. 7-14.
4. Livshits I. I. On the issue of assessing the compliance of electronic services with information security requirements based on the ISO 27001 standard in the customs Union / Lontsikh P. A., Livshits I. I. // Bulletin of the Irkutsk State Technical University. 2015. No. 11 (106). Pp. 229-234.
5. Livshits I. I. On the issue of evaluating performance in the implementation of information security management systems // Defense complex - scientific and technical progress of Russia. 2015. No. 2 (126). Pp. 3-9.
6. Best regional project in Central and Eastern Europe. 1C:Project of the year https://eawards.1c.ru/projects/vnedrenie-sistemy-elektronnogo-dokumentooborota-sed-na-baze-1s-dokumentooborot-8-v-gazprom-ep-international-bv-82950
7. Lobanova A.M. Legal force and legal significance of the document. Methodological aspects of normative and systematic concepts // Bulletin of VNIIAD. 2020. no. 3. Pp. 41-57.
8. Kuznetsov A.K. Change of legislation on electronic signature: Fundamentals // Law and practice. 2020. No. 2. Pp. 188-193.
9. Konarev D.I. Questions of trust in the absence of a third party in the blockchain technology // In the collection: Historical, philosophical, and methodological problems of modern science. Collection of articles of the 1-st International scientific conference of young scientists. Responsible editor A. A. Gorokhov. 2018. Pp. 118-122.
10. Veselitskaya P.D., Krotova E.L. Application of blockchain technology in public key infrastructure / / Innovative technologies: theory, tools, practice. 2017. Vol. 1. Pp. 227-229.
11. Tawfik A.M., Sabbeh S.F., EL-Shishtawy T.A. Secure multiparty computation for privacy preserving range queries on medical records for star exchange topology. International Journal of Computer Network and Information Security. 2018. Т. 10. № 3. С. 8-16.
12. Mubarakali A., Elsier O., Bose S.C., Srinivasan K., Elsir A. Design a secure and efficient health record transaction utilizing block chain algorithm. Journal of Ambient Intelligence and Humanized Computing. 2019.
13. Maslov D.V., Kiryanov A.E., Arefyeva I.E., Badalov A.B. ATD Internet marketing: the management for participants of the flight of a butterfly project. Навигатор в мире науки и образования. 2017. № 2 (35). С. 153.
14. Wang W., Li S., Du R., Dou J. Privacy-Preserving mixed set operations. Information Sciences. 2020. Т. 525. С. 67-81.
15. Tonyali S., Munoz R., Akkaya K., Ozgur U. A realistic performance evaluation of Privacy-Preserving protocols for SMART grid AMI networks. Journal of Network and Computer Applications. 2018. Т. 119. С. 24-41.

3 Ilya Livshitz, Dr.Sc., AssociateProfessor of InformationTechnology Security at ITMO University, St.Peterburg, Russia. E-mail: Livshitz.il@yandex.ru

4 Egor Sokolov, Chief Specialist of Gazprom International, St.Peterburg, Russia. E-mail: E.Sokolov@gazprom-iinternational.com

DOI:10.21681/2311-3456-2020-05-61-68

16. Giang Do.H., Keong Ng.W. Mult-Dimensional range query on outsourced Database with strong privacy guarantee. International Journal of Computer Network and Information Security. 2017. T. 9. № 10. C. 13-23.
17. Romanov K.O. Application of the mechanism of a trusted third party when using an electronic signature in international customs electronic document management // In the collection: Actual problems of customs development in the context of modern global changes. Collection of materials of the IX scientific and practical International conference. 2017. Pp. 167-170.
18. Vologdina E.S. Integration of information resources as a tool for interaction between customs authorities of the EAEU member States // Bulletin of the Academy of law and management. 2019. No. 3 (56). Pp. 16-20.
19. Kochkina O.V., Tyabina Y.A. Foreign experience of formation and functioning of electronic notary // Notary. 2020. no. 5. Pp. 42-44.
20. Kostina O.V., Kostin A.A. development of notaries in the Eurasian economic Union: problems and prospects // Notary. 2017. No. 1. Pp. 40-43.
21. Song B., Yan W., Zhang T. Cross-border e-Commerce commodity risk assessment using text mining and fuzzy rue-based reasoning. Advanced Engineering Informatics. 2019. V. 40. Pp. 69-80.
22. Wei K., Li Y., Zha Y., Ma J. Trust, risk and transaction intention in consumer-to-consumer e-marketplace: an empirical comparison between buyer' and sellers' perspectives. Industrial Management & Data Systems. 2019. V. 119. № 2. Pp. 331-350.
23. Sahid G.T., Mahendra R., Budi I. E-commerce merchant classification using website information. В сборнике: ACM International Conference Proceeding Series. 9. Сер. "Proceedings of the 9th International Conference on Web Intelligence, Mining and Semantics, WIMS 2019" 2019.
24. Aliev T.T., Bit-Shabo I.V. Legal regulation of e-Commerce and other entrepreneurial activities conducted with digital technologies. Advances in Intelligent Systems and Computing. 2020. V. 1100 AISC. Pp. 807-813.