
Евразийская Экономическая Комиссия

Государственная Дума Российской Федерации

Министерство связи и массовых коммуникаций Российской Федерации

Федеральная служба безопасности Российской Федерации

Федеральная служба по техническому и экспортному контролю

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

Федеральное казначейство

Правительство Санкт-Петербурга

Центральный Банк Российской Федерации

ОАО «Газпром»

ОАО «Ростелеком»

ОАО «РЖД»

Межрегиональная общественная организация

«Ассоциация защиты информации»

Технический комитет по стандартизации (ТК 26)

«Криптографическая защита информации»

Ассоциация Электронных Торговых Площадок

Всероссийский союз страховщиков

МЕМОРАНДУМ

Десятой международной научно-практической конференции

«РКИ-Форум Россия 2012»

18 – 20 сентября 2012 года в Санкт-Петербурге состоялась юбилейная десятая ежегодная международная научно-практическая конференция «РКИ-Форум Россия 2012». Организатором конференции выступила Межрегиональная общественная организация

«Ассоциация защиты информации» при активной поддержке Минкомсвязи России и Федеральной службы безопасности Российской Федерации.

В конференции приняли участие более 280 представителей из 7 стран, включая Беларусь, Венгрию, Казахстан, Польшу, Российскую Федерацию, Украину, Эстонию, а также представители Евразийской Экономической Комиссии.

От Российской Федерации в работе конференции участвовали руководители и специалисты 64 удостоверяющих центров, 23 федеральных органов власти, 33 региональных органов власти, 116 предприятий различных форм собственности, 5 учебных заведений, 13 общественных организаций и некоммерческих партнерств, представители 5 средств массовой информации.

На пленарном и четырех секционных заседаниях «РКИ-Форум Россия 2012» были представлены 49 докладов, проведено одно заседание в формате круглого стола и одно заседание в формате «Часа эксперта», подписано соглашение о сотрудничестве между Оргкомитетами конференций по проблематике электронной подписи и инфраструктуры открытых ключей Польши, Российской Федерации и Украины. В очередной раз РКИ-Форум стал эффективной площадкой для переговоров коммерческих организаций и предприятий.

В рамках работы секций и круглых столов был рассмотрен опыт удостоверяющих центров, производителей, интеграторов, эксплуатирующих организаций по вопросам внедрения и эксплуатации систем, использующих сервисы инфраструктуры открытых ключей, в том числе ориентированных на инфраструктуру электронного правительства. Участники конференции подвели итоги за год практической деятельности в сфере применения РКИ в информационных системах предприятий и организаций, выявили проблемные вопросы отрасли, обобщенные в настоящем Меморандуме, а также наметили конкретные цели по развитию РКИ, расширению практики применения данных технологий на 2013 год.

Главной особенностью «РКИ-Форума» в 2012 году явилось то, что он проходил в период активной деятельности Минкомсвязи и ФСБ по аккредитации удостоверяющих центров, в соответствии с Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи» (далее 63 -ФЗ), в период активной модернизации общегражданского законодательства и нормативного регулирования в смежных областях, а так же в период начала функционирования аккредитованных удостоверяющих центров и информационных систем, ориентированных на использование различных видов электронной подписи, в соответствии с новым законодательством. Данные обстоятельства в целом определяют переходный этап становления инфраструктуры открытых ключей в Российской Федерации, определяют перспективы развития проблематики РКИ на ближайшее время. Анализу опыта аккредитации и деятельности аккредитованных УЦ был посвящен ряд докладов, вызвавших значительный интерес участников Форума. В том числе было отмечено, что ФСБ в тесном сотрудничестве с Минкомсвязью и разработчиками средств УЦ и ЭП в сжатые сроки организовали доработку указанных средств. К настоящему времени проведена оценка соответствия требованиям приказов ФСБ №795 и №796 порядка 20 средств ЭП и УЦ. При этом значительные затруднения в процессе подготовки к аккредитации у участников рынка услуг удостоверяющих центров вызвало решение вопросов об обеспечении финансовой ответственности. Наибольшее число аккредитованных УЦ выполнили это требование путем заключения договора страхования ответственности. Однако, активные участники рынка страховых услуг, представленные на Форуме Всероссийским Союзом

Страховщиков (ВСС), отмечают, что на сегодня существует организационно-финансовая коллизия, по вопросу страхования ответственности УЦ. Нельзя считать, что предлагаемый в рамках аккредитации удостоверяющих центров страховой продукт на сегодня соответствует реальным рискам, деятельности УЦ. Требуется продолжение работы в рамках организованной в ВСС рабочей группы по данной тематике, с участием представителей Минкомсвязи России и представителей УЦ.

Значительный интерес участников Форума вызвал доклад, посвященный анализу законодательства, нормативного регулирования и правоприменительной практики в области электронной подписи и в смежных областях. В частности, отмечено, что ряд судебных споров, в которых существенную роль играют подписанные электронными подписями документы, обусловлена недостатками законодательства и договорной базы. Договорная документация часто не приводится в соответствие с действующим законодательством. Кроме того, в сферу проблематики ЭП должны попасть возникающие новые правовые институты и конструкции, такие как новые виды юридических лиц, «юридически значимое сообщение», и др. В части правового регулирования также актуальной является также гармонизация российского законодательства об ЭП с иностранным и международным правом в том числе с изменениями, которые предполагается внести в Европейскую директиву 1999/93.

Одной из главных тем Форума по-прежнему является тема единого пространства доверия сертификатам ключей проверки подписей (ЕПД). Рассмотрены правовые и технологические аспекты создания и функционирования ЕПД, информация об имеющихся мировых тенденциях в этой сфере. По мнению участников Форума, проводимая процедура аккредитации удостоверяющих центров не закрывает все аспекты, которые необходимо учесть при формировании ЕПД. В этой связи наиболее острой является задача учета различных уровней криптографической защиты при формировании отношений доверия. Отмечено, что для эффективного функционирования ЕПД необходимо рассмотреть целый комплекс первоочередных мер, учитывающих положения 63-ФЗ, в частности:

- нормативное закрепление границы ЕПД и порядок (регламент) его функционирования;
- нормативное разделение требований к сертификатам криптографических ключей, используемым для различных целей;
- нормативное закрепление требований по интероперабельности отечественных РКІ-систем при переходе на межведомственное и межуровневое взаимодействие при предоставлении государственных услуг в электронном виде;
- стандартизация форматов и интерфейсов сервисов и служб РКІ, включая стандартизацию форматов электронной подписи, используемых для целей межведомственного взаимодействия и предоставления государственных и муниципальных услуг;
- публичное информирование пользователей информационных систем о степени риска инфкоммуникационного взаимодействия с использованием различных по надежности способов и средств идентификации и аутентификации;
- формирование однородных публичных критериев к удостоверяющим центрам для последующей оценки качества их деятельности и доверия к реализуемым ими сервисам безопасности;
- обеспечение непрерывного мониторинга деятельности аккредитованных УЦ со стороны уполномоченных органов и общества;

- создание организационных и правовых условий для развития служб подтверждения полномочий участников информационного взаимодействия.

Часть вышеприведенных направлений построения ЕПД потребует адекватного и обязательного технического регулирования, которое в России в настоящее время отсутствует и не определен соответствующий регулятор.

Большое внимание участники конференции уделили теме межведомственной, межрегиональной, трансграничной и межгосударственной интероперабельности РКІ. Основными прикладными задачами, требующими трансграничной интероперабельности на протяжении ряда последних лет были и остаются задачи электронной коммерции, предварительного декларирования товаров в пограничных операциях, широкий спектр банковских приложений. Требование ст. 13 Федерального закона от 21 июля 2005 г. № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд», определяющее равный правовой режим для товаров и услуг, происходящих из иностранных государств, «Соглашение о государственных (муниципальных) закупках (г. Москва, 9 декабря 2010 года)» Комиссии Таможенного Союза предполагают наличие технологий трансграничной интероперабельности электронных подписей участников электронных торгов системы государственного заказа. В этой связи большой интерес вызвали доклады, в которых были представлены результаты развития сервисов, обеспечивающих интероперабельность электронной подписи.

Участники Форума отметили, что в целях реализации требований 63-ФЗ аккредитованным УЦ целесообразно предоставить возможность доступа к СМЭВ с целью упрощения процедуры проверки первичных документов заявителей на изготовление СКПП (выписка из ЕГРЮЛ в ФНС, соответствие ФИО-СНИЛС в ПФР и соответствие ФИО-номер_паспорта в МВД). Также была затронута актуальная проблема невозможности удовлетворения требований к наполнению сертификатов со стороны неограниченного круга информационных систем. Одним из предложенных способов решения данной проблемы является использование атрибутивных сертификатов для размещения дополнительных данных, полномочий, ролей и привилегий владельца сертификата ключа проверки электронной подписи. Данный способ базируется на международных стандартах и зарубежном опыте создания систем управления ролей и привилегий с использованием инфраструктуры открытых ключей.

При этом отмечено, что проблемы интероперабельности информационных технологий и средств защиты информации различных производителей частично могут быть решены в рамках деятельности технических комитетов (далее - ТК) по стандартизации, действующих в системе технического регулирования России. В частности, в ТК26 «Криптографическая защита информации» уже ведутся работы по выработке согласованной позиции в части стандартизации контейнеров хранения и транспортных контейнеров криптографических ключей, а также стандартизации интерфейсов СКЗИ.

Форум отмечает увеличение количества нормативных правовых актов Российской Федерации, определяющих необходимость использования усиленной электронной подписи. Возрастает и количество пользователей таких систем. Особый интерес участников форума вызвало обсуждение вопросов использования развитой инфраструктуры аккредитованных удостоверяющих центров для оказания услуг в интересах пользователей Единого портала государственных услуг www.gosuslugi.ru. За год работы количество пользователей данного

портала превысило 1 миллион и продолжает увеличиваться по мере введения в действие новых публичных сервисов электронного правительства. Данное обстоятельство приводит к необходимости применения высоконадежных средств и способов аутентификации участников информационного взаимодействия, активного применения технологий на основе открытых ключей для решения задач защиты персональных данных.

Актуальность этой темы также определяется требованиями ряда нормативных актов, определяющих порядок взаимодействия с иностранными контрагентами, а также интересами секторов B2B и B2G. В этой связи отмечено, что технологии РКІ являются эффективным решением, на базе которого успешно строятся безопасные интероперабельные решения в информационных процессах развитых стран, в том числе в проектах электронного правительства, информационного общества, электронной коммерции, электронного страхования, в задачах защиты персональных данных и другой информации ограниченного доступа и т.д.. В ряде докладов отечественных и зарубежных экспертов прозвучало подтверждение того факта, что поиск эффективных решений задачи интероперабельности электронной подписи и строгой аутентификации одинаково актуальны для России, Евросоюза, стран СНГ, ЕврАзЭС, ШОС, АТЭС и других государств и межгосударственных объединений. Отмечена и поддержана активная позиция Минкомсвязи России и ряда экспертных организаций-участников РКІ-Форума в части, касающейся разработки и продвижения в международных объединениях универсальных подходов к обеспечению интероперабельности, а также юридической и доказательной силы электронного юридически значимого документооборота.

Участниками Форума обсуждена тематика длительного хранения электронных документов с обеспечением их юридической силы и подтверждения подлинности электронных подписей за пределами срока жизни ключей проверки электронной подписи и сертификата ключа проверки электронной подписи. Участники обсуждения констатируют необходимость приоритетного развития нормативной и технологической базы в этой части в связи с быстро растущим интересом по переводу государственных и муниципальных услуг в электронный вид. А именно, предложено разработать государственный стандарт о применении технических средств для обеспечения долговременного архивного хранения электронных документов, созданных с использованием средств квалифицированной электронной подписи.

В свою очередь, данное направление потребует также опережающего развития института электронного нотариата для обеспечения нотариального свидетельствования электронных событий и фактов правоотношений в электронном виде как между физическими, так и между юридическими лицами..

Выделение на Форуме экономических аспектов развития РКІ становится традицией. Принимая во внимание важность экономики, как движущей силы развития отрасли участники Форума с большим интересом обсудили актуальные экономические аспекты в рамках тематической секции.

Большое внимание в программе Форума уделено прикладным вопросам РКІ. В этой части отмечено, что в настоящее время одним из основных драйверов роста массового применения РКІ являются электронные торги. И в перспективе эта тенденция будет усиливаться. Причиной тому являются новации нормативного регулирования в области электронной торговли – Федеральный закон от 18 июля 2011 г. N 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» и законопроект «Федеральной контрактной системы», а так же

Соглашение о государственных (муниципальных) закупках (г. Москва, 9 декабря 2010 года), ратифицированное участниками Единого Экономического Пространства.

В ходе дискуссий отмечен неизменно растущий на протяжении последних лет уровень Форума и глубина рассматриваемых на мероприятиях Форума вопросов, степень зрелости представляемых на конференции РКІ-ориентированных продуктов и решений. По общему мнению, «РКІ-Форум Россия» за свою десятилетнюю историю стал эффективной площадкой для обмена мнениями и рассмотрения актуальных вопросов в области РКІ на национальном, региональном и на международном уровне.

Заслушав и обсудив круг вопросов, связанных с использованием инфраструктуры открытых ключей, участники Конференции решили:

1. Направить настоящий Меморандум в Евразийскую Экономическую Комиссию, Комитеты Государственной Думы РФ по экономической политике, инновационному развитию и предпринимательству, Минкомсвязи России, Минюст России, ФСБ России, Минэкономики России, МВД России, Минобрнауки России, Федеральное Казначейство, ФТС России, ФНС России, ПФР, в Правительство Санкт-Петербурга, в ОАО «Ростелеком», ОАО «Газпром», ОАО «Универсальная электронная карта», ОАО «РЖД».
2. Довести до участников процесса создания электронного правительства (Минкомсвязи России, ОАО «Ростелеком», ОАО «Универсальная электронная карта») позицию РКІ-сообщества по ключевым вопросам, затронутым в настоящем Меморандуме и других материалах Форума, с целью рассмотрения ими возможностей использования предложений и компетенций РКІ-сообщества при решении базовых задач создания электронного правительства, в том числе в работах по совершенствованию единого пространства доверия инфраструктуры открытых ключей как технологической основы при получении государственных (муниципальных) услуг в электронном виде. В частности, отмечалась целесообразность приоритетного использования квалифицированной усиленной электронной подписи при получении государственных (муниципальных) услуг в электронном виде.
3. Довести до сведения профильных комитетов Государственной Думы Федерального собрания Российской Федерации предложения по конкретным вопросам, требующим доработки в федеральном законе № 63-ФЗ «Об электронной подписи». В частности, следует обратить внимание на такие насущные вопросы, как регулирование использования меток времени и их правового статуса; легализация технологии переподписания документов, подписанных усиленной электронной подписью; способы доказывания подлинности электронной цифровой подписи при длительном хранении (за пределами срока действия сертификата ключа подписи подписанта и/или удостоверяющего центра), использование электронных подписей государственными электронными архивами для обеспечения целостности и аутентичности электронных архивных документов. В том числе разработать правовые нормы, регулирующие использование сервисов доверия (проверки подлинности электронной подписи, меток времени, атрибутивных сертификатов, архивного хранения и др.). Одним из решений может быть дополнение пункта 3 статьи 8 указанного закона положением об обязанности головного удостоверяющего центра обеспечивать сохранность документации ликвидируемых (реорганизуемых) аккредитованных удостоверяющих центров.
4. Поддержать инициативу Комитета Государственной Думы РФ по экономической политике, инновационному развитию и предпринимательству по организации Экспертного совета по развитию юридически-значимого электронного документооборота и применению электронной подписи. При этом обратиться с предложением о привлечении

к работе Экспертного совета общественных организаций, представляющих интересы РКІ-сообщества (Межрегиональная общественная организация «Ассоциация защиты информации», РОСЭУ, АЭТП).

5. Обратить внимание представителей органов государственной власти, предприятий и организаций, физических лиц, на необходимость приведения и поддержания договорной базы в части электронного документооборота и электронной подписи в соответствии с динамично меняющимся законодательством.
6. Поддержать инициативу Всероссийского Союза Страховщиков по организации в рамках рабочей группы с участием Минкомсвязи России и представителей УЦ процесса согласования и оптимизации страховых продуктов для удостоверяющих центров и рекомендовать продолжить эту работу.
7. Обратить внимание Минкомсвязи России, ФСБ России и ТК26, что в связи с вступлением в силу стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 целесообразно совместно провести работу:
 - по определению объектных идентификаторов (OID) соответствующих алгоритмов согласно ITU-T X.660;
 - по определению ASN.1 нотаций;
 - по включению соответствующих полей в структуру квалифицированных сертификатов, утвержденных приказом ФСБ №796.
8. Рекомендовать техническому комитету ТК26 и ТК362 включить в план приоритетных направлений работы при поддержке Минкомсвязи России и ФСБ России адаптацию международных стандартов и развитие национальных стандартов в области РКІ, в частности – стандартов использования РКІ для организации защищенных каналов связи (SSL/TLS), стандартов форматов электронных документов с электронной подписью (в том числе архивных).
9. С целью дальнейшей совместимости СКЗИ различных разработчиков и повышения удобства потребителей в части возможности работы в различных защищенных системах рекомендовать при построении государственных систем с применением ЭП использовать СКЗИ с поддержкой форматов транспортного контейнера и контейнера хранения, разрабатываемых в рамках ТК26.
10. Считать целесообразным проведение очередной юбилейной XI международной научно-практической конференции «РКІ-Форум Россия» в Санкт-Петербурге в 2013 году.
11. Включить в программу деловой части «РКІ-Форум Россия 2013» выступление представителя Минкомсвязи России с отчетом о правоприменительной практике ФЗ-63 за I полугодие 2013 года.

Участники конференции выражают искреннюю благодарность:

- Оргкомитету, программному комитету и рабочей группе Форума за проделанную на высоком уровне работу по организации и проведению мероприятия.
- Представителям иностранных делегаций за ценную информацию, предоставленную в докладах и презентациях, об опыте стран ЕС и СНГ в области использования РКІ.
- Стратегическому бизнес-партнеру Форума - компании «Газинформсервис», Официальным партнерам Форума - компаниям «ИнфоТеКС», ООО «КРИПТО-ПРО», НП «Национальный удостоверяющий центр», ОАО «РЖД», партнерам деловой программы - компаниям «Аладдин», «Актив», «Аванпост», «Gemalto», компаниям и организациям, осуществлявшим организационную поддержку, в том числе МОО «АЗИ», Техническому комитету по стандартизации ТК26 «Криптографическая

защита информации», компании «Авангард-Центр», Компании «АНК» и информационным партнерам за финансовую, информационную и организационную поддержку конференции.

- Правительству Санкт-Петербурга за неизменное внимание к конференции, участие и поддержку.

Сопредседатель конференции
Президент Межрегиональной
общественной организации
«Ассоциации защиты информации»,
член- корреспондент Академии криптографии РФ,
действительный государственный советник 3 класса



Г.В. Емельянов