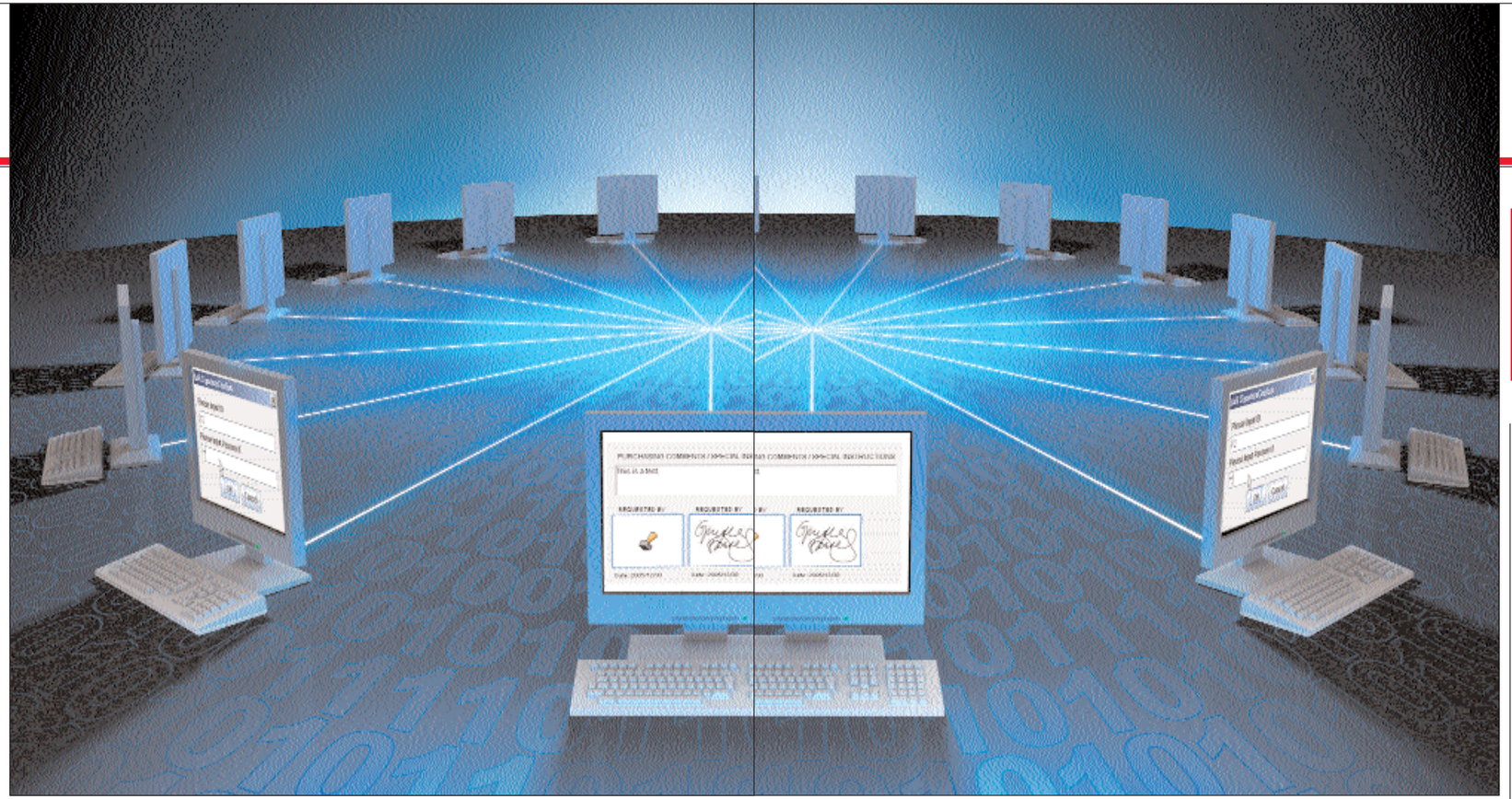
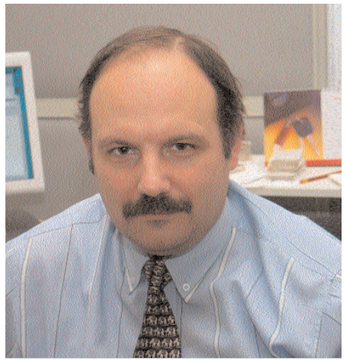




■ **Илья ТРИФАЛЕНКОВ**,
начальник Отдела информационной безопасности проекта «Информационное общество» ОАО «Ростелеком»

ЭЛЕКТРОННАЯ ПОДПИСЬ В ИНФРАСТРУКТУРЕ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

ПРОЕКТЫ ПРОГРАММЫ «ИНФОРМАЦИОННОЕ ОБЩЕСТВО» ОБОСНОВАННО НАХОДЯТСЯ В ФОКУСЕ ВНИМАНИЯ КАК ПРОФЕССИОНАЛОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ТАК И ОБЩЕСТВА В ЦЕЛОМ

Видимо, в силу высоких темпов развития этих проектов даже представления профессионалов о состоянии работ, основных подходах и направлениях развития проектов программы «Информационное общество» не всегда соответствуют реальной ситуации. В связи с этим хотелось бы рассмотреть, что представляет программа «Информационное общество», каковы её основные особенности, какое место занимает в ней создание электронного правительства.

«ИНФОРМАЦИОННОЕ ОБЩЕСТВО» И ИНФРАСТРУКТУРА ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

Собственно программа «Информационное общество» была принята как развитие более раннего проекта «Электронная Россия». При этом, учитывая накопленный опыт, постарались избежать ошибок, проявившихся при реализации федеральной целевой программы «Электронная Россия». В частности:

- проекты ФЦП «Электронная Россия» пытались охватить весь спектр применения информационных технологий, что привело к невозможности расстановки приоритетов и, как следствие, распылению средств и общей низкой эффективности проектов ФЦП;
- проекты ФЦП оказались наиболее успешными в части ведомственной автоматизации, особенно там, где не предполагалось обеспечивать межведомственное взаимодействие. В результате никаких механизмов межведомственного взаимодействия создано не было, и интеграция ведомственных систем превратилась в тяжелую задачу;
- создание систем, обслуживающих преимущественно внутренние процессы органов исполнительной власти, за редким исключением, никак не улучшило качество обслуживания конечных потребителей государственных услуг – граждан и юридических лиц;
- ФЦП «Электронная Россия» не имела четко определенных подходов, единой технической и технологической политики, единой инфраструктуры.

Программа «Информационное общество» призвана скомпенсировать недостатки предыдущей программы. В ней предусмотрены:

- ориентация на предоставление услуг конечным потребителям, как юридическим лицам, так и гражданам. При этом набор услуг не ограничивается только государственными услугами, а создается целый спектр национальных информационных услуг, потенциально предоставляемых как для решения задач электронного правительства, так и иным потенциальным пользователям;
- организация эффективного межведомственного взаимодействия для предоставления государственных услуг с использованием уже существующих систем автоматизации деятельности органов исполнительной власти, как федерального, так и регионального уровней;
- проведение единой технической и технологической политики единого оператора услуг и использование его инфраструктуры.

Таким образом, проект «Информационное общество» далеко не ограничивается электронным правительством, хотя это направление является значимым (***схема № 1***).

Электронное правительство – это форма организации деятельности органов государственной власти, обеспечивающаяся за счет широкого применения информационно-коммуникационных технологий (ИКТ)

Говоря собственно об услугах электронного правительства, хотелось бы разделить собственно электронное правительство и его инфраструктуру.

Электронное правительство – это форма организации деятельности органов государственной власти, обеспечивающая за счет широкого применения информационно-коммуникационных технологий (ИКТ) качественно новый уровень оперативности и удобства для организаций и граждан, которым предоставляются государственные услуги и информация о результатах деятельности государственных органов.

В то же время инфраструктура электронного правительства (ИЭП) – это совокупность автоматизированных и телекоммуникационных систем, обслуживающих процессы информационного взаимодействия всех субъектов электронного правительства, поддерживая необходимый уровень предоставления государственных услуг потребителям в электронной форме (***схема № 2***). Именно эта инфраструктура создается в рамках программы «Информационное общество».

ЭЛЕКТРОННАЯ ПОДПИСЬ В ПРОЕКТАХ «ИНФОРМАЦИОННОГО ОБЩЕСТВА»

Переход на предоставление услуг в электронном виде требует обеспечения такой же степени безопасности и доверия, как в традиционных механизмах предоставления услуг. При этом в рамках услуг инфраструктуры

Схема 1:
ПРОЕКТ «ИНФОРМАЦИОННОЕ ОБЩЕСТВО»

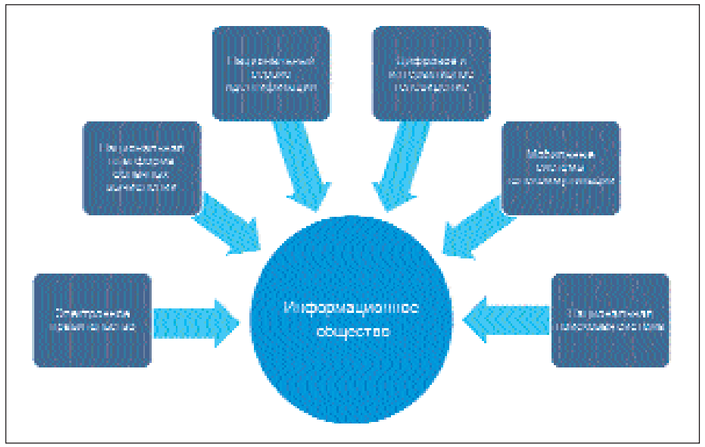
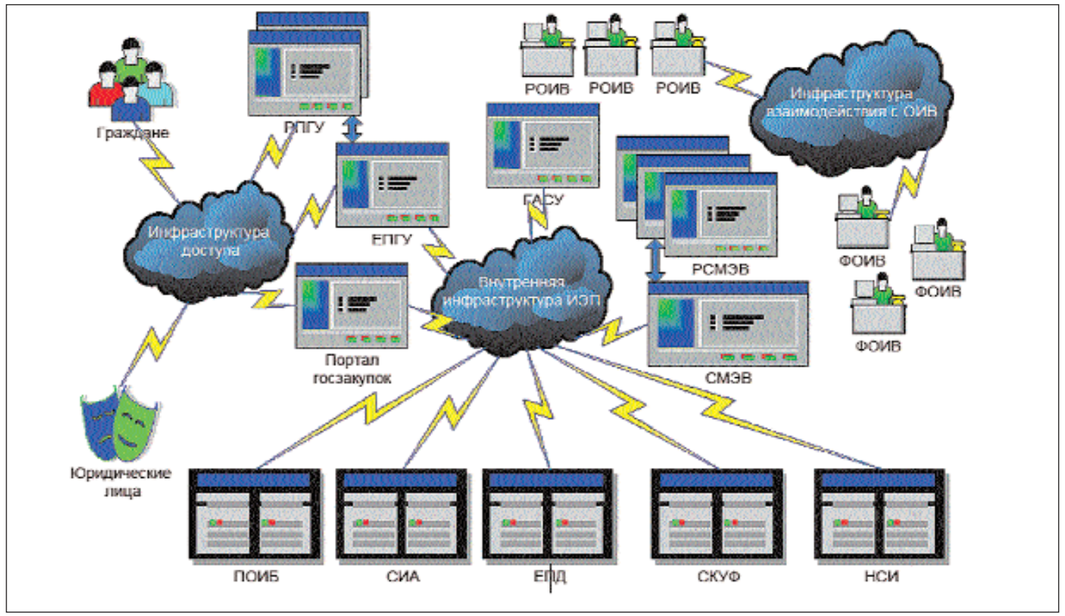


Схема 2:
АРХИТЕКТУРА ИНФРАСТРУКТУРЫ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА



Применение электронной подписи для авторизации получателей государственных информационных услуг в электронной форме, в особенности юридически значимых, осложнено очень большими объёмами запросов и разнообразием вариантов доступа – с домашнего компьютера, телевизионных приставок и различных мобильных устройств и др.

электронного правительства присутствует целый ряд существенных особенностей по сравнению с традиционными механизмами предоставления услуг, в том числе ведомственного или корпоративного уровня. В их числе:

- необходимость массового предоставления сложных услуг широким группам пользователей, у которых самый различный (к сожалению, в большинстве – минимальный) уровень подготовки к использованию информационных технологий;
- минимальная возможность добиваться выполнения необходимых требований к среде конечного пользователя либо порядку его работы;
- возможность злоупотреблений и правонарушений, растущая по мере увеличения номенклатуры и значимости таких услуг;
- потребность разработки, параллельно с самими услугами, нормативной базы их предоставления;
- необходимость использования современных технологий обработки информации при возможных потенциальных уязвимостях этих технологий.

Решение задачи обеспечения необходимого уровня доверия невозможно без широкого применения механизмов электронной подписи. При этом электронная подпись в рамках услуг инфраструктуры электронного правительства может применяться для:

- доступа заявителей услуг к данным личного кабинета, содержащего конфиденциальную информацию (для юридического лица) и персональные данные (для граждан);
- подтверждения заявок на исполнение услуг, в том числе информации в составе заявки, включая прилагаемые электронные документы;
- доступа сотрудников ведомств к услугам системы межведомственного электронного взаимодействия в соответствии с их полномочиями и полномочиями ведомств;
- подтверждения содержания запроса на предоставление информации со стороны запрашивающего ведомства и предоставляемой информации при исполнении запроса;
- подтверждения фактов передачи запроса и его исполнения в системе межведомственного электронного взаимодействия.

Последние два из перечисленных вариантов являются наиболее простыми, поскольку представляют собой, по сути, технологические подписи. Применение таких видов подписи легализовано в новой версии Закона об электронной подписи 63-ФЗ. В таком случае главная проблема в производительности систем, осуществляющих проверки сертификатов и самих электронных подписей.

Более сложной является ситуация с использованием электронной подписи для подтверждения прав сотрудников ведомств пользоваться услугами межведомственного взаимодействия. Трудность – в необходимости ведения реестра полномочий, что является непростой задачей даже для федеральных ведомств уровня, не говоря уже о региональных. Вряд ли решение этой задачи целесообразно возлагать на оператора системы межведомственного электронного взаимодействия. Оптимальным явилось бы внедрение распределенного механизма назначения полномочий, причем ведение реестра полномочий должно осуществляться силами ведомств.

Самый сложный – вопрос об использовании электронной подписи заявителями как при авторизации доступа к личному кабинету, так и при подтверждении заявок на получение государственных услуг. Проблема заключается, с одной стороны, в массовости предоставляемых услуг, с другой стороны, в разнообразии вариантов доступа пользователей. Такой доступ может осуществляться со специализированных устройств – инфоматов и телевизионных приставок, домашних компьютеров, а также различных мобильных устройств. При этом сами услуги могут быть различными, от чисто информационных (получения справок или свидетельств) до юридически значимых.

Сегодня в инфраструктуре электронного правительства реализовано два вида авторизации пользователей. Первый из них, по традиционному варианту логин-пароль, предназначен для получения информационных услуг. Второй вариант, при выдаче юридически значимых документов, предусматривает применение квалифицированной электронной подписи для авторизации. При этом для минимизации рисков, связанных с пользовательской средой, применяются решения, обеспечивающие выполнение электронной подписи без передачи ключей подписи с ключевого носителя.

Перспектива широкого применения для работы с порталом государственных услуг мобильных устройств требует, чтобы спектр способов авторизации пользователей и вариантов применения электронной подписи был расширен. По-видимому, рассчитывать на хранение ключей и сертификатов электронной подписи непосредственно в мобильном устройстве нецелесообразно, поскольку надёжно ограничить доступ к мобильному устройству, по большому счёту, нереально. Решением может быть разделение процедур авторизации и использования электронной подписи, с применением, во-первых, схемы аутентификации с помощью одноразовых паролей и, во-вторых, централизованного хранения ключей электронной подписи на специализированных устройствах.

Вторым важным вопросом является подтверждение соответствия личности гражданина и электронных средств идентификации. При использовании ключей и сертификатов электронной подписи необходимо быть уверенным, что соответствующие ключи выданы именно тому физическому лицу, которое осуществляет работу с инфраструктурой электронного правительства. Для электронных карт и ключей такое соответствие обеспечивается проверкой документов при их заказе и выдаче. Эта процедура требует четкой регламентации проверки и определения ответственности выдающей организации.

В частности, далеко не все сертификаты и ключи электронной подписи, выданные ранее даже аккредитованными Удостоверяющими центрами, могут использоваться для работы с ресурсами инфраструктуры электронного правительства. Если говорить о мобильных устройствах, то определение чёткого соответствия пользователя мобильного устройства с конкретным физическим лицом является сложной задачей и требует изменений нормативной базы.

Таким образом, существует целый ряд проблем, решение которых требуется для обеспечения эффективного механизма предоставления услуг с использованием инфраструктуры электронного правительства. Взаимодействие различных федеральных, региональных органов исполнительной власти и третьих сторон делает важным создание единого пространства доверия. Для чего необходим перечень организационных и технических мер, обеспечивающих проверку электронных подписей в процессах как авторизации, так и подтверждения подлинности передаваемых электронных документов.

Функции единого пространства доверия существенно шире, чем просто

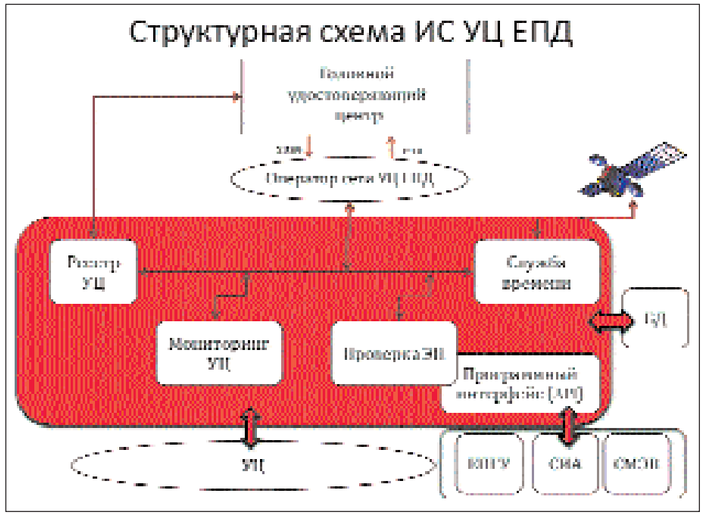
предоставление услуг информационным системам инфраструктуры электронного правительства. Тем не менее, значимость инфраструктуры электронного правительства накладывает существенные требования на организационные и технические решения при создании единого пространства доверия.

Единое пространство доверия включает в себя головной Удостоверяющий центр, информационную систему Удостоверяющих центров единого пространства доверия (ЕПД), а также множество аккредитованных и присоединенных к ЕПД удостоверяющих центров, обеспечивающих поддержку процессов управления сертификатами электронной подписи.

Информационная система Удостоверяющих центров единого пространства доверия (ИС УЦ ЕПД), предназначена для обеспечения информационно-технологической поддержки отношений по использованию электронных подписей, возникающих между субъектами. В том числе в процессах формирования и оказания электронных государственных и муниципальных услуг с помощью инфраструктуры электронного правительства.

Информационно-технологическая поддержка реализуется путем предоставления сторонам – субъектам отношений и взаимодействующим информационным системам – совокупности сервисов проверки и подтверждения аутентичности электронных подписей, для чего используются Удостоверяющие центры, входящих в Единое пространство доверенных Удостоверяющих центров. Структура ИС УЦ ЕПД приведена на ***схеме № 3***.

Схема 3:
ИНФОРМАЦИОННАЯ СИСТЕМА УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ ЕДИНОГО ПРОСТРАНСТВА ДОВЕРИЯ



ОТ ЕДИНОГО ПРОСТРАНСТВА ДОВЕРИЯ – К НАЦИОНАЛЬНОЙ УСЛУГЕ ИДЕНТИФИКАЦИИ

Обеспечение необходимого уровня доверия в инфраструктуре электронного правительства требует не только решения вопросов идентификации и аутентификации пользователей, но и вопросов предоставления полномочий пользователям. При этом структура полномочий оказывается достаточно сложной и определяется как статусом того или иного пользователя (гражданин, представитель юридического лица, представитель органа власти), так и способом обращения к инфраструктуре электронного правительства (посредством инфомата, мобильного устройства, с рабочего места). Данная задача требует создания принципиально новой услуги идентификации и авторизации, причем в национальном масштабе.

С использованием национального сервиса идентификации и авторизации в перспективе будет возможно обеспечить решение задач, связанных с управлением идентификационными и персональными данными пользователей при обращении ко всем видам электронного сервиса, предоставляемого разными организациями. Пользователей любых – физических лиц, индивидуальных предпринимателей, должностных лиц юридических лиц и сотрудников органов государственной власти. В зависимости от задач вопросы определения и назначения полномочий решаются не оператором сервиса, а его пользователями.

Наличие национального сервиса идентификации и авторизации позволяет получить следующие преимущества:

- быстрое создание систем разграничения доступа различного масштаба с использованием надежных механизмов идентификации и авторизации;
- обеспечение соответствия требованиям регуляторов систем, построенных с использованием этого сервиса;
- обеспечение эффективного и безопасного взаимодействия организаций различных типов, прозрачность использования информационного обмена;
- обеспечение заданного уровня безопасности персональных данных граждан РФ, контроль их использования;
- создание более широкого рынка услуг, в том числе новых, изменение качества услуг электронной подписи.

* * *

Применение электронной подписи в сочетании с сервисами авторизации позволит реализовать не меньший, а, возможно, больший уровень доверия электронных услуг в сравнении с традиционными услугами. И, тем самым, обеспечить реальный переход к инновационной экономике и новым формам организации деловой и общественной активности.

ВОЛЬНАЯ АССАМБЛЕЯ ЗАЩИТНИКОВ ИНФОРМАЦИИ

С 4 ПО 6 ОКТЯБРЯ ВСЕХ НЕРАВНОДУШНЫХ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (СВОЕЙ ИЛИ КОРПОРАТИВНОЙ) ЖДУТ НА КРАСНОЙ ПРЕСНЕ, ГДЕ ПРОЙДЕТ ТРАДИЦИОННЫЙ ДЛЯ ОСЕНИ ФОРУМ «INFOBEZ-EXPO/ИНФОБЕЗОПАСНОСТЬ».

Главный вопрос, который задают себе потенциальные посетители: что нового, кроме привычных стендов с решениями и (что уж скромничать!) блестящей конференционной программы, предложат организаторы. И здесь, не изменяя традициям, но возрождая и трансформируя их в современные реалии, организаторы (питерское выставочное объединение «РЕСТЭК») изменили форматы открытия форума, делового общения и проведения ряда мероприятий.

Перелистаем календарь INFOBEZ-EXPO. День первый, открытие, начнется с традиционного пленарного заседания. Затем вместо «генерального обхода» и перерезания ленточек все приглашаются на Ассамблею (ох уж эти питерцы!) в духе Петра I, непременным условием участия в которой станет обязательство приглашенных соблюдать Указ Петра I «О достоинстве гостевом, на ассамблеях быть имеющем». Впечатлениями от первого дня можно будет поделиться на «INFOBEZ-OKTOBER-FEST 2011». Подробности – на сайте организаторов.

Но не стоит расслабляться. После столь бурного начала, опять же согласно всем (и Петровским, и «инфобезовским») традициям, предстоит серьезная работа. В деловой программе следующий день форума - банковский, а третий и последний - отраслевой.

В промежутках между семинарами на актуальные темы рекомендуется пройти по выставке, где среди знакомых по прошлым форумам и известных на российском рынке ИБ названий компаний (системных интеграторов и поставщиков решений) будут и новые для мероприятия имена: Microsoft , G Data Software AG, Fortinet, CSBI, SAP, SafeNet, Imperva.

Конференция «INFOBEZ-EXPO/ИнфоБезопасность» давно заслужила Знак качества, благодаря и профессионалам-участникам, и важности и остроте обсуждаемых на семинарах и круглых столах проблем. Мода на «облака» вызывает у специалистов по ИБ справедливые опасения, поэтому семинары на эту тему и рекомендации экспертов «как не обжечься, внедрив на своем предприятии облачную экосистему» стали естественным отражением этой современной ИТ-тенденции.

В программе банковского дня – не менее актуальные проблемы дистанционного банковского обслуживания, обеспечения безопасности персональных данных, демонстрация возможностей управления инцидентами ИБ в процессе работы банка, особенности стандартизации и сертификации...

* * *

Особенно ожидаемы в этот день и два других мероприятия, уже заслужившие признание участников. Экспертная панель – конкурс вопросов ведущим экспертам отрасли, по результатам которой автор лучшего вопроса будет удостоен специального приза. А любимый всеми участниками рынка ИБ конкурс решений «Львы и Гладиаторы» невозможно описать. Это надо видеть!