СХЕМОТЕХНИЧЕСКИЕ РЕШЕНИЯ ДЛЯ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ БЕЗОПАСНОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА. ЧАСТЬ 1. АНАЛИТИЧЕСКИЙ ОБЗОР

УДК 004.056::005.92

И.И. Лившиц, д.т.н., проф., ФГАОУ ВО «Национальный исследовательский университет ИТМО» (Санкт-Петербург, Россия), Livshitz.il@yandex.ru

Е.О. Соколов, ФГАОУ ВО «Национальный исследовательский университет ИТМО»

А.А. Лукьянова, ФГАОУ ВО «Национальный исследовательский университет ИТМО»

Вопросы практической реализации безопасного электронного документооборота приобретают в последнее время исключительно важное значение. Несмотря на доступность некоторых типовых решений, до сих пор имеются существенные неразрешимые системные противоречия, например, между обеспечением безопасности, удобства, интероперабельности, достоверности и пр. Большим разнообразием отличаются типы электронных подписей, применяемых в мире и в России, а также варианты их использования в самых различных информационных системах с несколькими заданными показателями доступности. Даже при условии формирования междисциплинарных рабочих групп (Международная организация по стандартизации, Европейское агентство по сетевой и информационной безопасности и пр.) не всегда удается создать действительно работоспособное и эффективное решение, удовлетворяющее все заданные потребности.
Целями настоящей статьи стали изучение общемировой и российской практики проектов электронного документооборота, а также исследование основных технических проблем их реализации. Приведены результаты анализа отечественных и зарубежных публикаций. Установлено, что до сих пор не представлено эффективное схемотехническое решение, обеспечивающее риск-ориентированный подход при практической реализации схем электронного документооборота для международного трансграничного взаимодействия.
Полученные результаты позволяют приступить к практическому построению систем электронного документооборота с заданным уровнем информационной безопасности для различных типов организаций.

КЛЮЧЕВЫЕ СЛОВА: ДОКУМЕНТ, ЭЛЕКТРОННЫЙ ДОКУМЕНТ, ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ, ЭЛЕКТРОННАЯ ПОДПИСЬ, ПРОСТАЯ ЭЛЕКТРОННАЯ ПОДПИСЬ, УСИЛЕННАЯ КВАЛИФИЦИРОВАННАЯ ЭЛЕКТРОННАЯ ПОДПИСЬ, СЕРТИФИКАТ, КРИПТОГРАФИЧЕСКИЙ АЛГОРИТМ, РИСК.

Важность и актуальность применения современных ИТ-компонентов не вызывает сомнений, особенно если предлагаемые технические решения позволяют обеспечить одновременно несколько конкурентных преимуществ. К последним традиционно относятся грамотная техническая реализация, функциональная полнота и поддержание заданного уровня информационной безопасности (ИБ). В полной мере такими современными ИТ-решениями, предоставляющими комплекс преимуществ, являются технологии электронного документооборота (ЭДО). Следует отметить, что в РФ и в мире реализуется множество проектов и чистого ЭДО, построенных на известных ИТ-компонентах (SAP, Oracle, HCL Notes (ранее – IBM Lotus Notes/Domino)), и сложных коммерческих систем, изначально созданных для иных целей, например электронного обмена данными (Electronic Data Interchange). Вопросы обеспечения ИБ в доступных на рынке решениях чистого ЭДО, как правило, решаются целиком или в большей степени за счет базовых ИТ-компонентов: систем управления базами данных (Oracle, IBM Db2 и пр.), операционных систем и т.д. Однако, исходя из практики, многие из них имеют свои собственные уязвимости (например, известные «обновления по вторникам» программных продуктов Microsoft Corporation). В частности, можно привести пример множественных

I.I. Livshits, DSc in Engineering, Professor, ITMO University (Saint Petersburg, Russia), Livshitz.il@yandex.ru
E.O. Sokolov, ITMO University
A.A. Lukyanova, ITMO University

Concept design solutions on implementing secure electronic document flow in practice. Part 1. Analytical review

Nowadays, challenges in implementing a secure electronic document flow have become of utmost importance. Though some generic solutions are available, in a consistent manner there are still significant unresolvable contradictions i. e. they imply assurance of security, usability, interoperability, reliability, etc. The electronic signatures introduced in Russia and around the world differ as well as their application in quite a wide range of information systems having multiple specified accessibility indicators. Although interdisciplinary task forces (e. g. International Organization for Standardization, European Union Agency for Cybersecurity, etc.) have been established, it is not always possible to create a truly functional and efficient solution to achieve the goals set.
This paper is aimed at studying both global and Russian practices in electronic document management as well as analysing the main technical challenges related to their implementation. We have reviewed Russian and foreign publications. It was found that so far there had been no effective concept design solution that delivered a risk-based approach when implementing electronic document work flows in international cross-border interaction.
Review outcomes will help to proceed with development of electronic document management systems based on a given level of cybersecurity for different types of enterprises.

KEYWORDS: DOCUMENT, ELECTRONIC DOCUMENT, ELECTRONIC DOCUMENT FLOW, ELECTRONIC SIGNATURE, BASIC ELECTRONIC SIGNATURE, ENHANCED QUALIFIED ELECTRONIC SIGNATURE, CERTIFICATE, CRYPTOGRAPHIC ALGORITHM, RISK.

уязвимостей даже при реализации хорошо известного и популярного стека TCP/IP в компании Siemens AG [1].

Выявленные противоречия (стоимость чистого ЭДО и дополнительных наложенных средств защиты информации (СЗИ) и (или) средств криптографической защиты информации (СКЗИ); баланс функциональной полноты и уровня ИБ; баланс удобства конечного пользователя и требований трансграничной передачи данных) потребовали применения нового схемотехнического решения. В представленной статье дается общий аналитический срез технической реализации некоторых наиболее известных зарубежных и российских проектов, показаны основные современные тенденции развития ЭДО.

Во второй части публикации будет описано новое схемотехническое решение, разработанное авторами. Оно обладает рядом значительных преимуществ, использует электронные подписи (ЭП) в соответствии с применяемым законодательством, построено на базе современных унифицированных требований и прошло несколько успешных этапов практической апробации. Представленные результаты могут быть востребованы в компаниях топливно-энергетического комплекса, для которых реализация защищенного и безопасного ЭДО представляет собой насущную технологическую необходимость в связи с новым курсом на импортозамещение всех применяемых технологий, в том числе используемых для обработки и защиты электронных документов (ЭД).

ОБЗОР ИЗВЕСТНЫХ В МИРЕ РЕШЕНИЙ ЭДО

Для Казахстана известны примеры цифровой трансформации, основанные на новых требованиях национального законодательства. В частности, в статье [2] дается обзор опыта использования ЭП и ЭД, описаны применяемые в этой сфере нормативные документы, а также расширения имеющейся практики на блокчейн, цифровые активы, цифровые токены, электронное правительство и пр. Имеются параллельные заключения о возможностях цифровой интеграции с РФ, поскольку экономические связи между странами весьма тесные. Отраслевая практика применения современных технологий рассмотрена в [3]. В этой публикации раскрыты актуальные проблемы и перспективы применения в Казахстане индустриального сертификата для защиты от участия в государственных закупках предприятий, не имеющих в наличии достаточного количества оборудования. Показано, что необходимо ориентироваться на единые технические регламенты Таможенного союза ЕАЭС. Предполагается, что практика выдачи индустриального сертификата, утвержденная Национальной палатой предпринимателей Республики Казахстан «Атамекен», обеспечит высокий уровень доверия и безопасности работы предприятий.

Для Германии можно также отметить ряд публикаций на указанную тему. В частности, в [4] приводится подробный обзор современных примеров применения ЭП (используется термин electronic signature, или e-signature), значительное внимание уделено важности роли оператора, занимающегося выдачей этих подписей (certification service provider). Весьма интересно сопоставление существующих мер защиты с уровнями защиты

биометрических систем идентификации. Представлены сведения о необходимости развертывания инфраструктуры открытых ключей (public key infrastructure – PKI) и основных направлениях европейской интеграции в области управления ЭП провайдеров в общих экономических процессах. Отдельная глава посвящена уязвимостям технологии ЭП, в частности недостаткам удостоверяющих центров (УЦ) и сложностям применения формальных процедур ИБ. Следует упомянуть, что в примерах успешной интеграции отмечаются такие страны, как Индия, Малайзия и РФ, причем приведено значительное количество ссылок на российские нормативные документы, в частности федеральные законы №152-ФЗ и 63-ФЗ.

В статье [5] анализируется развитие информационно-коммуникационных технологий в целях регулирования электронных сделок в Германии. Рассматриваются законы «О цифровой подписи», «Об общих условиях использования электронных подписей» и «Об оказании электронных услуг по идентификации и обеспечению надежности электронных операций на внутреннем рынке». Важно, что здесь подробно описан регламент ЕС №910/2014, утвержденный 23.07.2014, также известный как Регламент eIDAS (electronic IDentification, Authentication and trust Services). Представлено значительное количество примеров практики заключения электронных сделок с применением ЭП.

Публикация [6] посвящена общим вопросам внедрения системы доверия и, в частности, задачам создания доверенных сервисов для обеспечения безопасных глобальных транзакций. Отмечено, что известные проблемы использования ЭП весьма существенны при построении действительно глобальных процессов цифровых транзакций с установленными требованиями в области ИБ в соответствии с применяемым в Германии и ЕС законодательством.

В статье [7] представлена экспертиза двух наиболее известных европейских регламентов – eIDAS и General Data Protection Regulation (GDPR). Примечательно, что помимо подробного описания этих двух документов рассмотрены более ранние и менее известные проекты, в частности FIDIS и STORK. Проанализированы риски идентификации и классификации носителей персональных данных – материальных сущностей (чипов) и собственно информации как нематериального актива. В указанной статье приводятся также примеры иных качественных и содержательных аналитических отчетов, в частности Privacy and data protection by design – From policy to engineering (создан Европейским агентством по сетевой и информационной безопасности (ENISA)).

В [8] дается обзор существующих решений для Латинской Америки. Отмечается, что здесь одним из факторов риска развития цифровых технологий стало обострение криминогенной обстановки. Наиболее существенные изменения произошли в сфере использования биометрических данных – как статических (полученных человеком с рождения), так и динамических (меняющихся со временем). К приоритетным направлениям применения цифровых решений отнесены: пограничный контроль, объекты критической инфраструктуры, технологии ЭП и доступ к процессу выборов. Среди наиболее впечатляющих отмечены проекты по обеспечению 14 аэропортов Бразилии системами идентификации по лицу и выдаче электронных цифровых идентификаторов в Мексике. В последней реализованы электронные биометрические карты граждан (Voter ID), которые были успешно применены на выборах 2018 г. В указанной статье дается общее описание используемых в Латинской Америке технологий, в том числе ЭП (табл.).

Авторы [9] рассматривают практику установления экономических и дипломатических коммуникаций России и Вьетнама на уровне стратегического сотрудничества. В статье дано описание требований и условий формирования пространства доверия, в том числе и в таких важных областях, как экономика, национальная безопасность и оборона. В [10] представлены решения цифровой суверенной идентичности (self-sovereign identity) и иные решения, применяемые для обеспечения успешного функционирования безопасных сервисов электронного правительства (e-government). Подчеркивается, что значительные негативные факторы риска, в том числе пандемия коронавирусной инфекции Covid-19, вызвали повышенный интерес к развитию новых безопасных цифровых сервисов. В статье уделяется достаточно внимания формальным требованиям к доверенным сервисам eIDAS. Представлены инновационные решения для создания служб федеративного управления идентификационными данными (federated identity management). Очень важно для целей обзора, что в указанной статье дается раздел оценки соответствия (Compliance) с учетом международных стандартов ISO/IEC 29115. Уровень соответствия предполагается определять как степень уверенности (level of assurance), в том числе в процессах безопасной аутентификации. Помимо упомянутых ISO/IEC 29115, авторы [10] рекомендуют принять во внимание требования стандарта NIST Special Publication 800-63B.

Отдельная часть статьи W. Gao и L. Yang [11] посвящена практике различных стран в области применения конкретных решений цифровой идентификации, ЭП и цифровых сертификатов. Например, рассматриваются кластеры скандинавских стран (Швеция, Норвегия и Финляндия), где широко используются BankID, Buypass, Commfides и др., балтийских (Эстония, Латвия и Литва), в которых имеются цифро-

Сферы применения средств электронной идентификации в Латинской Америке [8]
Applications of electronic identification means in Latin America [8]

Страна Country	Технология Technology					
	ПК BC	ЭДГУ EAPS	ДКИИ CIIA	ЭДКУ EACS	ЭЦП EDS	ДИП EPA
Бразилия Brazil	+	–	+	–	–	–
Венесуэла Venezuela	+	–	–	–	–	–
Колумбия Colombia	+	–	–	–	–	–
Мексика Mexico	+	–	+	+	–	+
Перу Peru	+	+	+	+	–	–
Уругвай Uruguay	+	+	+	+	+	–
Чили Chile	+	+	+	+	+	–

Примечание. ДИП – доступ к избирательному процессу; ДКИИ – доступ к критической информационной инфраструктуре; ПК – пограничный контроль; ЭДГУ – электронный доступ к государственным услугам; ЭДКУ – электронный доступ к коммерческим услугам; ЭЦП – возможность хранения и использования электронной цифровой подписи.
Note. BC – border control; CIIA – critical information infrastructure access; EACS – electronic access to commercial services; EAPS – electronic access to public services; EDS – e-signatures storing and using; EPA – election process access.

вые решения, например на базе блокчейна (называется инфраструктурой бесключевой подписи, или keyless signature infrastructure – KSI), идентификационных карт Mobiil-ID (используется аутентификация на основе SSL/TLS клиентских сертификатов), бесконтактных карт (contactless identity card) asmens tapatybes kortele, позволяющих создать публично доступные цифровые сервисы. В кластере стран Ближнего Востока весьма интересен пример ОАЭ. Здесь в 2017 г. был анонсирован проект цифровой идентификации на базе стандартов X.509, а также ISO/IEC 17799 в области ИБ.

В сфере современных технологий наиболее важными представляются квантовые вычисления и коммуникации. В этом направлении следует отметить работы [11, 12]. В них описываются новые подходы квантовых протоколов, которые смогут удовлетворять нескольким критериям, таким как полнота, надежность, конфиденциальность, верифицируемость, доступность получения и соответствие законодательным требованиям. Представлена краткая история протоколов для электронных выборов, начиная с предложенных Д.Л. Чаумом (1981), и рассмотрен ряд новых. Отдельное внимание уделяется вопросам оценки безопасности третьей стороны, методам верификации используемых ЭП и т.д. Шифрованию на эллиптических кривых посвящена статья [13], в которой рассматриваются задачи обеспечения ИБ в широком смысле. Подробно описаны проблемы защиты информации от несанкционированных действий (unsanctioned access to information) для беспроводных сетей, в том числе вопросы обеспечения аутентификации и шифрования данных с помощью криптографической схемы цифровой подписи на основе эллиптической кривой (elliptic curve digital signature algorithm – ECDSA).

Общие проблемы обеспечения ИБ в решениях международных приложений изложены в статье С. Уильямса «Overseas customers want to shop online in their native language» (2014). В ней представлена информация о том, что для более широкого продвижения сервисов различных мировых поставщиков (рассматриваются примеры Toshiba Corporation, Apple Inc., Microsoft Corporation) в Германии и Франции важно обеспечить безопасность технологий электронной коммерции, в том числе корректный перевод, безопасные транзакции и снижение стоимости. Практические примеры применения технологии блокчейн рассматриваются в [14, 15]. В статье [16] показан пример схемы, которая предлагается для государственных служб и обеспечивает решение известной проблемы – согласования схем управления идентификации с PKI и квалифицированными сертификатами (qualified digital certificate), которые выдаются квалифицированными поставщиками услуг доверия (qualified trust service providers). Для этого предлагается модель архитектуры, показанная на рис. 1.

Представленная схема позволяет предприятиям и государственным службам использовать

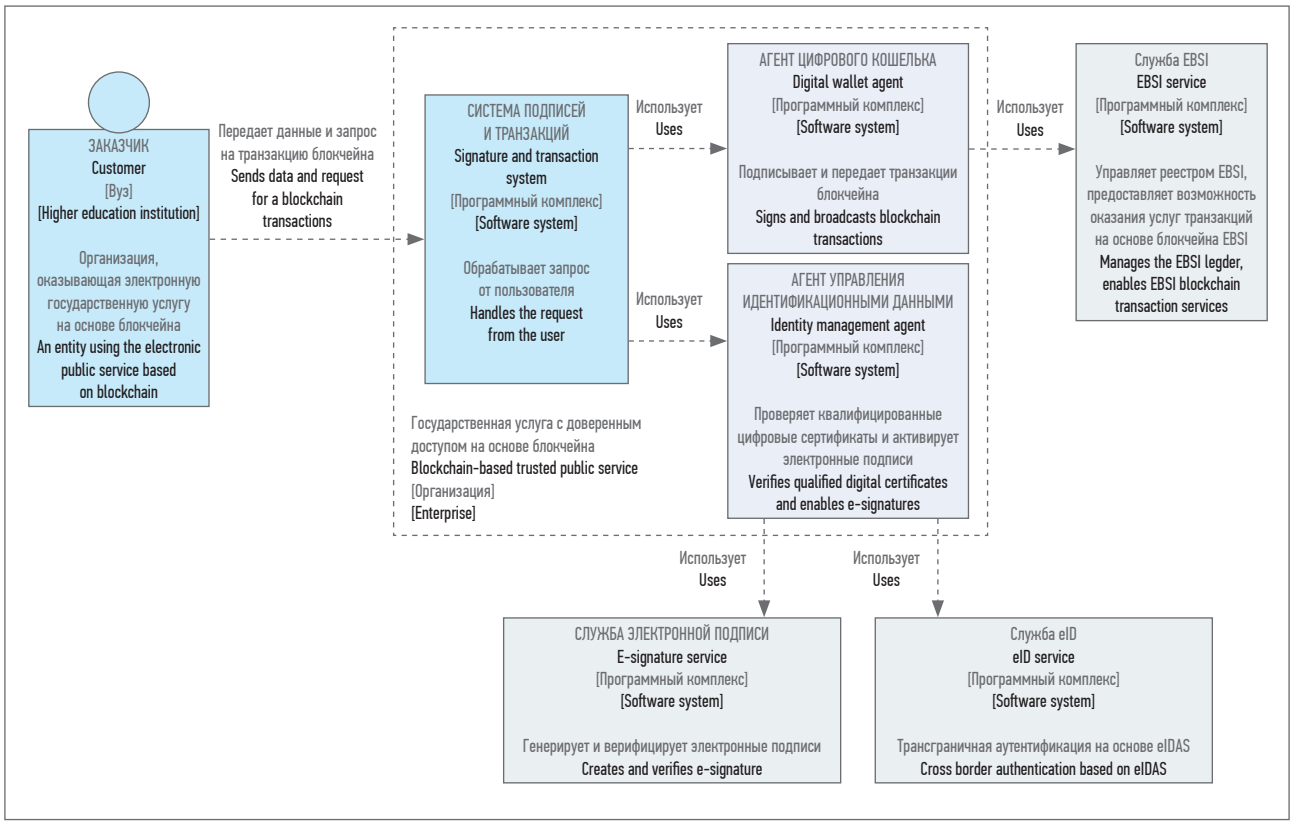


Рис. 1. Схема системного ландшафта эталонной модели архитектуры [14], где EBSI – Европейская сервисная инфраструктура блокчейна
Fig. 1. System landscape of the reference architecture pattern [14], where EBSI – European Blockchain Services Infrastructure

технологию блокчейн путем интеграции усиленных квалифицированных электронных подписей (УКЭП) с транзакциями. Помимо собственно функций УКЭП, провайдер должен обеспечить и иные опции, например электронный нотариат, выдачу дипломов, европейскую цифровую суверенную идентичность, функции цифрового правительства. Необходимо, чтобы все это было совместимо с eIDAS. Подобная инфраструктура получила наименование «Европейская сервисная инфраструктура блокчейна» (European Blockchain Services Infrastructure – EBSI). В статье также приводится пример выдачи диплома вуза.

В [15] рассматриваются вопросы баланса преимуществ и недостатков известных блокчейн-схем, в частности прозрачности транзакций и криптографической стойкости против доверия третьей стороне. Проведенное исследование показало, как сравнить уровни доверия и возможных потерь применительно к различным причинам возникновения ущерба.

Согласно отчету [15] при разработке новых схем, основанных на технологии блокчейн, необходимо учитывать не только вычислительное доверие, но и более общую экосистему, в которой оно играет важную роль. В ряде публикаций рассмотрены вопросы создания сервисов для безопасных транзакций с применением ЭП/УКЭП в различных отраслях: топливно-энергетической, обучения и управления качеством и пр. В [16] приведен пример сервисной платформы, которая предоставляет услуги для приложений в электроэнергетике, таких как торговля электроэнергией и подписание электронных контрактов с помощью ЭП (рис. 2).

Промежуточное программное обеспечение и поставщик услуг сертификации обеспечивают взаимодействие между приложением и цифровым сертификатом. Нижний уровень платформы состоит из сервисов шифрования, проверки ЭП, системы временных меток и совместных вычислений. Здесь же находятся хранилище данных, служба кэширования и серверное оборудование.

В [17] представлены некоторые размышления авторов относительно аспектов обеспечения ИБ и, прежде всего, конфиденциальности для приложений электронного обучения (e-learning). Отмечается, что хорошо известная триада «конфиденциальность, целостность и доступность» должна быть расширена за счет новых свойств, таких как аутентификация, авторизация, подтверждение происхождения. Для решения данной проблемы предлагаются известные криптографические функции на базе алгоритмов Rivest – Shamir – Adleman (RSA), Advanced Encryption Standard, Data Encryption Standard, ECDSA и, что особенно примеча-

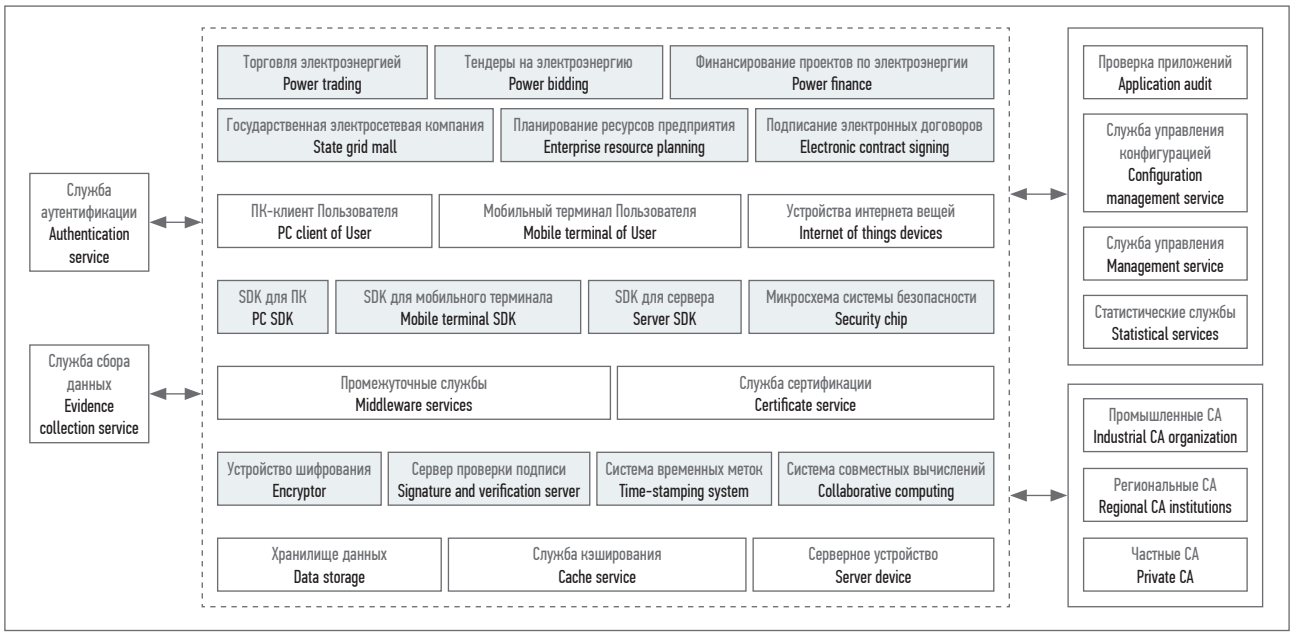


Рис. 2. Общая архитектура платформы обслуживания электронной подписи [16], где CA – поставщик услуг сертификации; SDK – комплект для разработки программного обеспечения
Fig. 2. Common architecture of e-signature service platform [16], where CA is a certified authority; SDK – software development kit

тельно, российского стандарта ЭП – ГОСТ 34.311–95. Конечно, можно обратить внимание, что сейчас действует ГОСТ 34.10–2018, но данную неточность допустимо отнести на аккуратность иностранных авторов.

В статье [18] представлен подробный отчет о реализации в странах Африки новых технологий, основанных на современных стандартах качества, системах сопоставления и оценки (benchmarking), что позволяет обеспечить быстрое внедрение новых сервисов. Основное внимание уделено различным функциям качества относительно применяемых технологий сбора данных, выполнения аналитических отчетов. Это в конечном итоге подразумевает существенное улучшение жизни для населения рассматриваемого кластера стран.

Далее приведено несколько примеров реализации хорошо известных сервисов в новом цифровом формате. В РФ, в частности, работает государственная почтовая сеть [19]. Представлено описание, как на современном этапе ее развития трансформируются традиционные формы передачи документов через АО «Почта России» с заполнением вручную типовых стандартных форм и передачей нарочно получателю. Внедрение системы ЭДО, как предполагается, позволит заполнить ЭД, далее подписать его ЭП/УКЭП в целях защиты и доставить до адресата в кратчайшие сроки. Предполагается также, что новая система будет иметь гибкий характер, и без привлечения сотрудников АО «Почта России» станет возможно отправить секретную документацию. В публикации [20] представлены новые характеристики системы ЭДО для нужд российских таможенных органов. Описаны особенности взаимодействия с ними участников внешнеэкономической деятельности, приведены основные субъекты ЭДО в данной сфере. Перечислены приоритетные направления совершенствования системы ЭДО в таможенных органах.

Вопросам выполнения регулятивных требований посвящены публикации [21, 22], в которых рассматриваются функции новой системы управления электронной идентификацией (eIDM). После внедрения она сможет принять на себя управление аутентификацией в государственных онлайн-службах Великобритании. Отмечается, что это будет первая система eIDM, в которой обеспечено соответствие Регламенту eIDAS. Рассматриваются также аспекты проектирования систем электронной идентификации (eID), основанные на принципе GDPR «Защита данных по замыслу». Весьма интересно, что авторы двух указанных публикаций уверены: различные типы архитектур могут привести к снижению уровня защиты данных.

В этом же ключе можно рассмотреть и статью [23], в которой исследуется технология смарт-контрактов в аспекте соответствия требованиям Регламента eIDAS. Для целей представленного обзора весьма важно отметить, что применение УКЭП признается эквивалентом заключения контрактов в бумажной форме с собственноручными подписями. Кроме того, в [23] рассматривается критерий доверия на соответствие требованиям eIDAS в отношении источника доверия в случае технологии распределенных реестров (distributed ledger technology), которая сама по себе может не соответствовать принципу технологической нейтральности.

Продолжая тему обеспечения ИБ в соответствии с регуляторными требованиями ЕС, можно отметить, например, Резолюцию A8–0189/2018 [23, 24]. В соответствии с ней странам – членам ЕС необходимо усилить свою защиту от кибератак со стороны государственных и негосударственных субъектов. Следует обратить внимание, что при голосовании «за» было 476 голосов, «против» – 151, «воздержался» – 36. Это может косвенно указывать на определенный интерес к политически мотивированным и поддерживаемым (явно или неявно) другими государствами кибер-атакам [1]. Известно об инициативе президента Франции Э. Макрона подписать Парижское соглашение в контексте Парижского форума мира для повышения доверия и безопасности в кибер-пространстве [1]. Следует снова обратить внимание, что не все государства готовы к заключению подобных договоров. В частности, США, Китай и еще около 50 других стран его не подписали. Такие политические заявления означают серьезные риски, как сказал Э. Макрон, «стать цифровой колонией США или Китая» [25].

Применительно к обеспечению ИБ для доверенных сервисов можно отметить, что в рамках работы CEN/TC 224 был утвержден окончательный вариант стандарта EN 419241–1–2018 «Надежные системы, поддерживающие подписывание сервера – Часть 1: Общие требования к безопасности системы». Ожидается разработка второй части этого документа – «Профиль защиты для доверенного модуля создания подписи». Внимание к профилям защиты можно признать значимым признаком общей стандартизации в соответствии с хорошо известным документом ISO/IEC 15408 (Common Criteria), принятым в России как ГОСТ Р ИСО/МЭК 15408–2013.

Сайт ENISA проинформировал о публикации отчета, в котором анализируются стандарты, относящиеся к поставщикам услуг доверия, а также устанавливается соответствие между положениями существующих документов и требованиями европейского законодательства eIDAS об электронной идентификации и услугах в области доверия, в том числе об ЭП [26]. В отчете, с одной стороны, анализируются требования eIDAS, а с другой – имеющиеся в настоящее время стандарты [1, 26]. Такое сопоставление ориентировано на требования, содержащиеся в различных статьях Регламента eIDAS. По итогам анализа данного отчета можно сделать вывод, что, как правило, имеющиеся стандарты частично или полностью охватывают многие требования eIDAS [27].

Ряд публикаций посвящен исследованиям уязвимостей в электронных системах. В частности, известны уязвимости пакета eIDAS-Node, при реализации которых можно выдать себя за любого члена ЕС во время официальных транзакций [1]. Патч был выпущен для двух указанных выше типов уязвимостей в системе авторизации eIDAS, обнаруженных исследователями компании SEC Consult [28]. Весьма полезные аналитические данные предоставляет отчет ENISA [27]. Отмечается, что сравнение многих применяемых стандартов для обеспечения ИБ в европейских странах позволяет определить, какие требования наиболее релевантны, а какие не в полной мере коррелируют с системой стандартизации ЕС.

Оценку соответствия (conformity assessment) удобно применять для анализа различных ИТ-продуктов, разработанных в США и странах Европы. Признание такой сертификации очень ценно: в частности, американские (NSTISSP No. 11) и европейские (ENS (Испания), Регламент eIDAS, общий для всех стран – членов ЕС) постановления требуют, чтобы при закупке программного обеспечения в правительственные органы оно имело признанные во всем мире сертификаты (наиболее часто требуют именно Common Criteria). В некоторых отраслях промышленности Common Criteria может быть требованием для работы на рынке (identity certificate или e-passport) или по безопасности в рамках тендеров (банки, операторы мобильной связи и т.д.) [29].

Кроме общего формального соответствия весьма важно обеспечить и независимую оценку, например, при исследовании известных проблем ИБ. В этой области можно отметить практику оценивания компании Arbor Networks [30]. В [31] приводятся примеры оценки защищенности информационных систем от атак социальной инженерии и, в частности, описываются такие аудиторские практики, как предположения, что пользователь может просто перейти по ссылке, не думая о последствиях (stupidest action), предположения о полной или частичной осведомленности относительно реализованных мер по обеспечению ИБ и пр. Эти техники могут быть весьма полезны в силу удобства, простоты и высокой эффективности при оценивании распределенных компонент систем ЭДО, особенно при условии, что к ним имеют доступ работники с различным уровнем осведомленности в области ИБ и из разных юрисдикций.

Для определения степени защищенности наиболее критичного ИТ-компонента систем ЭДО – УЦ – представляется полезным обратиться к известным фактам. Прежде всего предлагается рассмотреть инцидент со взломом одного из крупнейших УЦ в Монголии [1] – MonPass CA. Хакеры внедрили бэкдор в клиент установки сертификатов [32]. Как показало расследование, публичный web-сервер MonPass CA был взломан восемь раз. Известно также о серьезном инциденте с УЦ в Нидерландах. По причине вступления в силу закона, позволяющего спецслужбам перехватывать трафик, нидерландский центр сертификации

(Staat der Nederlanden) оказался под угрозой исключения из списка доверенных организаций [1]. В частности, ст. 45.1. b упомянутого закона разрешает использование ложных ключей в сторонних системах для получения доступа к данным. Поскольку центр сертификации подконтролен Службе общей разведки и безопасности Нидерландов, предполагается, что предоставляемые им сертификаты не могут более считаться безопасными. Известны также инциденты с отказом в обслуживании при обработке SSL-сертификатов в Windows [1]. Эта уязвимость идентифицирована как CVE-2013-3869 и в системе Common Vulnerability Scoring System имеет средний рейтинг: 7.1 (AV:N/AC:M/Au:N/C:N/I:N/A:C/E:U/RL:O/RC:C).

Далее рассмотрен весьма интересный пример анализа действий, если инцидент в области ИБ все же произошел. Как указано в отчете [30], среди причин отказа от обращения в правоохранительные органы называют недостаток времени, низкую уверенность в эффективности расследований правоохранительных органов и особенности корпоративной политики (рис. 3). Кроме того, доступны комментарии в свободной форме от респондентов, которые не обращаются в правоохранительные органы. В частности, высказываются опасения по поводу изъятого оборудования и фиксируется, что это решение клиента.

Применительно к анализу доли зарегистрированных атак важно, что их количество на уровне приложений (application-layer attacks) за последние несколько лет практически не изменилось для большинства сервисов, таких как HTTP, DNS, SMTP и т.д. Однако наблюдается определенное увеличение атак на HTTPS (с 24 до 37 %). Эксперты полагают, что этот факт может указывать на то, что сервисы с применением технологий шифрования (в том числе ЭДО) подвергаются атакам на уровне приложений.

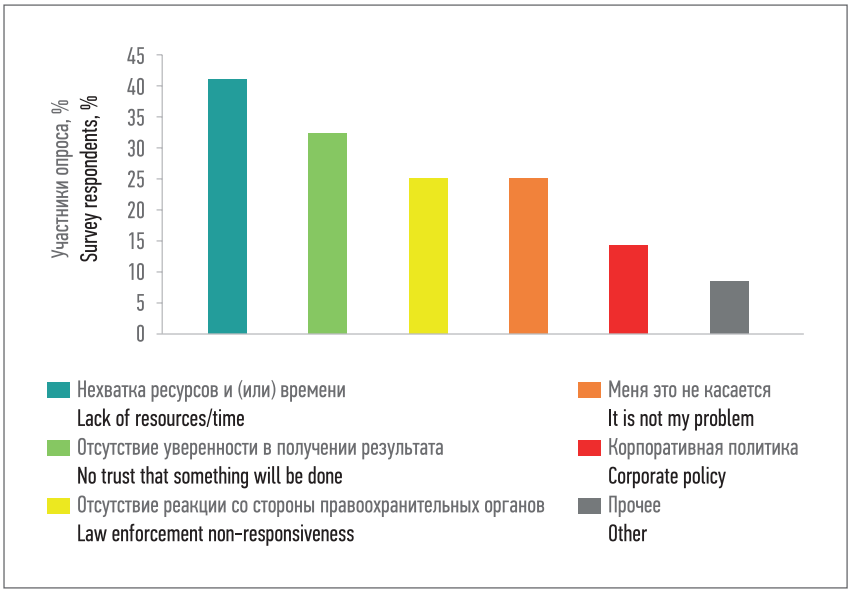


Рис. 3. Причины отказов от обращений в правоохранительные органы [21]
Fig. 3. Reasons for not contacting law enforcement agencies [21]

ПРИМЕРЫ ЭЛЕКТРОННЫХ СЕРВИСОВ

Имеется нидерландский сервис eHerkenning, выступающий средством верификации пользователя, а также инструментом, позволяющим обеспечить конфиденциальность обмена информацией. Это решение, как предполагается, сможет заменить системы различных государственных сервисов и, весьма вероятно, в ближайшем будущем станет единственным инструментом для безопасного удаленного взаимодействия. Как сообщается, eHerkenning позволяет взаимодействовать с более чем 500 различными поставщиками (среди которых, например, частные компании, муниципалитеты, налоговые органы и страховые организации). Кроме того, данный сервис соответствует европейским требованиям eIDAS [33]. При этом очевидно, что не всякая реклама достойна полного доверия. В частности, на сайте независимого источника [34] представлена карта покрытия eHerkenning в мире (рис. 4). Как можно видеть, основное (93,51 %) применение сервиса приходится на Нидерланды, и гораздо меньше он распространен в других странах. Очевидно, что вопросы интеграции с иными информационными системами, даже при допущении полного соответствия требованиям ЕС (eIDAS), – это, объективно, отдельная и большая задача.

Электронные сервисы ЭДО в РФ представлены весьма широко. На многочисленных научных и научно-практических конференциях (PKI-Форум, «РусКрипто», MSB, «Комплексная защита информации», ИБРР и пр.) традиционно заявляются несколько представителей, среди которых трудно объективно выделить самого безопасного и надежного оператора [35]. Помимо сервисов чистого ЭДО, многие предлагают и дополнительные опции. Например, чистый УЦ на базе ООО «Газинформсервис» [38] дополнительно предоставляет услуги доверенной третьей стороны [37] в соответствии с требованиями Федерального закона №476-ФЗ (рис. 5).

Другой известный российский оператор – АО «ПФ «СКБ Контур» [38] – предлагает динамический калькулятор экономии, позволяющий оперативно составлять приемлемый бюджетный план в зависимости от объема ЭД, обрабатываемых в установленный интервал. Кроме общих сервисов ЭДО, как основных, так и дополнительных (например, сервис

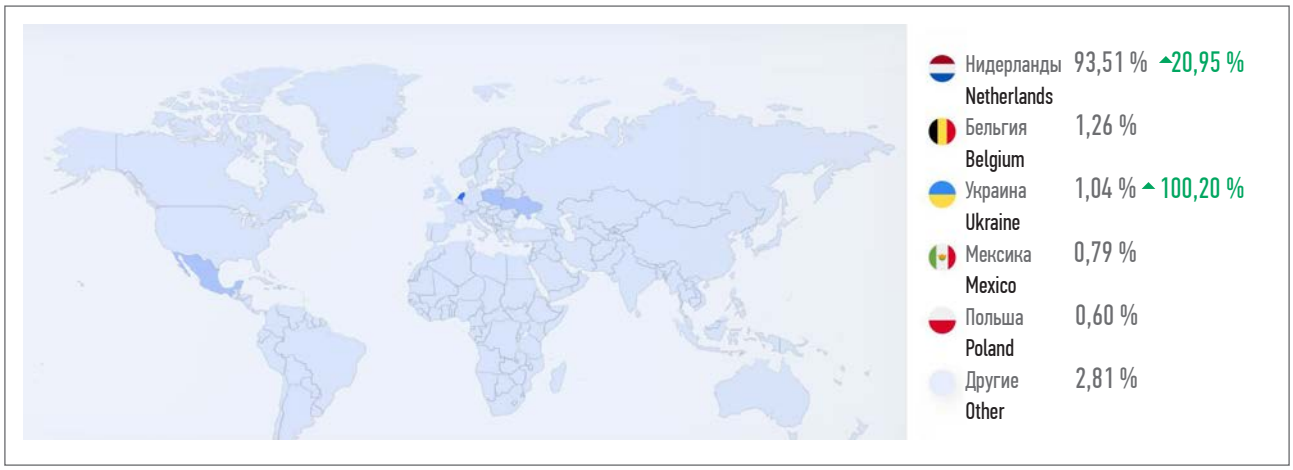


Рис. 4. Рейтинг и покрытие сервиса eHerkenning [34]
Fig. 4. eHerkenning rating and coverage [34]

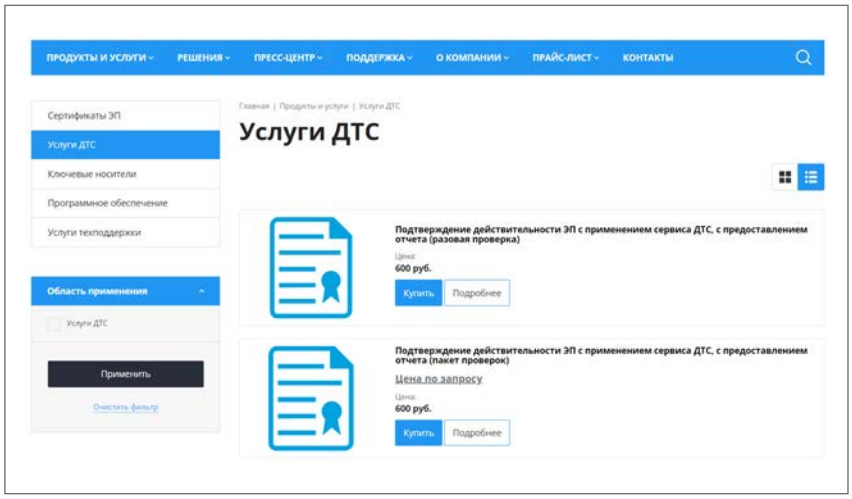


Рис. 5. Услуги доверенной третьей стороны в России [37]
Fig. 5. Trusted third party services in Russia [37]

выпуска сертификатов ЭП/УКЭП), имеются опции обеспечения ИБ. На сайте компании [39] размещена реклама, что «АО «ПФ «СКБ Контур» успешно прошло аудит состояния информационной безопасности системы юридически значимого электронного документооборота Диадок». Однако это заявление не содержит объективных свидетельств выполнения аудита ИБ по каким-либо международно признанным критериям, а просто информирует, что компания АО НИП «Информзащита» выдала свидетельство о том, что «Диадок соответствует высокому уровню защищенности и не содержит критичных уязвимостей информационной безопасности».

У конкурирующих провайдеров ЭДО нет даже такого сертификата, что в целом позволяет объективно оценить степень зрелости этого сегмента в РФ в отношении как общих финансовых сервисов (банки, лизинговые и страховые компании), так и специализированных (ЭДО, доверенной третьей стороны и пр.).

Имеется на российском рынке предложение специализированного сервиса и от другого известного отечественного провайдера ЭДО – АО «Калуга Астрал» [40]. Речь идет об аудите ИБ, который, как принято в международной практике, должен обеспечивать независимый, объективный и беспристрастный сбор доказательств с соблюдением самых строгих мер конфиденциальности. Несомненно, доверие к серьезным аудиторским компаниям стоит очень дорого и для определенных проектов играет важную и ключевую роль. При этом в мировой практике имеется несколько случаев компрометации данных очень известных аудиторов. Например, по сообщению The Guardian [41], взлом серверов компании Deloitte Touche Tohmatsu Limited (одна из аудиторских компаний «большой четверки») привел к утечке конфиденциальной переписки более 350 клиентов, среди которых ведомства США, ООН и крупнейшие транснациональные корпорации. В отношении аудиторов в РФ действуют такие же строгие правила, но на сайте АО «Калуга Астрал», кроме рекламной информации, не указан ни один из известных стандартов (ISO, ISO/IEC или ГОСТ Р серии 19011, 17021) или применяемых нормативно-методических документов Федеральной службы по техническому и экспортному контролю или ФСБ.

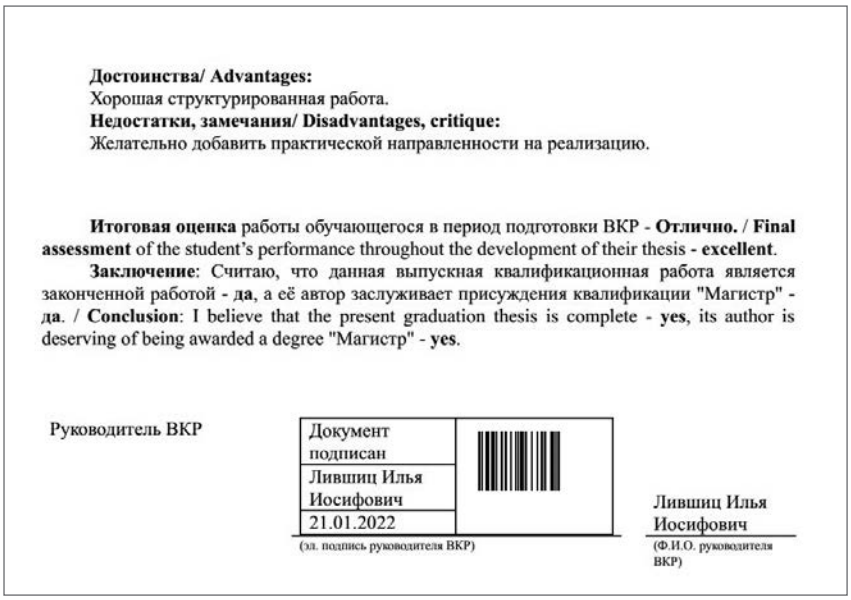
Еще один оператор – ООО «Такском» [42] – предлагает широкий спектр услуг как в области основного направления своей деятельности – ЭДО, сдача отчетности в цифровом виде, так и дополнительного – выдача ЭП, специальные предложения по решениям 1С, продажа USB-токенов, ветери-

нарные сертификаты и пр. Дается подробная информация по собственным сервисам ЭДО и возможности организации роуминга с другими операторами. В отношении обеспечения ИБ представлено достаточное количество сведений [42], однако вызывает определенное удивление использование старой терминологии (электронная цифровая подпись) в рамках отмененного федерального закона «Об электронной цифровой подписи», на смену которому пришел № 63-ФЗ с изменениями, принятыми согласно № 476-ФЗ.

Необходимо отметить, что 01.03.2022 была размещена информация о сотрудничестве АО «ИнфоВотч», специализирующегося в области ИБ, и ООО «Такском». В перечне совместных услуг и решений указано расследование инцидентов нарушения ИБ и злоупотребления доступом к конфиденциальной информации, что может быть интересно для предприятий малого и среднего бизнеса. Важно обратить внимание на аспект оснащения СЗИ: предполагается «частично решить задачи дорогостоящих средств защиты информации для решения проблем, связанных с ошибками персонала и действиями нелояльных сотрудников».

ИЗВЕСТНАЯ ПРАКТИКА ПРОЕКТОВ ЭДО

В настоящее время многие крупные компании заявили о выполнении ряда задач по цифровой трансформации, в том числе внедрении ЭДО. В частности, известны проекты ПАО «Сбербанк», ПАО «Ростелеком», X5 Group, ПАО «Газпром нефть» и некоторых других организаций [43–46]. Следует обратить внимание на значительное разнообразие всевозможных ИТ-систем, применяемых участниками – от классических тяжелых (SAP, Oracle и пр.) до известных российских решений – 1С и «Галактика ERP». Весьма интересно, что, по некоторым данным, проекты на базе 1С занимают до 53 % рынка, тогда


Достоинства/ Advantages:
Хорошая структурированная работа.
Недостатки, замечания/ Disadvantages, critique:
Желательно добавить практической направленности на реализацию.

Итоговая оценка работы обучающегося в период подготовки ВКР - **Отлично. / Final assessment** of the student's performance throughout the development of their thesis - **excellent**.
Заключение: Считаю, что данная выпускная квалификационная работа является законченной работой - **да**, а её автор заслуживает присуждения квалификации "Магистр" - **да**. / **Conclusion**: I believe that the present graduation thesis is complete - **yes**, its author is deserving of being awarded a degree "Магистр" - **yes**.

Руководитель ВКР

Документ подписан
Лившиц Илья Иосифович
21.01.2022
(эл. подпись руководителя ВКР)

Лившиц Илья Иосифович
(Ф.И.О. руководителя ВКР)

Рис. 6. Пример простой электронной подписи в приложении «ИСУ» Университета ИТМО
Fig. 6. Basic e-signature in ITMO University's ISU application

как на долю SAP и Oracle приходится только 22 и 3 % соответственно. Вызывает определенную обеспокоенность способность всех участников цифрового общения корректно запрашивать и проверять ЭП без участия технических сервисов безопасности, например УЦ. В определенной степени эти риски были изучены и рассмотрены в ряде публикаций [47–50]. Следует отметить, что многие разработчики пытаются защитить свою интеллектуальную собственность применительно к проектам чистого ЭДО и оформляют патенты и свидетельства. Так, имеются технические решения [51–53]. Рассматривая известные проекты, можно отметить ряд важных деталей и особенностей технологической реализации схем защищенного ЭДО.

ПАО «Газпром нефть». Известно, что при общей численности сотрудников примерно 75 тыс. в России работают около 71 тыс., но в проекте ЭДО приняли участие всего лишь около 100 человек только из центрального аппарата. К особенностям проекта компании можно отнести необходимость поддержки двух целевых шаблонов для 1С и SAP. Техническая реализация была выполнена на базе простой электронной подписи (ПЭП), предоставляемой Единой системой идентификации и аутентификации. В качестве примечания уместно обратить внимание, что в Национальном исследовательском университете ИТМО применение ПЭП позволяет удобно и оперативно подписывать выпускные работы студентов уже длительное время (рис. 6).

Проект *ПАО «Ростелеком»* ориентирован на использование УКЭП, которые выпускаются в необходимом количестве собственным УЦ. К особенностям можно отнести также незначительное количество типов ЭД (всего 23) и их невысокую долю (до 58 %) в общем объеме документов компании.

Статистика использования разных видов ЭП [54] дает интересные результаты. С большим отрывом среди приложений ЭДО лидирует ПЭП – до 79 %, далее идут УКЭП – 58 % и неквалифицированная электронная подпись (НЭП) – 16 % (при опросе допускалось несколько вариантов ответов). Этот факт подчеркивает технологическую уязвимость ряда проектов, поскольку скорость и стоимость реализации решений на базе ПЭП, безусловно, ниже, но в этом случае о безопасности говорить не приходится.

В аспекте ИБ весьма важно, как именно обеспечивается безопасное сопряжение многих компонентов программных продуктов, прежде всего иностранных решений (SAP, Oracle) и передачи чувствительных данных через шлюзы в федеральные органы исполнительной власти. Такие проблемы обсуждали представители компаний X5 Group и ПАО «ПИК СЗ», особенно с учетом большого количества внутренних проектов цифровой трансформации (совместное применение конструкторов 1С и системы ЭДО Tessa и др.).

К проблемным вопросам можно отнести также техническую реализацию НЭП/УКЭП в облаке (decision support system), двухфакторной аутентификации (решения F2A), механизмов принудительного периодического сброса паролей и иных эффективных мер. Однако нужно помнить и про баланс экономических интересов. Например, представители ПАО «ПИК СЗ» сообщали, что за 6 мес. выдали 2605 НЭП/УКЭП и подписали 2880 ЭД [54].

Следует отметить интересное решение, реализованное в ПАО «Сбербанк». Для систем длительного архивного хранения в компании применяется автоматическая технологическая ЭП, что обеспечивает заданный уровень доступности и целостности всего архива ранее подписанных документов.

ИЗВЕСТНЫЕ ПРОБЛЕМЫ ПРОЕКТОВ ЭДО

На основании доступных данных (материалов конференций MSB, PKI-Форум Россия 2021 [55], ИБРР-2021 [56]) можно определить основные технические проблемы реализации проектов ЭДО:

– работники не всегда видят маршруты движения ЭД, тем более не могут узнать, кто и какой подписью (ПЭП, НЭП или УКЭП) заверил конкретный тип документа;

– существует ориентация на сервис проверки ПЭП на сайте Министерства труда и социальной защиты РФ, что может привести к рискам корректной идентификации работника / его двойника, подписавшего (или отказавшегося от факта подписи) конкретный тип документа, поскольку ПЭП не предполагает использования доверенной и верифицируемой инфраструктуры УЦ;

– работники не смогут подписывать ЭД задним числом, что для многих организаций означает серьезные риски обрушения сервисов, связанных с применением ЭП;

– имеются проблемы интеграции большого набора разных ИТ-компонентов. SAP, Oracle, Lotus, 1С, различные порталы и пр. приводят к необходимости лоскутной автоматизации и ручного запуска многих процессов (в частности, в проекте ПАО «Ростелеком»);

– есть проблемы вовлеченности сотрудников в ЭДО (могут работать удаленно, не использовать НЭП/УКЭП, не выполнять установленные регламенты ИБ);

– не решена проблема подписи в разных юрисдикциях по разным протоколам и криптографическим алгоритмам (ГОСТ, RSA);

– не решена проблема многофилиальной сети, особенно в разных юрисдикциях.

ПРЕДМЕТНЫЕ ПРОБЛЕМЫ ПРОЕКТОВ ЭДО

Необходимо дополнительно отметить значительное количество специфических проблем при обеспечении ИБ в отношении чувствительной информации:

– передачи контента – как чисто технические, так и проблемы, присущие конкретным схемам работы (например, категории, логики, обновления процессов Use Case Management и Incident Management). Они подробно рассмотрены в докладе «Особенности передачи SIEM-контента. В Тулу со своим самоваром?», представленном на SOC-Форум 2021 [57];

– обеспечения совместимости с различными сертификациями и стандартами. Эти проблемы рассмотрены подробно в докладе «Дарвинизм безопасника: как приспособить SOC к эволюции корпорации», также представленном на SOC-Форум 2021;

– прохождения аудитов соответствия, в частности на соблюдение требований международного стандарта ISO/IEC 27001 и аудитов отраслевых регуляторов. Эти проблемы рассмотрены подробно в докладе «Практика построения гибридного SOC: внешний SOCaaS и собственный Open-Source», представленном на SOC-Форум 2021;

– общей оценки доверия, в частности, формирования реалистичных оценок возможностей существующих СЗИ/СКЗИ, прошедших в установленном порядке сертификационные испытания в системе ФСБ или Федеральной службы по техническому и экспортному контролю. Как отмечается в докладе «Опыт обеспечения кибербезопасности органов государственной власти в сервисной модели силами корпоративного центра ГосСОПКА», представленном совместно Министерством экономического развития РФ и Solar JSOC, необходимо принять во внимание возможности «обхода фактически любых СЗИ любых вендоров» для злоумышленников пятого уровня. Этот пример объективно свидетельствует об абсолютном риске убийцы проекта (kill project), при котором наступает техническая катастрофа.

ЗАКЛЮЧЕНИЕ

В статье представлен краткий обзор существующих подходов и примеров выполненных проектов в области ЭДО, показаны их основные преимущества и недостатки. Полученные результаты могут быть востребованы в компаниях топливно-энергетического комплекса, для которых реализация защищенного и безопасного ЭДО в соответствии с заданными требованиями ИБ представляет собой насущную технологическую необходимость. ■

ЛИТЕРАТУРА

1. SecurityLab.ru: информ. портал. URL: https://www.securitylab.ru/ (дата обращения: 10.08.2022).
2. Amangeldy A.A. Digital technologies incorporation into legislation of the Republic of Kazakhstan // European and Asian Law Review. 2021. Vol. 4, No. 1. P. 52–60.
3. Бейсекеев А.Е., Дубровин П.В., Темербаева М.В. Проблемы и перспективы применения индустриального сертификата в Республике Казахстан // Вестник инновационного Евразийского университета. 2021. № 2 (82). С. 64–71.
4. Blythe S.E. A critique of German e-commerce law and recommendations for improvement // Academic and Business Research Institute: офиц. сайт. URL: http://www.aabri.com/SA12Manuscripts/SA12045.pdf (дата обращения: 10.08.2022).
5. Жетибаев Ж.К. Правовое положение электронных сделок по опыту Германского государства // Вестник Института законодательства и правовой информации Республики Казахстан. 2020. № 3 (61). С. 201–207.
6. Hühnlein D., Frosch T., Schwenk J., et al. Futuretrust – future trust services for trustworthy global transaction // Proceedings of the Open Identity Summit 2016. Bonn, Germany: Gesellschaft für Informatik, 2016. P. 27–41.
7. Andraško J., Mesarčík M. Those who shall be identified: The data protection aspects of the legal framework for electronic identification in the Europe Union // TalTech Journal of European Studies. 2021. Vol. 11, No. 2. P. 3–24.
8. Минаев В.А., Вайц Е.В., Ефремов Е.А., Ковалевский А.Е. Безопасность и технологии электронной идентификации в странах Латинской Америки // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2019. № 2. С. 142–151.
9. Nguyen T.Ph.H., Nguyen X.C. Looking back on Vietnam – China relations since the establishment of strategic cooperative partnership // Russian Journal of Vietnamese Studies. 2020. No. 1. P. 8–17.
10. Pöhn D., Grabatin M., Hommel W. eID and self-sovereign identity usage: An overview // Electronics. 2021. Vol. 10, No. 22. Article ID 2811. DOI: 10.3390/electronics10222811.
11. Gao W., Yang L. Quantum election protocol based on quantum public key cryptosystem // Security and Communication Networks. 2021. Vol. 2021. Article ID 5551249. DOI: 10.1155/2021/5551249.
12. Meshram C., Obaidat M.S., Hsiao K.-F., et al. An effective fair off-line electronic cash protocol using extended chaotic maps with anonymity revoking trustee // Proceedings of the IEEE International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI). New York, NY, USA: IEEE, 2021. Article ID 21403178. DOI: 10.1109/CCCI52664.2021.9583217.
13. Qazi R., Qureshi K.N., Bashir F., et al. Security protocol using elliptic curve cryptography algorithm for wireless sensor networks // Journal of Ambient Intelligence and Humanized Computing. 2020. Vol. 12. P. 547–566. DOI: 10.1007/s12652-020-02020-z.
14. Turkanovic M., Podgorelec B. Signing blockchain transactions using qualified certificates // IEEE Internet Computing. 2020. Vol. 24, No. 6. P. 37–43. DOI: 10.1109/MIC.2020.3026182.
15. Craggs B., Rashid A. Trust beyond computation alone: Human aspects of trust in blockchain technologies // Proceedings of the IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS 2019). New York, NY, USA: IEEE, 2019. P. 21–30. DOI: 10.1109/ICSE-SEIS.2019.00011.
16. Li L., Liao H., Xuan J., Wang H. Research on the integrated electronic signature service platform of energy and power // J. Phys.: Conf. Ser. 2020. Vol. 1626. Article ID 012063. DOI: 10.1088/1742-6596/1626/1/012063.
17. Mihailescu M.I., Nita S.L., Corneliu P.V. Applied cryptography in designing e-learning platforms // eLearning and Software for Education: Proceedings of the 16th International Scientific Conference / I. Roceanu (ed.), et al. Bucharest: Editura Universitara, 2020. Vol. 2. P. 179–189. DOI: 10.12753/2066-026X-20-108.
18. Johnson M.C., Schellekens O., Stewart J., et al. SafeCare: An innovative approach for improving quality through standards, benchmarking, and improvement in low-and middle-income countries // Joint Commission Journal on Quality and Patient Safety. 2016. Vol. 42, No. 8. P. 350–360. DOI: 10.1016/S1553-7250(16)42049-0.
19. Шаповаленко С.Г. Внедрение системы электронного документооборота при отправлении воинских почтовых отправлений на узлах фельдъегерско-почтовой связи // Стратегическая стабильность. 2020. № 2 (91). С. 82–83.
20. Губарьков С.В. Использование инновационных технологий для организации документооборота в таможенных органах Российской Федерации // Проблемы развития предприятий: теория и практика: сб. статей VII Междунар. науч.-практ. конф. / под ред. В.И. Будиной. Пенза: Пензенский гос. аграр. ун-т, 2020. С. 58–62.
21. Tsakalakis N., O'Hara K., Stalla-Bourdillon S. Identity assurance in the UK: Technical implementation and legal implementations under the eIDAS regulation // WebSci '16: Proceedings of the 8th ACM Conference on Web Science. New York, NY, USA: ACM, 2016. P. 55–65. DOI: 10.1145/2908131.2908152.
22. Tsakalakis N., Stalla-Bourdillon S., O'Hara K. Data protection by design for cross-border electronic identification: Does the eIDAS interoperability framework need to be modernized? // Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data. Privacy and Identity 2018. IFIP Advances in Information and Communication Technology / E. Kosta (ed.), et al. Cham, Switzerland: Springer, 2019. Vol. 547. P. 255–274. DOI: 10.1007/978-3-030-16744-8_17.
23. Veerpalu A., Jürgen L., Rodrigues e Silva E.D.C., Norta A. The hybrid smart contract agreement challenge to European electronic signature regulation // International Journal of Law and Information Technology. 2020. Vol. 28, No. 1. P. 39–84. DOI: 10.1093/ijlit/eaaa005.
24. Paet U. Report on cyber defence: report No. A8-0189/2018 // European Parliament: офиц. сайт. URL: https://www.europarl.europa.eu/doceo/document/A-8-2018-0189_EN.pdf (дата обращения: 10.08.2022).
25. Panda Security и Парижское соглашение для повышения доверия и безопасности в кибер-пространстве // Panda: сайт. URL: https://www.cloudav.ru/mediacenter/news/supports-paris-call-cyberspace/ (дата обращения: 10.08.2022).
26. Храмцовская Н. Новое европейское законодательство об электронной идентификации и услугах в области доверия (в том числе об электронных подписях) // Blogger: веб-сервис. URL: http://rusrim.blogspot.com/2014/09/blog-post_95.html (дата обращения: 10.08.2022).
27. Barreira I., Bordier J., Delos O., et al. Analysis of standards related to Trust Service Providers. Mapping of requirements of eIDAS to existing standards // ENISA: офиц. сайт. URL: https://www.enisa.europa.eu/publications/tsp_standards_2015 (дата обращения: 10.08.2022).
28. Vulnerability Lab // SEC Consult Unternehmensberatung GmbH: офиц. сайт. URL: https://sec-consult.com/vulnerability-lab/ (дата обращения: 10.08.2022).
29. Resolución de 18 de abril de 2018, del Centro Criptológico Nacional, por la que se certifica la seguridad del producto "Panda Adaptive Defense Protection Agent, versión 8.0", desarrollado por Panda Security, SL. // Agencia Estatal Boletín Oficial del Estado: офиц. сайт. URL: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-6640 (дата обращения: 10.08.2022).
30. Worldwide infrastructure security report // SecurityLab.ru: информ. портал. URL: https://www.securitylab.ru/upload/WISR2012_EN.pdf (дата обращения: 10.08.2022).
31. Styran V. My article in Hakin9 magazine Issue 7/12 // SecurityLab.ru: информ. портал. URL: https://www.securitylab.ru/blog/personal/securegalaxy/23982.php (дата обращения: 10.08.2022).
32. Camastra L., Morgenstern I., Vojtěšek J. Backdoored client from Mongolian CA MonPass // Avast Software s.r.o.: офиц. сайт. URL: https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass/ (дата обращения: 10.08.2022).
33. A single standardised login system // eHerkenning: офиц. сайт. URL: https://www.eherkenning.nl/en (дата обращения: 10.08.2022).
34. eHerkenning // Similarweb LTD: офиц. сайт. URL: https://www.similarweb.com/ru/website/eherkenning.nl/#overview (дата обращения: 10.08.2022).
35. Материалы конференции РусКрипто'2022 // Ассоциация «РусКрипто»: офиц. сайт. URL: https://www.ruscrypto.ru/accociation/archive/ (дата обращения: 10.08.2022).
36. Электронный юридически значимый документооборот // ООО «Газинформсервис»: офиц. сайт. URL: https://www.gaz-is.ru/reshenija/resheniya/dokumentooborot.html (дата обращения: 10.08.2022).
37. Услуги ДТС // ООО «УЦ ГИС»: офиц. сайт. URL: https://ca.gisca.ru/catalog/uslugi-dts/ (дата обращения: 10.08.2022).
38. Калькулятор экономии с Диадоком // КонтурДиадок: сайт. URL: https://www.diadoc.ru/kalkulator-vygodnosty-edo (дата обращения: 10.08.2022).

39. СКБ Контур успешно подтвердил высокий уровень информационной безопасности системы Диадок // КонтурДиадок: сайт. URL: https://www.diadoc.ru/blog/7804 (дата обращения: 10.08.2022).
40. Аудит информационной безопасности // АО «Калуга Астрал»: офиц. сайт. URL: https://is.astral.ru/services/zashchita-informatsii/audit-informatsionnoy-bezopasnosti/ (дата обращения: 10.08.2022).
41. The Guardian: взломавшие сервер Deloitte хакеры получили доступ к письмам ООН и госорганов США // ИД «Коммерсантъ»: офиц. сайт. URL: https://www.kommersant.ru/doc/3434992 (дата обращения: 10.08.2022).
42. ООО «Такском»: офиц. сайт. URL: https://taxcom.ru/ (дата обращения: 10.08.2022).
43. Кильдеева С.С., Катасев 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.
44. Чарыева К.А., Байрамбердиев К.Б. Важность электронного документооборота // Интернаука. 2021. № 5–1 (181). С. 17–18.
45. Грудинина Е.А., Мкоян Г.В. Оптимизация электронного документооборота на примере компании «Связьтранзит» // Бизнес-образование в экономике знаний. 2021. № 1 (18). С. 32–35.
46. Коробейникова К.В. Защита конфиденциальной информации в ЭДО и архивном хранении // Защита информации. Инсайд. 2019. № 4 (88). С. 4–7.
47. Петренко А.С., Петренко С.А. Безопасная Agile-разработка системы ЭДО // Защита информации. Инсайд. 2019. № 3 (81). С. 30–35.
48. Сосина А.В., Шишина Ю.А. Электронный документооборот и его безопасность // Наука и научный потенциал – основа устойчивого развития общества: сб. статей Междунар. науч.-практ. конф. Уфа: ОМЕГА САЙНС, 2018. Ч. 2. С. 98–103.
49. Арванова С.М., Шогенова З.А., Маремшаова А.Р., Цавкилова М.А. Средства криптографической защиты информации в системе ЭДО // Фундаментальные и прикладные научные исследования: актуальные вопросы современной науки, достижения и инновации: сб. науч. статей по материалам III Междунар. науч.-практ. конф. Уфа: НИЦ Вестник науки, 2020. С. 42–47.
50. Свидетельство о регистрации программы для ЭВМ № 2018617864 Российская Федерация. БИФИТ ЭДО Контрагенты: № 2018615043: заявл. 18.05.2018: опубл. 03.07.2018 / Власов А.Ю., Дмитричев А.С., Иванов А.С. и др.; заявитель ООО «БИФИТ ЭДО» // ФГБУ «Федеральный институт промышленной собственности»: офиц. сайт. URL: https://new.fips.ru/iiss/document.xhtml?faces-redirect=true&id=ba5949b125735601935c4f9f3375694a (дата обращения: 10.08.2022).
51. Свидетельство о регистрации программы для ЭВМ № 2019611718 Российская Федерация. ViPNet EDI Soap Gate 3 (ViPNet ЭДО Шлюз безопасности 3): № 2019610561: заявл. 23.01.2019: опубл. 04.02.2019 / заявитель АО «ИнфоТеКС» // ФГБУ «Федеральный институт промышленной собственности»: офиц. сайт. URL: https://new.fips.ru/iiss/document.xhtml?faces-redirect=true&id=93aed55dbb5f60f2d7cdf70fdd72f2af (дата обращения: 10.08.2022).
52. Свидетельство о регистрации программы для ЭВМ № 2021611393 Российская Федерация. Модуль ЭДО с ЭЦП(УКЭП): № 2021610544: заявл. 20.01.2021: опубл. 27.01.2021 / заявитель ООО «ИМПЕЛТЕХ» // ФГБУ «Федеральный институт промышленной собственности»: офиц. сайт. URL: https://new.fips.ru/iiss/document.xhtml?faces-redirect=true&id=eff016b9c9b4f6b631debff9e9dee803 (дата обращения: 10.08.2022).
53. Свидетельство о регистрации программы для ЭВМ № 2020617308 Российская Федерация. Программа «Технологический электронный документооборот. Очередь 2019 (КП ЭДО. Очередь 2019)»: № 2020616287: заявл. 22.06.2020: опубл. 03.07.2020 / заявитель ОАО «Российские железные дороги» // ФГБУ «Федеральный институт промышленной собственности»: офиц. сайт. URL: https://new.fips.ru/iiss/document.xhtml?faces-redirect=true&id=0f4ea4d8b75298eb4ee44e5f6f6566fe (дата обращения: 10.08.2022).
54. Конференции // MSB Events: сайт. URL: https://msbevents.com/#conferences (дата обращения: 10.08.2022).
55. PKI-Форум: сайт. URL: https://pki-forum.ru/ (дата обращения: 10.08.2022).
56. Программа конференции ИБРР-2021 // Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления: офиц. сайт. URL: http://www.spoisu.ru/conf/ibrr2021/programma (дата обращения: 10.08.2022).
57. VII SOC Форум 2021 // АО «РБК»: офиц. сайт. URL: https://soc-forum.bizconf.rbc.ru/soc2021 (дата обращения: 10.08.2022).

REFERENCES

(1) SecurityLab.ru. *Homepage*. Available from: https://www.securitylab.ru/ [Accessed: 10 August 2022]. (In Russian)
(2) Amangeldy AA. Digital technologies incorporation into legislation of the Republic of Kazakhstan. *European and Asian Law Review*. 2021; 4(1): 52–60.
(3) Beisekeyev AE, Dubrovin PV, Temerbayeva MV. Problems and prospects of using the industrial certificate in the Republic of Kazakhstan. *Bulletin of Innovative University of Eurasia* [Innovaciâlyķ Eurazіâ universitetìnìņ habaršysy]. 2021; 82(2): 64–71. (In Kazakh)
(4) Blythe SE. *A critique of German e-commerce law and recommendations for improvement*. Available from: http://www.aabri.com/SA12Manuscripts/SA12045.pdf [Accessed: 10 August 2022].
(5) Zhetibayev ZhK. Legal status of electronic transactions according to the experience of German state. *Bulletin of Institute of Legislation and Legal Information of the Republic of Kazakhstan* [Qazaqstan Respýblıkasy Zańnama jáne quqyqtyq aqparat ınstıtýtynyń jarshysy]. 2020; 61(3): 201–207. (In Kazakh)
(6) Hühnlein D, Frosch T, Schwenk J, Piswanger CM, Sel M., Hühnlein T, et al. Futuretrust – future trust services for trustworthy global transaction. In: Hühnlein D, Roßnagel H, Schunck CH, Talamo M (eds.) *Proceedings of the Open Identity Summit 2016, 13–14 October 2016, Rome, Italy*. Bonn, Germany: Gesellschaft für Informatik; 2016. p. 27–41.
(7) Andraško J, Mesarčík M. Those who shall be identified: The data protection aspects of the legal framework for electronic identification in the Europe Union. *TalTech Journal of European Studies*. 2021; 11(2): 3–24.
(8) Minaev VA, Vaits EV, Efremov EA, Kovalevsky AE. Safety and technologies of electronic identification in Latin America. *Vestnik of Russian New University. Series "Complex Systems: Models, Analysis, Management"* [Vestnik Rossijskogo novogo universiteta. Seriya Slozhnye sistemy: modeli, analiz i upravlenie]. 2019; (2): 142–151. (In Russian)
(9) Nguyen TPhH, Nguyen XC. Looking back on Vietnam – China relations since the establishment of strategic cooperative partnership. *Russian Journal of Vietnamese Studies*. 2020; (1): 8–17.
(10) Pöhn D, Grabatin M, Hommel W. eID and self-sovereign identity usage: An overview. *Electronics*. 2021; 10(22): article ID 2811. https://doi.org/10.3390/electronics10222811.
(11) Gao W, Yang L. Quantum election protocol based on quantum public key cryptosystem. *Security and Communication Networks*. 2021; 2021: article ID 5551249. https://doi.org/10.1155/2021/5551249.
(12) Meshram C, Obaidat MS, Hsiao KF, Imoize AL, Meshram A. An effective fair off-line electronic cash protocol using extended chaotic maps with anonymity revoking trustee. In: IEEE *Proceedings of the 2021 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), 15–17 October 2021, Beijing, China*. New York, NY, USA: IEEE; 2021. article ID 21403178. https://doi.org/10.1109/CCCI52664.2021.9583217.
(13) Qazi R, Qureshi KN, Bashir F, Islam NU, Iqbal S, Arshad A. Security protocol using elliptic curve cryptography algorithm for wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*. 2020; 12: 547–566. https://doi.org/10.1007/s12652-020-02020-z.
(14) Turkanovic M, Podgorelec B. Signing blockchain transactions using qualified certificates. *IEEE Internet Computing*. 2020; 24(6): 37–43. https://doi.org/10.1109/MIC.2020.3026182.
(15) Craggs B, Rashid A. Trust beyond computation alone: Human aspects of trust in blockchain technologies. In: IEEE *Software Engineering in Society: Proceedings of the 2019 IEEE/ACM 41st International Conference on Software Engineering, ICSE-SEIS, 15 August 2019, Montreal, Canada*. New York, NY, USA: IEEE; 2019. p. 21–30. https://doi.org/10.1109/ICSE-SEIS.2019.00011.
(16) Li L, Liao H, Xuan J, Wang H. Research on the integrated electronic signature service platform of energy and power. *J. Phys.: Conf. Ser.* 2020; 1626: article ID 012063. https://doi.org/10.1088/1742-6596/1626/1/012063.
(17) Mihailescu MI, Nita SL, Corneliu PV. Applied cryptography in designing e-learning platforms. In: Roceanu I, Ciolan L, Trăușan Matu Ș, Stefan IA (eds.) *eLearning and Software for Education: Proceedings of the 16th International Scientific Conference, 30 April – 1 May 2020, Bucharest, Romania*. Bucharest: Editura Universitara; 2020. p. 179–189. https://doi.org/10.12753/2066-026X-20-108.

(18) Johnson MC, Schellekens O, Stewart J, van Ostenberg P, de Wit TR, Spieker N. SafeCare: An innovative approach for improving quality through standards, benchmarking, and improvement in low-and middle-income countries. *Joint Commission Journal on Quality and Patient Safety*. 2016; 42(8): 350–360. https://doi.org/10.1016/S1553-7250(16)42049-0.
(19) Shapovalenko S. The introduction of an electronic document management system for sending military mail items at the courier and postal sites. *Strategic Stability* [Strategicheskaya stabil'nost']. 2020; 91(2): 82–83. (In Russian)
(20) Gubarkov SV. Use of innovative technologies for organizing documentary turnover in the customs authorities of the Russian Federation. In: Budina VI (ed.) *Problems of Enterprise Development: Theory and Practice: Proceedings of the 7th International Scientific and Practical Conference, 13–14 April 2020, Penza, Russia*. Penza, Russia: Penza State Agrarian University; 2020. p. 58–62. (In Russian)
(21) Tsakalakis N, O'Hara K, Stalla-Bourdillon S. Identity assurance in the UK: Technical implementation and legal implementations under the eIDAS regulation. In: Nejdl W, Hall W, Parigi P, Staab S (eds.) *WebSci '16: Proceedings of the 8th ACM Conference on Web Science, 22–25 May 2016, Hannover, Germany*. New York, NY, USA: ACM; 2016. p. 55–65. https://doi.org/10.1145/2908131.2908152.
(22) Tsakalakis N, Stalla-Bourdillon S, O'Hara K. Data protection by design for cross-border electronic identification: Does the eIDAS interoperability framework need to be modernized? In: Kosta E, Pierson J, Slamanig D, Fischer-Hübner S, Krenn S (eds.) *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data. Privacy and Identity 2018. IFIP Advances in Information and Communication Technology. Vol. 547*. Cham, Switzerland: Springer; 2019. p. 255–274. https://doi.org/10.1007/978-3-030-16744-8_17.
(23) Veerpalu A, Jürgen L, Rodrigues e Silva EDC, Norta A. The hybrid smart contract agreement challenge to European electronic signature regulation. *International Journal of Law and Information Technology*. 2020; 28(1): 39–84. https://doi.org/10.1093/ijlit/eaaa005.
(24) Paet U. *Report on cyber defence*. European Parliament's Committee on Foreign Affairs. Report No.: A8-0189/2018, 2018.
(25) Panda. *Panda security and Paris cybersecurity tech accord, increasing trust and security in cyberspace*. Available from: https://www.cloudav.ru/mediacenter/news/supports-paris-call-cyberspace/ [Accessed: 10 August 2022]. (In Russian)
(26) Khramtsovskaya N. *New European laws on electronic identification and trust services (including e-signatures)*. Available from: http://rusrim.blogspot.com/2014/09/blog-post_95.html [Accessed: 10 August 2022]. (In Russian)
(27) Barreira I, Bordier J, Delos O, Fiedler A, Mielnicki T, Miękina A, et al. *Analysis of standards related to Trust Service Providers. Mapping of requirements of eIDAS to existing standards*. Available from: https://www.enisa.europa.eu/publications/tsp_standards_2015 [Accessed: 10 August 2022].
(28) SEC Consult Unternehmensberatung GmbH. *Vulnerability Lab*. Available from: https://sec-consult.com/vulnerability-lab/ [Accessed: 10 August 2022].
(29) Agencia Estatal Boletín Oficial del Estado. *Resolución de 18 de abril de 2018, del Centro Criptológico Nacional, por la que se certifica la seguridad del producto "Panda Adaptive Defense Protection Agent, versión 8.0", desarrollado por Panda Security, SL*. Available from: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-6640 [Accessed: 10 August 2022]. (In Spanish)
(30) Arbor Networks, Inc. *Worldwide infrastructure security report*. Available from: https://www.securitylab.ru/upload/WISR2012_EN.pdf [Accessed: 10 August 2022].
(31) Styran V. *My article in Hakin9 magazine Issue 7/12*. Available from: https://www.securitylab.ru/blog/personal/securegalaxy/23982.php [Accessed: 10 August 2022].
(32) Camastra L, Morgenstern I, Vojtěšek J. *Backdoored client from Mongolian CA MonPass*. Available from: https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass/ [Accessed: 10 August 2022].
(33) eHerkenning. *A single standardised login system*. Available from: https://www.eherkenning.nl/en [Accessed: 10 August 2022].
(34) Similarweb LTD. *eHerkenning*. Available from: https://www.similarweb.com/ru/website/eherkenning.nl/#overview [Accessed: 10 August 2022]. (In Russian)
(35) RusCrypto Association [Associaciya "RusKripto"]. *Proceedings of the RusCrypto'2022 conference*. Available from: https://www.ruscrypto.ru/accociation/archive/ [Accessed: 10 August 2022]. (In Russian)
(36) OOO Gazinformservice (limited liability company). *Legally relevant electronic document flow.* Available from: https://www.gaz-is.ru/reshenija/resheniya/dokumentooborot.html [Accessed: 10 August 2022]. (In Russian)
(37) OOO Gazinformservice Certification Authority (limited liability company) [OOO UTs GIS]. *Trusted third party services*. Available from: https://ca.gisca.ru/catalog/uslugi-dts/ [Accessed: 10 August 2022]. (In Russian)
(38) KonturDiadoc. *Diadoc savings calculator*. Available from: https://www.diadoc.ru/kalkulator-vygodnosty-edo [Accessed: 10 August 2022]. (In Russian)
(39) KonturDiadoc. *SKB Kontur successfully confirms high level of Diadoc cybersecurity*. Available from: https://www.diadoc.ru/blog/7804 [Accessed: 10 August 2022]. (In Russian)
(40) AO Kaluga Astral (joint-stock company). *Information security audit*. Available from: https://is.astral.ru/services/zashchita-informatsii/audit-informatsionnoy-bezopasnosti/ [Accessed: 10 August 2022]. (In Russian)
(41) Kommersant. *The Guardian: Deloitte hack hit server containing emails from across UN and US government*. Available from: https://www.kommersant.ru/doc/3434992 [Accessed: 10 August 2022]. (In Russian)
(42) OOO Taxcom (limited liability company). *Homepage*. Available from: https://taxcom.ru/ [Accessed: 10 August 2022]. (In Russian)
(43) Kildeeva SS, Katasev AS, Talipov NG. Models and methods of prognostication and task distribution for performers in the electronic document management system. *Herald of Technical University* [Vestnik tehnologicheskogo universiteta]. 2021; 24(1): 79–85. (In Russian)
(44) Charyeva KA, Bayramberdiev KB. Importance of electronic document management. *Interscience* [Internauka]. 2021; 181(5–1): 17–18. (In Russian)
(45) Grudinina EA, Mkoyan GV. Optimization of electronic document flow on the example of company "Svyaztransit". *Business Education in the Knowledge Economy* [Biznes-obrazovanie v ekonomike znanij]. 2021; 18(1): 32–35. (In Russian)
(46) Korobeinikova KV. Defence of confidential information in electronic document management and archived storage. *Data Protection. Inside* [Zaschita informacii. Inside]. 2019; 88(4): 4–7. (In Russian)
(47) Petrenko AS, Petrenko SA. Secure agile-development of electronic document management. *Data Protection. Inside*. 2019; 81(3): 30–35. (In Russian)
(48) Sosina AV, Shishina YuA. Electronic document management and security. In: Omega Science *Science and Research Potential Are the Basis of Sustainable Society Development: Proceedings of the International Scientific and Practical Conference. Part 2, 11 October 2018, Magnitogorsk, Russia*. Ufa, Russia: Omega Science; 2018. p. 98–103. (In Russian)
(49) Arvanova SM, Shogenova ZA, Maremshaova AR, Tsavkilova MA. Cryptographic tools for data security in electronic document flow systems. In: Herald of Science Research Center [NIC Vestnik nauki] *Fundamental and Applied Research: Current Challenges, Achievements and Innovations in Contemporary Science: Proceedings of the 3rd International Scientific and Practical Conference, 13 June 2020, Ufa, Russia*. Ufa, Russia: Herald of Science Research Center; 2020. p. 42–47. (In Russian)
(50) Vlasov AYu, Dmitrichev AS, Ivanov AS, Smirnov VA, Turunov SA, Chat EA. *BIFIT EDO Contractors*. Available from: https://new.fips.ru/iiss/document.xhtml?faces-redirect=true&id=ba5949b125735601935c4f9f3375694a [Accessed: 10 August 2022]. (In Russian)
(51) AO InfoTeKS (joint-stock company). *ViPNet EDI Soap Gate 3 (ViPNet electronic document flow Security Gateway 3)*. Available from: https://new.fips.ru/iiss/document.xhtml?faces-redirect=true&id=93aed55dbb5f60f2d7cdf70fdd72f2af [Accessed: 10 August 2022]. (In Russian)
(52) OOO IMPELTEKH (limited liability company). *Electronic document flow module with electronic signature (enhanced qualified electronic signature)*. Available from: https://new.fips.ru/iiss/document.xhtml?faces-redirect=true&id=eff016b9c9b4f6b631debff9e9dee803 [Accessed: 10 August 2022]. (In Russian)
(53) OJSC Russian Railways. *The software "Technological electronic document management. Queue 2019 (KP EDO. Queue 2019)"*. Available from: https://new.fips.ru/iiss/document.xhtml?faces-redirect=true&id=0f4ea4d8b75298eb4ee44e5f6f6566fe [Accessed: 10 August 2022]. (In Russian)
(54) MSB Events. *Conferences*. Available from: https://msbevents.com/#conferences [Accessed: 10 August 2022]. (In Russian)
(55) PKI-Forum. *Homepage*. Available from: https://pki-forum.ru/ [Accessed: 10 August 2022]. (In Russian)
(56) Saint Petersburg Society of Informatics, Computer Facilities, Communication, and Control Systems. *ISRR-2021 conference program*. Available from: http://www.spoisu.ru/conf/ibrr2021/programma [Accessed: 10 August 2022]. (In Russian)
(57) RosBiznesConsulting. *VII SOC Forum 2021*. Available from: https://soc-forum.bizconf.rbc.ru/soc2021 [Accessed: 10 August 2022]. (In Russian)