# ЭЛЕКТРОННЫЕ ДОВЕРИТЕЛЬНЫЕ УСЛУГИ И ИХ РЕАЛИЗАЦИЯ

УДК 681.3.06(07)

## EIDAS: ПРИНЦИПЫ ПРЕДОСТАВЛЕНИЯ ДОВЕРИТЕЛЬНЫХ ЭЛЕКТРОННЫХ УСЛУГ И ПРОБЛЕМА ИНТЕРОПЕРАБЕЛЬНОСТИ

*А.В. ПОТИЙ, Ю.И. ГОРБЕНКО, А.В. КОРНЕЙКО, Ю.Н. КОЗЛОВ, А.И. ПУШКАРЕВ, И.Д. ГОРБЕНКО*

В работе на основе анализа законодательства ЕС формулируется система принципов предоставления электронных доверительных услуг. Рассматриваются принципы электронной идентификации и принципы предоставления электронных доверительных услуг. Отдельно рассматриваются проблемы интероперабельности в данной сфере, а также подход европейских организаций к стандартизации и решению вопросов технической интероперабельности.

*Ключевые слова:* электронная идентификация, электронные доверительные услуги, интероперабельность.

### ВВЕДЕНИЕ

Нет сомнений в том, что в Украине начинает формироваться существующий рынок электронных услуг. И хотя мы не найдем определения понятия «электронная услуга», их предоставление и использование уже регулируются рядом законных и подзаконных актов в различных сферах. Электронные платежи, осуществления финансовых операций с помощью Интернет-банкинга, открытие депозитов и оформление кредитов online, подача отчетных документов (деклараций, финансовой отчетности и пр.) в электронном виде и многое другое – все это можно назвать «электронной услугой». Все эти электронные услуги» регулируются законами в банковской сфере, в сфере электронной цифровой подписи и иных сферах [4, 5, 6]. Уже появилась законодательная инициатива по принятию закона «Об электронной торговле», а там не за горами и настоящее регулирование электронного рынка Украины.

ЕС имеет большой опыт формирования и регулирования подобного рода вопросов и изучение этого опыта является важным и полезным для нашего государства, учитывая подписанные документы политической и экономической ассоциации Украины с ЕС. С содержанием Регламента [1] можно познакомиться на сайте XXXX. С анализом положений данного документа можно ознакомиться в работе [7].

В настоящей работе авторы делают попытку формирования системы принципов, лежащих в основе электронной идентификации и предоставления электронных доверительных услуг, опираясь на материалы конференции, проведенной в июне 2014 в Польше (European Forum on Electronics Signature (EFPE 2014). – Miedzyzdroje, Poland. – www.efpe.pl). Также в работе анализируются проблемы интероперабельности в сфере электронных услуг.

### 1. ЦЕЛЬ, ЗАДАЧИ И ФУНКЦИИ РЕГЛАМЕНТА

Итак, вы законопослушный гражданин и добросовестный налогоплательщик, который ежегодно представляет в налоговый орган свою декларацию. Государство, в лице налоговой администрации, заинтересовано в создании максимально комфортных условий для организации этого процесса, а также для упрощения порядка подачи деклараций гражданами. Нет ничего лучше, когда подача декларации будет осуществляться без непосредственного контакта представителя налоговой администрации и налогоплательщика. Еще лучше, когда у налогоплательщика будет возможность подать декларацию в любое удобное для него время и в любом удобном ему месте (дома, в офисе, в заграничной командировке, на пляже под ласковым солнцем). Реализация этого процесса в виде совокупности электронных транзакций позволяет предложить налогоплательщику такую удобную публичную электронную услугу. На рис. 1 как раз и представлена такая услуга. Результатом этой услуги является поданная налогоплательщиком и принятая налоговой администрацией налоговая декларация.

Удобно? Да, несомненно. Но есть, как говориться, вопросы. Как убедиться в том, что вы загрузили сайт именно налоговой администрации? А может его подменили? Вы уверены в том, что никто кроме Вас не сможет войти в Ваш персональный кабинет и сформировать отчетность? Вы уверены в том, что при формировании декларации и ее регистрации в налоговом органе она не будет модифицирована (подделана), даже уполномоченным сотрудником налоговой администрации? Вы доверяете этому обезличенному сотруднику или даже роботу по приему деклараций? Вы уверены, что налоговый орган получил Вашу декларацию? А Вам не скажут, что Вы нарушили сроки подачи декларации или вообще ее

не подавали? И как доказать свою правоту, если Вас в этом обвинят? А как и где эта декларация будет храниться? А можно ли ее будет получить в виде твердой копии? Вы уверены, что ее не опубликуют в Интернете? Вы уверены...? Вы доверяете...? Таких вопросов у каждого пользователя может быть тысяча, ведь мы все сомневаемся и такие консервативные.

Заметим, что скорее всего обычный гражданин мало будет беспокоиться о технических средствах реализации этого процесса, он просто не будет их замечать, поскольку мы стремимся сделать такой и подобные процессы максимально комфортными, прозрачными, нетрудоемкими. Основной вопрос, который всегда будет волновать гражданина это ДОВЕРИЕ (trust) к услуге и УВЕРЕННОСТЬ (confident) в ее безопасности. И без обеспечения этих краеугольных качеств нельзя говорить о полноценном рынке электронных услуг. Именно это является основной целью Регламента – укрепление единого Европейского рынка электронных услуг путем поддержки доверия и уверенности в безопасности, а также прозрачности трансграничных электронных транзакций [2].

Положения Регламента охватывают две основные сферы: *электронная идентификация и электронные услуги*.

В области *электронной идентификации* Регламент определяет условия взаимного признания странами ЕС средств электронной идентификации физических и юридических лиц, выданных в рамках национальных нотифицированных схем электронной идентификации. Это формирует правовую, организационную и технологическую основы трансграничной идентификации и аутентификации в странах ЕС, как минимум для публичных электронных услуг.

В сфере *электронных услуг* Регламент определяет правила предоставления квалифицированных доверительных электронных услуг, к которым относятся:

– услуги выпуска и управления сертификатов открытых ключей для поддержки электронной подписи и электронной печати;

– услуги по проверке (валидации) электронной подписи и печати;

– услуги по предоставлению метки времени;

– услуги по подтверждению подлинности (аутентификации) веб-сайтов;


Рис. 1. Услуга предоставления электронной декларации

– услуги по регистрации и подтверждению доставки электронных документов;

– услуги по безопасному хранению (в том числе архивному) подписанных электронных документов.

По сути Регламент формирует условия приемлемости электронных документов в отношениях между различными субъектами и взаимного признания электронных доверительных услуг, предоставляемых провайдерами, на всей территории ЕС.

Основные задачи, на решение которых направлено принятие и последующее внедрение положений Регламента, можно сформулировать следующим образом:

1. Обеспечение правовой определенности и основ для использования электронной идентификации гражданами ЕС, формирование культуры использования средств электронной идентификации и электронных услуг в повседневной жизни.

2. Формирование правовых основ для разработки и широкого внедрения набора механизмов и услуг по поддержке доверия и уверенности в безопасности электронных транзакций, в том числе и трансграничных.

3. Внедрение практики управления рисками, опирающееся на следующие принципы:

– транспарентность и наблюдаемость: четкое определение обязанностей провайдеров доверительных услуг (Trusted Service Provider) и установление их ответственности;

– доверительность услуг на основе выполнения провайдерами установленных требований безопасности;

– поднадзорность деятельности провайдеров доверительных услуг по предоставлению доверительных электронных услуг;

– технологическая нейтральность: исключение требований, которые могут быть удовлетворены специальными технологиями и техническими методами;

– стандартизация и единые правила технического регулирования.

4. Формирование единого набора правил предоставления доверительных электронных услуг, применимых для всех стран членов ЕС.

Принятие и внедрение положений Регламента будет играть важную роль в различных сферах общественной жизни.

В *правовой сфере* Регламент формирует надежный правовой фундамент предоставления доверительных электронных услуг с полноценной защитой прав потребителей на территории всех стран членов ЕС, с общими правилами предоставления этих услуг провайдерами на основе взаимного признания электронной идентификации.

В *экономической сфере* Регламент способствует формированию и развитию свободного единого Европейского рынка продуктов и доверительных электронных услуг на основе общих правил Регламента.

В *социальной сфере,* путем формирования доверия и уверенности в безопасности через обеспечение свободы выбора в едином рынке электронных услуг, обеспечивается больший комфорт для граждан ЕС при осуществлении электронных транзакций.

В *технологической сфере* Регламент формирует основы для создания единой инфраструктуры электронного (цифрового) рынка и рынка электронных услуг, объединяющей в себя инфраструктуру электронной идентификации, инфраструктуру открытых ключей (PKI) и полномочий, органично вписывающейся в иные информационные инфраструктуры (в том числе и критические) стран-членов ЕС.

## 2. БАЗОВЫЕ ПРИНЦИПЫ ЭЛЕКТРОННОЙ ИДЕНТИФИКАЦИИ

Говоря об электронной идентификации (eID), мы будем учитывать следующие аспекты.

Во-первых, eID – это идентификация физических и юридических лиц путем выдачи им в установленном законом порядке и на основе установленной *схемы* специальных персональных средств электронной идентификации (электронных карточек, паспортов и проч., т.е. электронных идентификаторов, связанных с конкретным лицом).

Во-вторых, eID – это обеспечение технологической возможности осуществления аутентификации (подтверждения подлинности) владельца электронного идентификатора при выполнении им каких-либо электронных транзакций.

Эти два аспекта являются обязательными для предоставления электронных услуг и осуществления электронных транзакций. Регламент определяет базовые принципы электронной идентификации, которые рассматриваются ниже.

*1. Принцип взаимного признания.* Страны ЕС должны признавать средства электронной идентификации, которые выпущены в соответствии с национальными требованиями в рамках «нотифицированных» схем. Взаимное признание призвано способствовать трансграничному доступу к публичным электронным и иным услугам, требующих электронной идентификации. Таким образом, Регламент не вводит требования создания единой общеевропейской схемы электронной идентификации. Каждая страна формирует свою национальную инфраструктуру электронной идентификации.

*2. Принцип нотификации схемы электронной идентификации.* Страны ЕС обязаны уведомить Европейскую комиссию о национальных схемах электронной идентификации, которые используются на территории страны. Для этого определяются общие условия, формат и процедуры нотификации национальных схем.

*3. Принцип предоставления гарантий безопасности.* Нотифицированная схема электронной идентификации должна предоставлять определенный уровень гарантий безопасности (assurance level) средств электронной идентификации. Определены три уровня гарантий:

а. Низкий (low) уровень гарантий, который предполагает добровольное взаимное признание средств;

б. Достаточный (substantion) уровень гарантий;

в. Высокий (high) уровень гарантий.

Последние два уровня гарантий предполагают обязательное (мандатное) признание. Спецификация требований гарантий будет базироваться на результатах работы в рамках проекта STORK (XXX) или требованиях международного стандарта ISO/IEC 29115 [16]. Можно предположить, что требования гарантий средств электронной идентификации будут согласовываться с требованиями гарантий Единых критериев ISO/IEC 15408 [14].

*4. Принцип интероперабельности нотифицированных схем электронной идентификации.* Обеспечение интероперабельности является одним из основных требований при реализации трансграничных электронных транзакций и предоставления публичных электронных услуг. Комплексное решение проблемы интероперабельности направлено на устранение «электронных барьеров» для публичных услуг Евросоюза, построение «бесшовного» электронного пространства и единого электронного рынка.

*5. Принципы аутентификации.* Аутентификация должна базироваться на принципах безвозмездности предоставления услуги аутентификации, трансграничности и отсутствия дискриминации. Страны члены ЕС должны обеспечить возможность трансграничной онлайн аутентификации на основе электронной идентификации (eID-аутентификация). Траснграничная eID-аутентификация должна предоставляться публичной администрацией (уполномоченным государственным органом) на безвозмездной основе. Трансграничность и отсутствие дискриминации предполагает, что режимы и процедуры аутентификации в национальном приватном секторе должны быть применимы без каких-либо ограничений в приватном секторе других стран-членов ЕС. По сути, эти требования требуют согласования бизнес процессов в рамках единого рынка ЕС.

*6. Принцип кооперации.* Кооперация предполагает обмен опытом и хорошей практикой применения средств электронной идентификации и аутентификации между странами членами ЕС.

*7. Принцип ответственности.* Принцип ответственности предполагает установление ответственности стран-членов ЕС, провайдеров услуг электронной идентификации и аутентификации за возможное нанесение ущерба в ходе предоставления услуги электронной идентификации. Одним из направлений реализации этого принципа является страхование рисков в данной сфере.

## 3. ПРИНЦИПЫ ПРЕДОСТАВЛЕНИЯ ЭЛЕКТРОННЫХ ДОВЕРИТЕЛЬНЫХ УСЛУГ

Как отмечалось выше, Регламент регулирует деятельность в сфере предоставления электронных услуг. На наш взгляд принципиальным является то, что Регламент формирует основу рынка электронных услуг и переводит, например, электронную цифровую подпись из статуса уникальной технологии, в категорию одной из многих возможных электронных услуг свободно предоставляемых на рынке. Кроме того, перечень таких услуг будет расширяться по мере развития рынка и заинтересованности в таких услугах потребителей. Сейчас можно говорить, что закладываются основы формирования некой инфраструктуры единого рынка электронных услуг, которая будет интегрировать инфраструктуру открытого ключа, инфраструктуру электронной идентификации и другие «инфраструктуры». Регламент в явном виде определяет такие услуги:

– услуги выпуска и управления сертификатов открытых ключей для поддержки электронной подписи и электронной печати;

– услуги по проверке (валидации) электронной подписи и печати;

– услуги по предоставлению метки времени;

– услуги по подтверждению подлинности (аутентификации) веб-сайтов;

– услуги по регистрации и подтверждению доставки электронных документов;

– услуги по безопасному хранению (в том числе архивному) подписанных электронных документов.

Перечень услуг будет расширяться, например, уже сейчас рассматривается возможность предоставления услуги электронного апостиля.

Для широкого распространения электронной услуги, необходимо дать потребителю четкое и ясное ее определение, а также указать на те полезные эффекты (или выгоды), которые получит потребитель от использования данной услуги. В ряде исследований указывается на недостаточный уровень мотивации потребителя по использованию этих услуг [19]. Задача государственных органов, с одной стороны, и свободного рынка, с другой стороны, и заключается в формировании такой мотивации и распространения электронных услуг в приватном и публичном секторах.

Основным принципом предоставления электронных услуг является принцип ***ДОВЕРИЯ***. Электронные услуги предоставляются *третьей доверительной стороной-провайдером доверительной услуги.* Доверительная третья сторона (ДТС) – это независимая организация, предоставляющая электронные услуги, которой доверяют пользователи на основе выполнения ДТС

определенных действий безопасным образом [14]. Регламент определяет два типа провайдеров доверительных услуг (trusted service provider-TSP) – квалифицированный (QTSP) и неквалифицированный. Отличаются они по уровню ответственности, надзору за их деятельностью и ограничениям, которые накладываются на их деятельность.

*Принцип ответственности провайдера.* Любой провайдер электронных доверительных услуг несет ответственность за нанесение ущерба, наступившего в результате его умышленных или неумышленных действий. Причем, изменение (установление) меры ответственности для QTSP возможны только в судебном порядке, в то время как для неквалифицированных TSP уровень ответственности является объектом договорного урегулирования с пользователем. На ответственность провайдеров распространяется принцип применимости национальных правил взыскания ущерба.

*Принцип признания* TSP третьих стран предполагает, что провайдеры доверительных электронных услуг третьих стран (не членов ЕС) могут быть признаны только через соответствующее международное соглашение между Еврокомиссией и третьей стороной или международной организацией, при обязательном соблюдении принципа отсутствия дискриминации.

*Принцип доступности услуги* провайдера для лиц с ограниченными возможностями (физическими недостатками).

Регламент определяет необходимость организации и осуществления надзора за деятельностью TSP и формирования соответствующих органов надзора. При этом для неквалифицированных TSP вводится реактивный мониторинг (т. е. контроль по факту (ex post) инцидента или облегченный надзор). А для QTSP вводится полноценный предварительный (ex ante) надзор и надзор по факту. Регламент определяет перечень задач органов надзора, правила взаимодействия национальных органов надзора между собой и с Еврокомиссией.

Регламент накладывает ряд обязательств на провайдеров электронных услуг. Для всех провайдеров вводятся минимальные требования по безопасности, в том числе требования по анализу уязвимостей. Для QTSP вводятся дополнительные требования безопасности, предъявляемые к персоналу, надежности (гарантоспособности) систем, эксплуатируемых провайдером, к схемам страхования ответственности, к порядку первой идентификации держателя сертификатов и т.д.

Подтверждение соответствия этим и иным требованиям квалифицированный провайдер получает в ходе аккредитации, в результате успешного прохождения которой, он вносится органом надзора в список квалифицированных провайдеров доверительных услуг. Ежегодно, не менее одного раза, провайдер доверительных услуг должен проходить проверку, по результатам которой орган по надзору может исключить провайдера из списка. Орган надзора является держателем реестра квалифицированных провайдеров доверительных электронных услуг и реестра квалифицированных доверительных услуг, предоставляемых провайдерами. Для индикации квалифицированных доверительных услуг внедряется единая Европейская метка доверия (EU trustmark). Она используется квалифицированными провайдерами и в простой, легкоузнаваемой и ясной форме указывает на квалифицированный статус доверительной услуги, предоставляемой провайдером.

Требования и условия предоставления конкретных услуг достаточно подробно рассмотрены в работах [8,9].

## 4. ПРОБЛЕМА ИНТЕРОПЕРАБЕЛЬНОСТИ ПУБЛИЧНЫХ ЭЛЕКТРОННЫХ УСЛУГ: КОНЦЕПТУАЛЬНЫЙ ПОДХОД К РЕШЕНИЮ

В контексте инфраструктуры доверительных электронных услуг, на проблему интероперабельности необходимо смотреть гораздо шире, чем просто как согласование форматов данных, протоколов и технических спецификаций средств электронной идентификации, ЭЦП и т.п.

«Интероперабельность – это способность несопоставимых и различных организаций взаимодействовать в интересах взаимной выгоды и согласования общих целей, путем распределения общей информации и знаний между организациями, через бизнес процессы, которые они поддерживают, посредством обмена данными между соответствующими информационно-телекоммуникационными системами.

Интероперабельность публичных электронных услуг является ключевым фактором формирования единого цифрового рынка Европы и обеспечения прозрачного трансграничного обмена информацией, что позволит гражданину и бизнесу воспользоваться всеми преимуществами свобод единого европейского рынка» [10].

Для решения проблем интероперабельности при внедрении схем электронной идентификации и публичных электронных услуг, европейская комиссия по коммуникациям разработала Европейскую стратегию по обеспечению интероперабельности (Europen Interoperability Strategy – EIS). В рамках этой стратегии реализуется программа «Интероперабельность Европейских публичных услуг», которая включает в себя ряд проектов и инициатив. Одной из такой инициатив является Europen Interoperability Framework (EIF, www.ec.europa.eu/isa/documentations/isa_annex_ii_eif_en.pdf).

Основная цель усилий в рамках этой инициативы является разработка общих методологических подходов к обеспечению интероперабельности администраторов (провайдеров)

публичных электронных услуг – т.е. услуг, которые предоставляются национальными государственными органами гражданам и бизнесу.

Интероперабельность играет важную роль в поддержание единого электронного рынка Европы. Всё возрастающее использование гражданами и бизнесом возможностей и свобод единого ринка Европы является основной причиной взаимодействия граждан и бизнеса с публичными администрациями за пределами своих национальных государств. Гражданам необходим постоянный доступ к информации и документам для работы, учебы и путешествий в странах ЕС. Деловым партнерам необходима информация для эффективного взаимодействия с партнерами из различных стран. На пути эффективного решения этих повседневных задач возникают *электронные барьеры* и причины их возникновения лежат не только в технической плоскости. Интероперебальность позволяет провайдерам публичных электронных услуг обмениваться информацией и взаимодействовать между собой для эффективного предоставления трансграничных электронных услуг.

Таким образом, интероперабельность позволяет обеспечить:

– взаимодействие между провайдерами публичных электронных услуг;

– обмен информацией между провайдерами для наиболее полного удовлетворения правовых требований и политических обязательств;

– распределение и совместное использование провайдерами публичных электронных услуг информации с целью повышения административной эффективности и устранения электронных барьеров для граждан и бизнеса.

В основе понимания и формулировки путей решения проблемы обеспечения интероперабельности лежит трехуровневая модель предоставления публичных электронных услуг (рис. 2) [10].

Агрегирование предполагает объединение публичных услуг в единый сервис для пользователей (государственных органов, бизнеса и граждан) и координацию действий провайдеров публичных услуг. При этом предполагается, что электронные транзакции будут трансграничными и осуществляются между различными административными и корпоративными уровнями через механизмы, удовлетворяющие специфическим бизнес требованиям. Публичные услуги не должны предоставляться исключительно правительственными web-сайтами. Они должны легко интегрироваться в web-приложения посредников, но при этом ответственность за услугу не снимается с государственного органа. Необходимо реализовать четкую и ясную идентификацию, на основе которой пользователи однозначно различают публичную и приватную услуги.

На втором уровне решаются проблемы защиты данных и управления безопасностью. Вся публичная информация подлежит защите и должна соответствующим образом контролироваться. Безопасность потенциально является основным барьером к обеспечению интероперабельности, если требования безопасности не будут гармонизированы между организациями.

Уровень базовых публичных услуг определяет основные компоненты, на основе которых могут быть построены публичные электронные услуги.


Рис. 2. Трехуровневая модель предоставления публичных электронных услуг

Во-первых, это всевозможные электронные реестры (регистры), под которыми понимают надежные источники информации, находящиеся под управлением различных государственных администраций. К таким реестрам можно отнести реестр недвижимости, земельный кадастр, реестры лицензиатов и т.д. Эти реестры должны быть доступны для широкого и многократного использования при соблюдении требований безопасности информации и приватности.

Во-вторых, вводится понятие посредник интероперабельности (Interoperability Facilitators), который является провайдером таких услуг, как трансляция между протоколами, форматами данных и языками или действует как информационный брокер.

И, наконец, внешние услуги, например, электронные платежи или коммуникационные услуги.

На практике интероперабельность рассматривается на четырех уровнях: правовом, организационном, семантическом и техническом.

***Правовая интероперабельность***. Каждый национальный публичный орган предоставляет публичные электронные услуги в рамках национального законодательства и несовместимость законодательства стран-членов ЕС может существенно затруднить совместную работу органов в сфере предоставления публичных электронных услуг.

***Организационная интероперабельность***. Кооперация различных организаций направлена на интеграцию бизнес процессов и удовлетворение требований пользователей (потребителей) через обеспечение наблюдаемости услуг, легкости использования услуг, доступности услуг и ориентированности на конечного пользователя. Объектами организационной интероперабельности являются:

– согласование (выравнивание) бизнес процессов;

– организационное (корпоративное) взаимодействие;

– управление изменениями.

***Семантическая интероперабельность***. Существующие различия в языковой, культурной, правовой и административной среде стран ЕС являются серьезными вызовами для обеспечения однозначного и точного взаимопонимания взаимодействующих субъектов и распознавания форматов обмениваемой информации.

***Техническая интероперабельность*** предполагает согласование формализованных технических спецификаций при реализации публичных электронных услуг.

В качестве механизма достижения интероперабельности на рассмотренных выше уровнях предлагается использовать ***соглашения по интероперабельности*** (interoperability agreements). На правовом уровне соглашение по интероперабельности предполагает, что предоставление публичных электронных услуг осуществляется либо на основе национального законодательства, включающего требования Европейских директив, перенесенных на национальный уровень, либо на основе дву- и многосторонних соглашений между субъектами отношений в сфере публичных электронных услуг.

Соглашение на организационном уровне могут применять форму MoUs (XXX) или SLA (XXX), которые уточняют обязательства для участников трансграничных процессов и определяют ожидаемый уровень услуг, поддержки процедур, взаимодействия и т.п.

Соглашения на семантическом уровне могут принимать форму справочных таксономий, схем, сводов правил, словарей данных, библиотек и т.д.

Соглашения на техническом уровне включают в себя интерфейсы, механизмы безопасности, спецификации услуг, форматы данных, коммуникационные протоколы и др.

В последнее время предпринимаются значительные усилия по обеспечению интероперабельности на всех уровнях. Особая активность наблюдается на техническом уровне. Большую организационную и техническую работу проводит Европейская организация по стандартизации (CEN) и Европейский комитет по телекоммуникациям (ETSI) [12]. На рис. 3 представлена рационализированная структура нормативных документов и стандартов в сфере доверительных электронных услуг, которая закреплена Мандатом по стандартизации M460 [13] или просто Мандат 460.

Анализ требований стандартов из комплекса представленных в M460 документов будет предметом наших дальнейших публикаций.

## ВЫВОДЫ

1. Страны Европейского союза активно работают над формирование единого и свободного цифрового рынка или рынка электронных услуг. По сути создается инфраструктура электронной идентификации граждан, на основе которой формируется инфраструктура электронных трансграничных доверительных услуг. Электронная подпись становиться одной из этих услуг. Регламент закладывает методологические основы формирования такого рынка с учетом обеспечения прав и свобод граждан стран членов ЕС.

2. Формирование украинского национального законодательства в сфере электронной цифровой подписи и электронных услуг должно проводиться с учетом и на основе Регламента. Уже на уровне разрабатываемых законов необходимо обеспечить правовую интероперабельность схем электронной идентификации и предоставления электронных доверительных услуг.

3. Актуальными являются исследования проблем обеспечения интероперабельности электронных доверительных услуг на различных уровнях с привлечением широкого круга экспертов и исследователей из различных сфер (право,

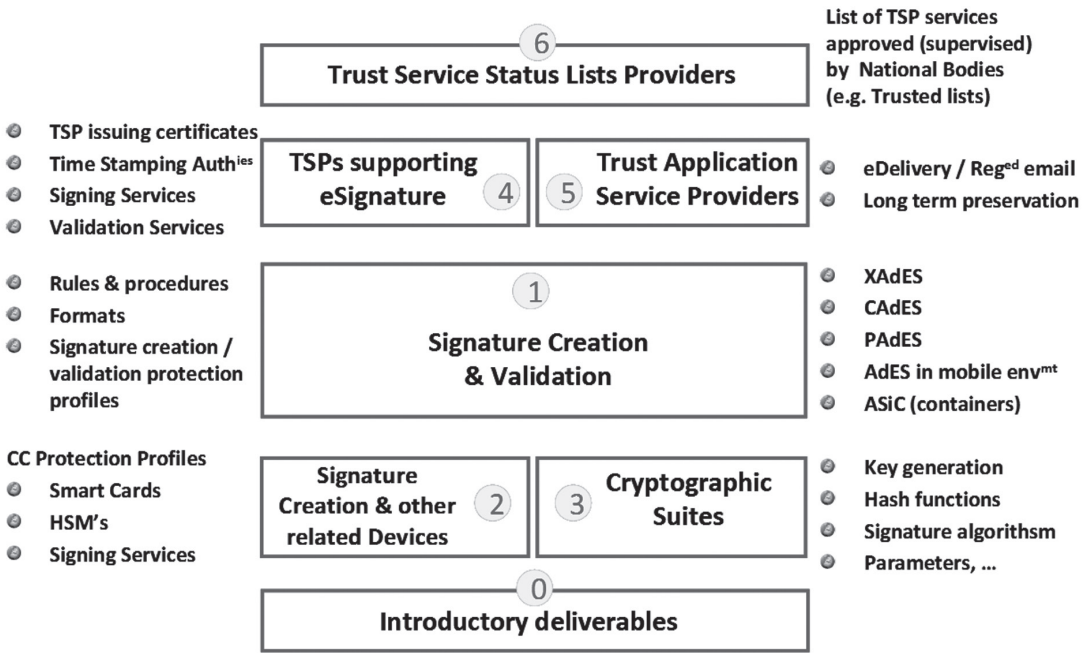


Рис. 3. Рационализированная структура стандартов, регулирующих технические вопросы в сфере электронных услуг (взято из доклада [12])

проектирование бизнес процессов, административное управление, бизнес администрирование, менеджмент, техническое регулирование). Украина должна приложить определенные усилия, чтобы отечественные специалисты были включены в различные группы и проекты, которые проводятся под руководством Европейской комиссии в этой сфере.

4. Ближайшей задачей разработчиков является анализ требований стандартов системы М460 и определения путей гармонизации стандартов с национальными стандартами в данной сфере. Наиболее рациональным подходом к гармонизации в данной сфере является гармонизация европейских стандартов методом обложки. В противном случае имеется риск отставания Украины от mainstream европейской стандартизации в данной сфере.

**Литература**

[1] Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS).

[2] Servida A. Draft Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) // European Forum on Electronics Signature (EFPE 2014). – Miedzyzdroje, Poland. – www.efpe.pl.

[3] Директива Европейского парламента и совета Европы от 13.12.1999 о системе электронных подписей, применяющихся в границах Союза.

[4] Закон України «Про електронний документ та електронний документообіг» №851-IV від 22.05.2003.

[5] Закон України «Про електронний цифровий підпис». № 852-IX від 22.05.2003.

[6] Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». №2594- IV від 31.05.2005 р.

[7] Горбенко Ю.І. Сутність законодавчих основ та умови надання довірчих послуг в ЕС в період 2015-2030 рр. // Захист інформації. – Т.15, №2. – С. 164–174.

[8] Горбенко Ю.І., Гончарова Ю.В. Електронна ідентифікація: поняття, визначення, вимоги // Радіотехніка. – Вип. 176. – 2014. – С. 138–144.

[9] Горбенко Ю.І. Сутність та необхідність виконання додаткових вимог відносно надання довірчих послуг в ЕС та Україні в період до 2015-2030 років. // Радіотехнгіка. – Вип.176. – 2014. – С.145–152.

[10] European interoperability Framework (EIF). Towards Interoperability for European Public Services // European Commission. – 2011.

[11] Jon Ølnes. Technical aspects of the eIDAS regulation // European Forum on Electronics Signature (EFPE 2014). – Miedzyzdroje, Poland. – www.efpe.pl.

[12] Arno Fiedler. EU eSignature Standards – making e-signatures (easy?) in the EU and beyond. Overview of the M/460 rationalisation executed so far and future challenges in the context of eIDAS Regulation // European Forum on Electronics Signature ( EFPE 2014). – Miedzyzdroje, Poland. – www.efpe.pl.

[13] Standardisation mandate m460 to CEN and ETSI on electronic signatures https://ec.europa.eu/digital-agenda/en/news/standardisation-aspects-esignatures.

[14] ISO/IEC 14516 Information technology -- Security techniques -- Guidelines for the use and management of Trusted Third Party services.

[15] ISO/IEC 15408-3 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components.

[16] ISO 29115:2013 Information technology – Security techniques – Entity authentication assurance framework.

[17] Luca Castellani. The contribution of UNCITRAL texts on electronic commerce to cross-border electronic transactions: an European perspective. // European Forum on Electronics Signature (EFPE 2014). – Miedzyzdroje, Poland. – www.efpe.pl.

Поступила в редколлегию 15.05.2014

**Потий Александр Владимирович,** доктор технических наук, профессор, профессор кафедры безопасности информационно-телекомуникационных систем Харьковского национального университета им. Каразина. Научные интересы: проектирование комплексных систем защиты информации, криптографических средств защиты информации; методы системного анализа процессов защиты информации; методы оценки безопасности объектов информационной деятельности.

**Горбенко Юрий Иванович**, фото и сведения об авторе см. на стр. 251.

**Корнейко Александр Васильевич,** кандидат технических наук, доцент, Первый заместитель Председателя Государственной службы специальной связи и защиты информации Украины. Научные интересы: криптографические системы и протоколы, проектирование и разработка систем, комплексов и средств криптографической защиты информации.

**Козлов Юрий Николаевич,** начальник отдела организации обеспечения услугами электронной цифровой подписи и сопровождения информационно-телекоммуникационной системы центрального удостоверяющего органа ГП «Информационный центр» Министерства юстиции Украины. Научные интересы: проектирование информационно-телекоммуникационных систем центров сертификации ключей; проектирование комплексных систем защиты информации в информационно-телекоммуникационных системах органов государственной власти; методы системного анализа процессов защиты информации; методы оценки безопасности объектов информационной деятельности.

**Пушкарев Андрей Иванович,** директор Департамента криптографической защиты информации Администрации Госспецсвязи Украины, лауреат Государственной премии Украины в области науки и техники. Научные интересы: криптографическая защита информации.

**Горбенко Иван Дмитриевич,** фото и сведения об авторе см. на стр. 216.

УДК 681.3.06(07)

**EIDAS: принципи надання довірчих електронних послуг і проблема інтероперабельності** / О.В. Потій, Ю.І. Горбенко, А.В. Корнейко, Ю.Н. Козлов, А.І. Пушкарьов, І.Д. Горбенко // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 252–260.

В роботі на основі аналізу законодавства ЄС формулюється система принципів надання електронних довірчих послуг. Розглядаються принципи електронної ідентифікації та принципи надання електронних довірчих послуг. Окремо розглядаються проблеми інтероперабельності в даній сфері, а також підхід європейських організацій до стандартизації щодо вирішення питань технічної інтероперабельності.

*Ключові слова:* електронна ідентифікація, електронні довірчі послуги, інтероперабельность.

Рис.: 3. Бібліогр.: 17 найм.

UDC 681.3.06(07)

**EIDAS: principles of providing confidence electronic services and interoperability problem** / A.V. Potiy, Yu.I. Gorbenko, A.V. Korneyko, Yu.N. Kozlov, A.I. Pushkarev, I.D. Gorbenko // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 252–260.

The paper formulates a system of principles of providing electronic confidence service on the basis of analyzing the EU legislation . Principles of e-identification and those of providing electronic confidence services are considered. Interoperability problems in this area, as well as the approach of the European standardization organizations to standardization and solution of problems of technical interoperability are considered separately.

*Keywords:* electronic identification, electronic confidence services, interoperability.

Fig.: 3. Ref.: 17 items.