Министерство образования и науки
Российской Федерации

САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

Д. Р. Трутнев

ИНФРАСТРУКТУРА ДОВЕРИЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Учебное пособие

Санкт-Петербург

2012

Трутнев Д. Р. **Инфраструктура доверия в государственных информационных системах:** Учебное пособие. – СПб.: НИУ ИТМО, 2012. – 95 с.

Учебное пособие посвящено изучению наиболее важных механизмов, обеспечивающих условия для создания доверительных отношений между участниками информационного обмена в современном государстве. Рассматривается специфика формирования пространства доверия и инфраструктуры открытых ключей; использования электронной подписи и идентификации личности с использованием электронных карт.

Издание адресовано студентам магистерской программы «Управление государственными информационными системами» по направлению 220100 «Системный анализ и управление» и слушателям дополнительной образовательной программы повышения квалификации «Электронное правительство и инновационные технологии управления», реализуемой Центром технологий электронного правительства НИУ ИТМО.

Рекомендовано к печати Ученым советом Магистерского корпоративного факультета (прот. № 1 от 06.04.2012).

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена Программа развития государственного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет информационных технологий, механики и оптики» на 2009–2018 годы.

© Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, 2012
© Д.Р.Трутнев, 2012

Оглавление

Введение

Бурное развитие сферы электронных услуг и строительство электронного правительства резко актуализировали проблему обеспечения информационной безопасности как в сетях организаций, так и в сетях общего пользования - Интернет. Как известно, решение этой проблемы достигается одновременным выполнением трех условий: доступности необходимой информации, целостности и конфиденциальности информационных ресурсов или, иными словами, обеспечением безопасности электронного документооборота. Устанавливая деловые контакты, стороны, субъекты информационных правоотношений, должны быть полностью уверены в «личности» партнеров, конфиденциальности обмена электронными документами и подлинности самих документов.

В последнее время термин «единое пространство доверия» стал довольно распространенным, особенно в связи с созданием электронного правительства и связанными с ним процессами образования ведомственных инфраструктур открытых ключей (PKI – Public Key Infrastructure), охватывающих всю страну.

Почти философское определение этого понятия дает Федеральная служба судебных приставов (ФССП): «Единое пространство доверия ключевой информации ФССП России – всеобъемлющая неделимая форма существования ключевой информации в ФССП России, при которой каждый пользователь средств криптографической защиты информации, использующий пространство доверия, может однозначно идентифицировать владельца сертификата ключа подписи по ключам электронной цифровой подписи»[1].

Другое определение дает в своих нормативных документах Федеральная налоговая служба: «Единое пространство доверия - структура, определяющая организационные границы, в пределах которых находятся только заслуживающие доверия удостоверяющие центры, а сертификаты ключей подписей, изготовленные ими, признаются всеми участниками информационного взаимодействия в границах структуры и на равных условиях»[2].

Своё определение есть и у Правительства Москвы: «Единое пространство доверия сертификатам ключей подписей - информационное пространство, в котором обеспечивается подтверждение подлинности

[1] Положение о ведомственном удостоверяющем центре ФССП России (Проект) - http://www.fssprus.ru/db/files/polojenie_ob_uc.doc

[2] Порядок регистрации участников электронного документооборота для представления налоговых деклараций (расчетов) и иных документов в электронном виде и информирования налогоплательщиков по телекоммуникационным каналам связи. Утв. Приказом ФНС России от 18 декабря 2009 г. № ММ-7-6/691@

электронной цифровой подписи вне зависимости от того, каким удостоверяющим центром изготовлен сертификат ключа подписи и какая программно-аппаратная платформа используется удостоверяющим центром»[3].

Методические рекомендации по разработке электронных сервисов и применению технологии электронной подписи (2011 г)[4] рассматривают следующие виды подписи:

- электронная подпись физического лица;
- электронная подпись информационных систем.

Безусловно, говоря об электронной цифровой подписи (ЭЦП) невозможно не затронуть проблему защиты информации. Минкомсвязью России формируется единое пространство доверия (ЕПД) – совокупность удостоверяющих центов, прошедших процедуру добровольного подтверждения соответствия требованиям по присоединению к ЕПД.

Единое пространство доверия обеспечивает информационно-технологическую поддержку при использовании ЭЦП в процессах оказания электронных государственных и муниципальных услуг с помощью инфраструктуры электронного правительства.

Учебное пособие «Инфраструктура доверия в государственных информационных системах» предназначено для использования в рамках магистерской программы «Управление государственными информационными системами» по направлению «Системный анализ и управление».

Курс (учебный модуль) предназначен также для использования в рамках системы дистанционного обучения Магистерского корпоративного факультета НИУ ИТМО и ориентирован на реализацию дополнительной образовательной программы повышения квалификации «Электронное правительство и инновационные технологии управления». Программа реализуется Центром технологий электронного правительства НИУ ИТМО и ориентирована на повышение квалификации государственных и муниципальных служащих по вопросам развития электронного правительства, информационного общества, применения инновационных

[3] Термины и определения. Приложение к «Положению о системе уполномоченных удостоверяющих центров органов исполнительной власти города Москвы» (утв. постановлением Правительства Москвы от 26 июля 2005 г. № 544-ПП)

[4] Методические рекомендации по разработке электронных сервисов и применению технологии электронной подписи при межведомственном электронном взаимодействии. Версия 2.3.3. [Опубликовано 06.08.2011 на Портале методической поддержки реализации 210-ФЗ - доступ авторизованный]. Версия 2.3.3 одобрена Протоколом заседания Подкомиссии по использованию информационных технологий при предоставлении государственных и муниципальных услуг Правительственной комиссии по внедрению информационных технологий в деятельность государственных органов и органов местного самоуправления от 29 июля 2011 г. № 9 // http://210fz.ru/mdx/assets/files/documents/smev_i_rsmeb/Prilogenie_mp_v2_3_3.doc

технологий управления, построения единого информационного пространства органов государственной власти и местного самоуправления, а также оптимизации управления на основе перевода государственных и муниципальных услуг в электронный вид.

Глава 1.
Понятие «Доверие» в электронном государстве

Многочисленные исследования показали, что люди по-разному определяют понятие «доверие». Все зависит от особенностей их личной жизни, бизнеса, отношений с государственными органами. Некоторые считают, что доверие — это прежде всего конфиденциальность, другие — честность и искренность. А есть и те, для которых доверие определяется умением решать их специфические задачи. Таким образом, понятие «доверие» имеет разный смысл для разных людей. В контексте создания электронного правительства, задача государства — обеспечение уровня доверия, необходимого для активного использования гражданами государственных услуг, оказываемых в электронном виде, а следовательно, и обеспечение доверительного и эффективного межведомственного взаимодействия.

Активное развитие государственных электронных услуг в развитых странах мира остро поставило вопрос о том, насколько такого рода услуги востребованы гражданами, и, следовательно, в полной ли мере реализуется потенциал электронного правительства. Учитывая, что переход на электронные услуги сопряжен с весьма значительными бюджетными затратами, вопрос представляет не только теоретический интерес.

Конечно, само представление о том, какой уровень востребованности следует считать удовлетворительным, в разных странах может варьироваться. Например, когда А. Колсакер и Л. Ли-Келли в 2008 г. обнаружили, что только 22,1% жителей Великобритании когда-либо скачивали информацию с официальных сайтов органов власти, 7,1% загружали образцы документов для заполнения, а 4,8% отправляли заполненные формы в электронном виде[5], данные результаты были оценены как свидетельство запредельно низкого интереса к электронному правительству и даже вызвали сомнения в достоверности опроса. В Австралии ситуация, когда 61% граждан предпочитает обращаться в органы власти не в электронном виде, а лично, по телефону или с использованием традиционной почты, а оставшиеся в основном воспринимают официальные сайты как источник информации, и неохотно пользуются интерактивными услугами, особенно финансового плана[6],

[5] Kolsaker A., Lee-Kelley L. Citizen's Attitude Towards E-Government and E-Governance: A UK Study // International Journal of Public Sector Management. 2008. V. 21 (7). P. 723 – 738.

[6] Gauld D. Do They Want It? Do They Use It? The 'Demand-Side' of E-Government in Australia and New Zealand / Gauld D., Goldfinch Sh., Horsburgh S. // Government Information Quarterly. 2010. V. 27. P. 177 – 186.

также была воспринята как тревожный показатель низкой востребованности электронного правительства.

На российском фоне, когда, по результатам исследования Фонда «Общественное мнение» на начало 2011 г. к электронным государственным услугам прибегало не более 6% населения (которые, к тому же, проявляли тенденцию путать государственные сервисы и электронные торговлю)[7], а по данным московских властей в городе с уровнем проникновения широкополосного Интернета близким к среднеевропейскому (60%) получали государственные услуги в электронном виде не более 3% жителей[8], такие оценки могут показаться излишне суровыми. Однако это не снимает вопроса о том, какие факторы препятствуют (или, наоборот) содействуют процессам освоения гражданами электронного правительства.

Первоначально при поиске ответа на данный вопрос исследователи опирались на теорию распространения инноваций Э. Роджерса[9], в рамках которой освоение любой новой технологии рассматривалось как результат сравнительной оценки пользователем пяти основных факторов: сравнительных преимуществ, которые предполагает использование этой технологии, совместимости ее с предыдущими технологиями того же типа, сложности освоения новых навыков, возможности самостоятельно опробовать новую технологию и степени ее наглядности, а также на более упрощенную модель освоения технологии («technology acceptance model») Ф. Дэвиса[10], которая описывала намерение использовать новую технологию как результат рационального соотнесения ожидаемой пользы от технологии с ожидаемыми сложностями при ее освоении.

Однако обе эти модели фактически исключали из рассмотрения социальный контекст, в рамках которого осуществляется адаптация технических инноваций, поэтому довольно скоро они были дополнены положениями, основанными на теории социального конструирования технологии Д. Маккензи и Дж. Веджкман[11].

[7] В тридевятом царстве, в электронном государстве. // Пресс-релиз «Фонда Общественное Мнение». 13 июля 2011 г. http://bd.fom.ru/report/cat/smi/smi_int/pressr_080711.

[8] Проценко Л. «Чиновник с айпадом»: Станет ли лучше жизнь москвичей в электронном городе? // Российская газета. Столичный выпуск № 5538. 27 июля 2011г. http://www.rg.ru/2011/07/27/infograd.html.

[9] Rogers E. Diffusion of Innovations. 5th ed. N.Y., The Free Press. 2003. 512 p.

[10] Davis F.D. Perceived Usefulness, Perceived Ease of Use, and User Accepatance of Information Technology // MIS Quarterly. 1989. V. 13. № 3. P. 319 – 339.

[11] The Social Shaping of Technology / McKenzie D., Wajcman J. (eds.) 1st ed. L., Open Univ. Press. 1985. 462 p.

В результате в рамках исследований электронного правительства Л. Картером и Ф. Беланже[12], была предложена расширенная модель адаптации технологии, в рамках которой основными факторами, содействующими адаптации информационно - коммуникационных технологий, наряду с ожидаемой пользой и ожидаемой легкостью освоения было названо доверие. Впоследствии, анализируя проблему адаптации государственных электронных услуг, Л. Картер и В. Вираккоди уточнили понятие «доверия», разделив его на доверие к информационно-коммуникационным технологиям и доверие к органам власти, которые предлагают воспользоваться своими услугами в электронном виде[13]. В дальнейшем это понятие было еще более конкретизировано М. Хорстом, М. Кутшройтер и Я.М. Гуттелингом. В их работе доверие органам власти было интерпретировано, как, с одной стороны, потребность пользователей доверять умению органов власти управлять новой системой предоставления услуг («information management capacity»), а с другой – как уверенность в технической надежности соответствующей инфраструктуры и тех, кто эту инфраструктуру обслуживает[14].

Эмпирические исследования показали наличие прямой корреляции между уровнем доверия органам власти и готовностью использовать электронные услуги. В уже упоминавшемся исследовании М. Хорста и его соавторов на голландском материале было продемонстрировано, что чем выше уровень доверия способности органов власти предоставлять услуги в электронном виде и чем меньше беспокойства вызывает техническая надежность системы электронных услуг, тем сильнее выражено у респондентов намерение использовать такого рода услуги. Иными словами, доверие органам власти является сильным позитивным стимулом, содействующим адаптации государственных электронных услуг.

Доверие непосредственно «вплетено» в механизм, обеспечивающий интеграцию и стабильность общества. Подчеркивая роль доверия в организации общественной жизни, известный американский социолог А. Селигмен отмечает, что власть, господство и насилие на какое-то время могут решить проблему социального порядка, организации разделения труда, но «они не способны сами по себе обеспечить основу для поддержания этого порядка в долговременной перспективе»[15].

[12] Carter L., Belanger F. The Utilization of E-Government Services: Citizen Trust, Innovation and Acceptance Factor // Information System Journal. 2005. P. 5 – 25.

[13] Carter L., Weerakkody V. E-government Adoption: A Cultural Comparison // Information Systems Frontiers. 2008. V. 10. P. 473-482.

[14] Horst M., Kuttschreuter M., Gutteling J.M. Perceived Usefulness, Personal Experience, Risk Perception and Trust as Determinants of Adoption of E-Government Services in The Netherlands // Computers in Human Behavior. 2007. V. 23. P. 1838 – 1852.

[15] *Селигмен А.* Проблема доверия / Перевод с англ. - М: Идея-Пресс, 2002.

К проблеме доверия в разное время обращались такие мыслители прошлого, как Г. Гроции, Дж. Локк, И. Кант и Э. Дюркгейм. Доверие рассматривалось ими в контексте анализа «договорного» начала общественных отношений. Тема доверия проходит через социологические теории, рассматривающие общественные связи как социальный обмен (П.Блау, Дж.Хоманс). В той или иной форме к этой проблеме обращался Т. Парсонс. Так, по мнению этого американского социолога, социетальная самодостаточность (сохранение обществом себя как системы) должна быть обеспечена стабильным характером отношений взаимообмена как с физической средой и другими системами, так и особыми устойчивыми отношениями личности и общества. «Общество может быть самодостаточным только в той мере, в какой оно может полагаться на то, что деяния его членов будут служить адекватным вкладом в его социетальное функционирование», — пишет он в книге «Система современных обществ»[16]. Общество полагается, другими словами, ожидает (ожидание включает в себя момент неопределенности, отсутствие полной уверенности), что его члены будут добросовестно выполнять свои роли, следовать нормативно определенным обязательствам, таким образом, реализуя себя в качестве членов этого общества. Если трактовать доверие как ожидание взаимности в осуществлении каких-либо действий, то в концепции Т. Парсонса доверие — одно из условий, обеспечивающих общественную стабильность. Проблема доверия рассматривается им в рамках концепции взаимообменов ресурсами между подсистемами общества. В частности, во взаимообменах с подсистемой интеграции политика обменивает обязательства эффективной реализации коллективных целей на доверие социума. Доверие избирателей выступает как своеобразное кредитование политики.

Значимость фактора доверия в поддержании социального порядка становится очевидной, если рассматривать социальные взаимодействия как обмен услугами, ценностями (ресурсами). Выполнение взаимных обязательств может закрепляться договорами и гарантироваться санкциями. Но далеко не все взаимоотношения принимают оформленные «договорные» формы (последние распространены, прежде всего, в сферах экономики и политики). Как указывают социологи, большая часть обменов в рамках семейных, партнерских, соседских, товарищеских и других отношений построена на механизмах доверия к партнеру, честности, дружбы и взаимоответственности. Кроме того, как совершенно справедливо отмечает А. Г. Эфендиев, какими бы жесткими не были договорные формы обмена, они также базируются на таких нежестких материях, как ожидание и доверие. «Основная масса обменов между

[16] *Парсонс Т.* Система современных обществ /Перевод, с англ. - М.: Аспект Пресс, 1998.

людьми в обществе, — продолжает он, — осуществляется *в кредит, на основе риска*, ожидания взаимности и доверия»[17].

Доверие все же не тождественно уверенности и выступает как полагание, ожидание полезности действий и ситуаций, в которые включен индивид. Для большинства авторов, исследующих эту проблему, доверие выступает своеобразной реакцией индивидов на неопределенность повседневной жизни. «Мы можем определить «безопасность» как такую ситуацию, в которой определенный комплекс опасностей нейтрализован или минимизирован. Опыт безопасности обычно опирается на баланс доверия и приемлемого риска», — пишет британский социолог Э. Гидденс[18]. Сохранение «приемлемого риска» в отношениях доверия объясняется наличием некой неопределенности в том, что ожидания неких действий со стороны других людей или институтов будут реализованы в полной мере.

Э. Гидденс выдел два вида доверия: доверие к людям, которое построено на личностных обязательствах («персонифицированное») и доверие к абстрактным системам («анонимное»), предполагающее безличностные обязательства. Под абстрактными системами понимаются символические знаки (например, деньги как инструмент обмена, средства политической легитимации) и информационные системы — системы технического исполнения, организующие наше материальное и социальное окружение. Последний тип доверия, по мнению социолога, формируется в современную эпоху.

Преодоление «синдрома недоверия» определяется сочетанием многих факторов, важнейшими среди которых являются развитие демократических основ общественной жизни, повышение нравственной и гражданской культуры населения и ответственности самой власти, применение информационных систем, формирующих инфраструктуру доверия.

[17] *Эфендиев А. Г.* Социальные взаимодействия: формы, типы и принципы регуляции // Общая социология: Учебное пособие / Под общ. ред. А. Г. Эфендиева. - М.: ИНФРА-М, 2000.

[18] *Giddens A.* Modernity and self-identity. - Stanford (Col.) Stanford univ. press, 1991.

КОНТРОЛЬНЫЕ ВОПРОСЫ

Тест

Доверие, в контексте электронного правительства является фактором:

а) Экономическим

б) Социальным

в) Техническим

Доверие к ИТ и органам власти было рассмотрено отдельно в работах:

а) Д. Маккензи и Дж. Веджкмана

б) Л. Картера и Ф. Беланже

в) Л. Картера и В. Вираккоди

Доверие это:

а) Уверенность в действиях партнера

б) Уверенность в надежности инфраструктуры

в) Ожидание взаимности в осуществлении каких-либо действий

Глава 2.
Формирование пространства доверия электронного государства

Инфраструктура доверия

Электронное государство - способ осуществления информационных аспектов государственной деятельности, основанный на использовании ИКТ-систем. Электронное государство подразумевает поддержку при помощи ИКТ деятельности как исполнительной власти («электронное правительство»), так и парламентских («электронный парламент») и судебных органов («электронное правосудие»).

Очевидно, что невозможно избежать проблем безопасности в столь сложной и географически распределенной системе электронных коммуникаций, но, в дополнение к технологиям защиты, можно выработать решение, способное уменьшить риск. Это решение также известно как доверие. Доверие в сфере электронных коммуникаций не ограничивается доверием к защищенным компьютерным системам - ведь безопасность компьютерной системы зависит не только от надежной операционной системы, но и от физических средств защиты, от квалификации и надежности персонала и многого другого. Доверие между партнерами напрямую зависит от специфики сферы реализации их деловых отношений.

Для обеспечения доверия необходимо создать институты, обеспечивающие внедрение ИКТ в административное управление и формирующие инфраструктуру электронного правительства, которая необходима для подтверждения проведения должных процедур уполномоченными на это участниками административных процессов.

К инфраструктурным институтам электронного правительства обычно относят:

- инфраструктура обеспечения доверия для цифровых подписей (подтверждение идентичности уполномоченных лиц);
- инфраструктура электронного нотариата (подтверждение времени совершения информационных операций);
- инфраструктура внешнего архивирования (обеспечение сохранения данных);
- инфраструктура раскрытия информации (обеспечение публичного доступа к данным);
- инфраструктура электронного каталога (регистрация государственных информационных систем и приложений (услуг));
- инфраструктура обеспечения юридической значимости информации, представленной в электронном виде.

Создание всех этих инфраструктурных элементов позволяет, в первую очередь, обеспечить предсказуемость, то есть способность государства, как поставщика услуг, постоянно производить ожидаемый (позитивный) результат и позволяет получателю услуг не поддерживать все время высокий уровень бдительности. Чем более предсказуем уровень безопасности и качества услуг, тем легче гражданам их получать.

Политики доверия

Один из простейших, но не всегда самых эффективных методов установления доверия в сфере электронных транзакций заключается в использовании прозрачных *политик* доверия.

Политики доверия должны обеспечивать:

- конфиденциальность;
- корректное использование информации;
- реагирование в случае нарушения доверия;
- внутренние механизмы гарантирования непрерывности доверия;
- согласие пользователей.

Политики *конфиденциальности* разрабатываются для того, чтобы граждане правильно понимали, как орган власти будет обращаться с той персональной и деловой информацией, которую они ему предоставляют. Опубликованная на веб-сайте органа власти политика конфиденциальности объясняет правила использования персональных данных и способствует установлению контакта с гражданами. Граждане должны ознакомиться с этой политикой и подтвердить свое согласие с указанными правилами.

Другой аспект политик доверия - *корректное использование информации*. Это касается ситуаций, когда персональная информация может использоваться не в интересах человека, а, например, для оценки его финансовых возможностей (доходов, суммы медицинской страховки). В настоящее время некоторые компании практикуют отбор и классификацию потребителей определенных товаров и услуг, а затем продают эту информацию другим компаниям. Подобная практика приводит к тому, что люди начинают получать по почте нежелательные сообщения рекламного характера, спам, их вынуждают отвечать на телефонные звонки, пытаются привлечь в качестве потенциальных клиентов кредитных карточных систем и т.п.

Политика доверия должна предлагать некоторые гарантии, то есть страховать пользователя, на тот случай, когда невозможно обеспечить полную защиту его информационных ресурсов. Достаточно часто в политиках содержится утверждение о том, что споры о нарушении конфиденциальности рассматриваются в арбитражном суде. Следует учитывать, что арбитражное разбирательство имеет гораздо менее серьезные последствия для стороны, нарушившей политику доверия, чем

судебное. Очевидно, что в штате государственных организаций, заинтересованных в поддержке отношений доверия, должен присутствовать администратор информационной безопасности или ответственный за конфиденциальность персональных данных. К сожалению, на практике чаще всего единственным выходом для граждан при нарушении конфиденциальности является прекращение использования услуг данного web-сайта и государственного органа.

Политика доверия должна раскрывать внутренние механизмы доверия и демонстрировать, что доверие базируется не просто на обещаниях, а является важной составной частью оказания государственных услуг. Примерами внутренних механизмов доверия могут служить строгий контроль над уровнем подготовки и соблюдением служащими политики конфиденциальности, защищенность компьютерных систем и оборудования, а также аудит административных процессов.

Наконец, политика доверия должна предусматривать механизм получения согласия пользователей. Он обычно называется участием. Многие организации либо не дают возможности пользователям выражать согласие на участие, либо не обладают системами, позволяющими отслеживать и исполнять предпочтения пользователей. Часто организации автоматически предполагают согласие пользователя на участие, тем самым перекладывая на него ответственность за возможные последствия нарушения конфиденциальности.

Ассоциации доверия

В повседневной жизни люди часто допускают транзитивные отношения доверия. Например, если наш друг дает хорошую рекомендацию человеку, которого мы не знаем, то мы обычно склонны относится к этому незнакомцу с большим доверием, чем если бы познакомились с ним сами. В этом случае, поскольку мы доверяем своему другу, то полагаемся на правильность его мнения.

Точно так же в сфере электронных коммуникаций и Интернета появился ряд ассоциаций доверия, которые осуществляют контроль соблюдения политики конфиденциальности, оценку безопасности и надежности программного и аппаратного обеспечения, занимаются аудитом систем и сертификацией специалистов и продуктов в сфере информационных технологий. Некоторые примеры таких ассоциаций приведены в Таблице 1.

Так, например, известные ассоциации доверия Better Business Bureau и TrustE знакомят другие компании с законами в области обеспечения конфиденциальности и помогают им разрабатывать собственные политики и правила. Если компания выполняет все рекомендации ассоциации доверия, то получает ее «печать одобрения» (некоторый символ или логотип ассоциации) для размещения на своем web-сайте.

Таблица 1. Примеры ассоциаций доверия

Общепринятое название	**Тип**	**Формальное название**	**Описание**
BBB	Web-сайт	Better Business Bureau	Выдача компаниям свидетельств о соблюдении ими правил конфиденциальности
CCSA	Кадры	Certification in Control Self-Assessments	Сертификация специалистов по аудиту информационных систем
CISA	Кадры	Certified Information Systems Auditor	Сертификация специалистов по аудиту информационных систем
CISSP	Кадры	Certified Information Systems Security Professional	Сертификация специалистов по безопасности информационных систем
Common Criteria	Системы	Common Criteria	Оценка и сертификация безопасности и надежности ИТ-продуктов
CPP	Кадры	Certified Protection Professional	Сертификация специалистов в сфере безопасности
GIAC	Кадры	Global Information Assurance Certification	Сертификация специалистов
Good Housekeeping	Web-сайт	Good Housekeeping Web Certification	Контроль соблюдения конфиденциальности и сертификация
SAS70	Системы	Statement on Auditing Standards ¹ 70	Аудит систем
Trust E	Web-сайт	Trust E	Контроль соблюдения конфиденциальности, выдача компаниям свидетельств

По существу эта печать идентифицирует доверие, связанное с рекомендациями авторитетных ассоциаций, и подтверждает обязательства организаций в отношении предоставленных гражданами и организациями сведений. Когда пользователь сталкивается с неизвестной электронной услугой и видит «печать одобрения» авторитетной ассоциации, то относится с большим доверием к компании-владельцу сайта. Ассоциации доверия берут на себя функции контроля над соблюдением политики конфиденциальности. Если проверка выявляет нарушение, то ассоциация уведомляет об этом компанию и рекомендует ей пересмотреть принятые правила - с тем чтобы либо правила отражали изменения в ее коммерческой деятельности, либо компания отказалась от подобной практики.

Инфраструктура безопасности

Важным фундаментом доверия в сфере электронных коммуникаций является поддержка инфраструктуры безопасности. Инфраструктура может рассматриваться как базис некоторой масштабной среды. Всем известны такие инфраструктуры, как компьютерные сети, позволяющие выполнять обмен данными между различными компьютерами, и электросети, обеспечивающие работу разнообразного электро-оборудования. Несмотря на различия, их объединяет один и тот же принцип: инфраструктура существует для того, чтобы совершенно разные субъекты могли подключиться к ней и использовать ее в своих целях.

Инфраструктура, отвечающая целям безопасности, должна строиться на тех же принципах и предоставлять те же преимущества. Инфраструктура безопасности обеспечивает защищенность целой организации и должна быть доступна для всех приложений и объектов организации, которым необходима безопасность. «Точки входа» в инфраструктуру безопасности должны быть удобны и унифицированы, как электрические розетки в стене, - ничто не должно мешать объектам, желающим использовать инфраструктуру.

Инфраструктура безопасности, по сути, является рациональной архитектурой для многих сред. Понятие инфраструктуры безопасности - достаточно широкое, включающее в себя многие аспекты, в том числе совместимость имен, политики авторизации, мониторинг, аудит, управление ресурсами, контроль доступа и т.п.

Большинство технических специалистов связывают доверие в сфере электронных коммуникаций с надежной инфраструктурой, к которой относятся системы, приложения и процессы, обеспечивающие надежную, защищенную обработку транзакций. Важными компонентами этой инфраструктуры являются межсетевые экраны, маршрутизаторы, сканеры вирусов, средства оценки уязвимости и защищенные серверы. Большая доля ИТ-затрат приходится на них, поскольку они образуют наиболее осязаемую материальную базу защиты доверия.

Уровни инфраструктуры

Обычно выделяют три уровня инфраструктуры безопасности (Рис. 1). Простейший уровень, находящийся внизу, - это физический уровень. Принимая во внимание ограниченное число рисков, связанных с физическими атаками, этот уровень защищать проще, чем другие. Чтобы гарантировать трудность физического доступа к центру хранения и обработки данных или аналогичным ресурсам, используют одновременно средства сигнализации, охрану и замки. Интересно отметить, что бывает проще физически разрушить хорошо защищенный сайт, чем взломать его. Следовательно, организации важно иметь хорошо проработанный план

восстановления после аварии, включая организацию центров "горячего" и «теплого» резервирования данных.

Физический уровень

Хотя физический доступ и не рассматривается как реальная угроза сегодняшнего дня, очевидно, что нарушение физической безопасности может привести к нарушению информационной безопасности. Для обеспечения высокой степени доверия к защите физического уровня необходимы следующие меры:

- Ограниченный доступ с использованием нескольких механизмов аутентификации (например, применение биометрического устройства и считывателя карт).
- Постоянный мониторинг безопасности с использованием видео- и аудиоаппаратуры, сенсорный мониторинг внешней и внутренней среды.
- Обученный персонал, отвечающий за безопасность.
- Журналы, регистрирующие доступ по ID-картам, проверку документов службой охраны и т.п.

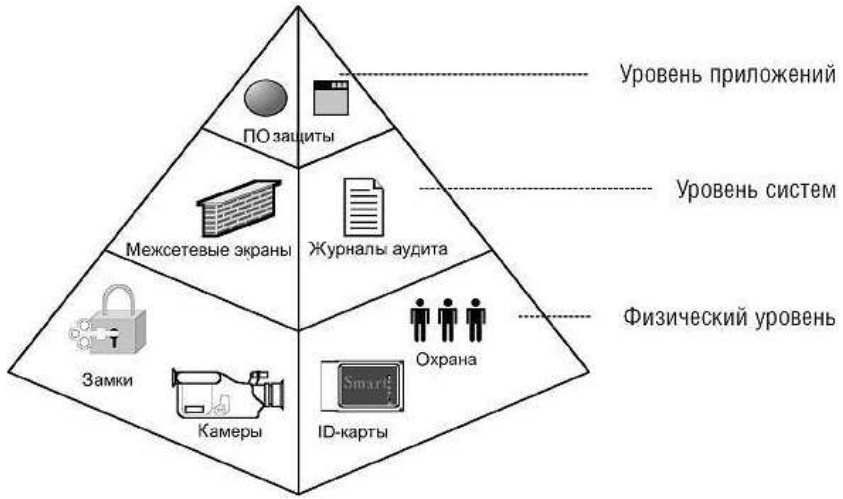

Рис. 1. **Уровни инфраструктуры безопасности**

Системный уровень

Следующий уровень, системный, включает совокупность взаимодействующих друг с другом систем. Поддержку доверия на этом

уровне реализовать сложнее, потому что может быть обеспечена безопасность систем в комплексе, а может быть защищена отдельно каждая система.

На системном уровне должна быть обеспечена безопасность двух ключевых компонентов - операционной системы (ОС) и сети. Бреши в ОС являются базисом многих атак на инфраструктуру. Уязвимость ОС связана с их постоянным обновлением: системные администраторы иногда забывают устанавливать «заплаты» (файлы с исправлениями), чтобы своевременно защищать уязвимые места. Кроме того, модификация разработчиком ОС функций безопасности способна иногда влиять на базовую функциональность, вынуждая системных администраторов откладывать обновление системы.

Сетевые компоненты еще более уязвимы, чем ОС. Современная сеть подвергается и внутренним, и внешним атакам, для защиты от них требуется сложный набор технологий. Многие исследования показали, что организации часто бывают более уязвимы для внутренних атак, чем для прямых атак из Интернета. Защита сети изнутри немного более сложна и требует строгого контроля доступа, использования межсетевых экранов, контрольных журналов и т.д. Строгий контроль доступа позволяет повысить степень *доверия* пользователей при доступе к частной сети. В настоящее время угрозу представляет использование карманных персональных компьютеров (Personal Digital Assistants). Эти устройства могут подсоединяться непосредственно к узлу сети и обходить защиту межсетевых экранов, маршрутизаторов и антивирусных средств. Таким образом, вирус или другой злонамеренный код может быть занесен непосредственно в сеть. Для фиксации подозрительной активности и событий после инцидента необходимы контрольные журналы. Важно, чтобы файлы регистрации хранились отдельно, вне функционирующих систем, причем таким способом, который делает их неизменяемыми (во избежание мошенничества системных администраторов).

Уровень приложений

Уровень приложений, вероятно, наиболее сложен для защиты и обеспечения доверия, так как частота использования программных утилит здесь намного выше, чем на любом другом уровне, и, следовательно, потенциально выше риск безопасности. Компрометация уровня приложений чаще всего связана с нехваткой ресурсов памяти и невозможностью управлять данными пользователей, а также с избыточностью функций приложений. Ограниченность ресурсов памяти приводит к переполнению буфера или непреднамеренному принятию фальсифицированных данных, что обычно происходит в результате неадекватной фильтрации пользовательских данных при вводе или

попытке получить доступ к большему объему памяти, чем имеется фактически. Для защиты уровня приложений используются:

- программные средства (например, сканирование или блокирование вирусов);
- программное обеспечение превентивного действия (обнаружение уязвимостей или тестирование);
- просмотр кодов приложений вручную с целью выявления возможных проблем безопасности.

Уровень приложений является наиболее сложным для защиты еще и потому, что наиболее доступен. Например, любой, кто может получить доступ к web-сайту организации, оказывающей электронные услуги, немедленно получает доступ к приложению (Active X), которое позволяет выполнить транзакцию. Получить доступ на физическом или системном уровне труднее. Важно понимать, что компрометация одного уровня ведет к компрометации другого. Часто системный уровень атакуется, а затем используется для доступа к данным приложения. Например, злоумышленник может атаковать ОС и использовать бреши в ней для атаки на размещаемые в уровне приложений данные граждан с целью получения конфиденциальной информации.

Цель и сервисы инфраструктуры безопасности

Главная цель инфраструктуры безопасности состоит в обеспечении безопасной работы приложений. Если проводить аналогию с функционированием инфраструктуры электросетей, то можно сказать, что электросеть обеспечивает правильную работу таких «приложений», как электроприборы. Более того, универсальность инфраструктуры электросетей такова, что она способна поддерживать «приложения», которые были неизвестны в то время, когда она проектировалась (к ним относится практически вся современная бытовая техника, компьютеры и многое другое). Под приложением в контексте инфраструктуры безопасности понимается любой модуль, использующий инфраструктуру в целях безопасности, такой как web-браузер, клиентское приложение электронной почты, устройство, поддерживающее протокол IPsec, и т.п.

Инфраструктура безопасности дает возможность приложениям защищать их собственные данные или ресурсы и придавать безопасность их взаимодействию с другими данными или ресурсами. Доступ к инфраструктуре должен быть простым и быстрым - подобно включению электроприбора в розетку. Инфраструктура безопасности должна обладать знакомым и удобным интерфейсом, пригодностью и предсказуемостью сервисов. Кроме того, устройствам, использующим инфраструктуру, нет необходимости знать, каким образом достигается результат. Так, например, для работы любого электроприбора не имеет значения, каким образом происходит передача электроэнергии, а важно лишь то, что при

его включении в электрическую розетку предсказуемый «сервис» обеспечивает прибор электроэнергией, необходимой для его правильной работы. То есть инфраструктура безопасности должна иметь хорошо известные точки входа, которые могут доставить сервис безопасности нуждающемуся в нем устройству. Причем для устройства неважно, как это делается, но существенно, что это делается удобно и корректно.

Рассмотрим наиболее важные аспекты сервисов, предоставляемых инфраструктурой безопасности.

Защищенная регистрация

Концепция регистрации пользователя для доступа к приложению широко известна. Обычно этот процесс заключается в том, что пользователь вводит информацию, которая его идентифицирует (имя или ID пользователя) и аутентифицирует (пароль или другая секретная информация). Процесс регистрации предполагает, что никто, кроме законного пользователя, не знает аутентифицирующую его информацию, и обеспечивает защищенный доступ пользователя к определенному приложению.

Проблемы безопасности, возникающие при регистрации, также хорошо известны. Если приложение, требующее регистрации, удалено от пользователя (находится, например, на другом компьютере), то пароли, передаваемые по незащищенной сети, становятся объектом перехвата. Даже зашифрованные пароли не защищены от атак воспроизведения (replay attacks), когда они могут быть скопированы и использованы позднее для имитации аутентичности. Более того, общеизвестно, что пользователи редко выбирают «хорошие» пароли (достаточной длины и непредсказуемости), как правило, не запоминают их без записывания и не меняют своевременно, когда этого требует локальная политика безопасности.

Инфраструктура безопасности может решить некоторые из этих проблем. Поддержка безопасности подразумевает, что событие регистрации для инфраструктуры происходит локально (на устройстве, посредством которого пользователь физически осуществляет взаимодействие) и что корректный результат регистрации, когда необходимо, защищенно распространяется на удаленное приложение.

Таким образом, для удаленной регистрации пользователей могут использоваться механизмы аутентификации, при которых отпадает необходимость в передаче паролей по сети. Развертывание инфраструктуры безопасности полностью не исключает применение паролей, но решает серьезную проблему передачи паролей по ненадежным и незащищенным сетям.

Защищенная однократная регистрация

Проблемы безопасности при регистрации многократно возрастают, когда пользователю необходим доступ ко многим приложениям. Практика показывает, что если пользователю нужно множество паролей, он просто принимает решение сделать все свои пароли одинаковыми. Это ведет к эффекту «самого слабого звена»: при взломе слабейшей из систем (например, при помощи программы-сниффера) злоумышленник получает доступ ко всем системам одновременно. Применение одного и того же пароля для доступа ко всем приложениям снижает общую безопасность, а запоминание множества паролей и трата времени на доступ ко многим системам существенно затрудняют работу пользователя и вынуждают его искать пути обхода этих процедур, что также небезопасно.

Преимущества системы однократной регистрации заметны пользователям с первого взгляда: отпадает необходимость запоминать множество паролей и тратить время на аутентификацию при входе в каждую конкретную систему. Однократная регистрация не просто удобна для пользователей, но также снижает нагрузку на централизованную службу поддержки информации о регистрации и обслуживания паролей (плановая или внеплановая смена паролей, работа с забытыми паролями и пр.), которая уязвима к атакам.

Комплексная безопасность

Наиболее важное достоинство всеобъемлющей инфраструктуры безопасности заключается в том, что она гарантирует сквозную доступность в среде единой, надежной технологии безопасности. В результате в комплексе может работать неограниченное количество приложений, устройств и серверов для защиты процессов передачи, хранения и поиска данных, обработки транзакций, доступа к серверам.

Приложения электронной почты, web-браузеры, межсетевые экраны, устройства удаленного доступа, серверы приложений, файл-серверы, базы данных и т.п. - все они способны понимать и использовать инфраструктуру унифицированным способом. Такая среда существенно упрощает как взаимодействие пользователей с различными устройствами и приложениями, так и сложное администрирование устройств и приложений, гарантируя, что они функционируют в соответствии с требованиями заданного уровня безопасности.

Всеобъемлющая инфраструктура безопасности предоставляет организации ряд существенных преимуществ:

- экономию затрат;
- функциональную совместимость внутри организации и между организациями;
- стандартность решения;
- реальное обеспечение безопасности;

– возможность выбора поставщика технологии.

Реализация единого решения по безопасности для большой организации экономически более эффективна, чем реализация нескольких решений по отдельным проблемам безопасности, поскольку масштабирование среды требует меньших дополнительных капиталовложений. При поддержке нескольких решений подключение к работе дополнительных пользователей или приложений бывает сложной, а иногда и невыполнимой задачей, интеграция нового решения в существующий комплекс также требует значительных усилий и затрат. Стоимость развертывания, поддержки и функционирования набора решений по отдельным проблемам безопасности сопоставима со стоимостью развертывания, поддержки и функционирования единой инфраструктуры.

Использование нескольких разнородных решений может препятствовать функциональной совместимости внутри организации, поскольку они разрабатывались независимо и часто характеризуются несовместимыми базовыми допущениями и принципами функционирования. Инфраструктура же гарантирует функциональную совместимость, поскольку каждое приложение и устройство получает доступ и использует инфраструктуру идентичным образом. Кроме того, на базе единой технологии развертывания инфраструктуры, основанной на открытых международных стандартах, организации проще поддерживать функциональную совместимость с другими организациями.

Инфраструктура безопасности обеспечивает согласованное и стандартное решение для всех использующих ее приложений и устройств. Организации намного проще поддерживать стандартное решение, чем устанавливать, контролировать и поддерживать несколько решений, не всегда совместимых между собой. Стоимость и сложность администрирования также говорят в пользу инфраструктурного решения.

Инфраструктура безопасности обеспечивает реальную защищенность взаимодействий между различными приложениями и устройствами, поскольку все взаимодействия управляются совместимым способом. Более того, функционирование инфраструктуры и взаимодействия внутри нее могут быть проверены на корректность внешними аудиторами. Безопасность взаимодействия набора решений проверить существенно сложнее, а иногда и просто невозможно, даже если каждое решение в отдельности строго контролируется.

Важным достоинством единого решения является возможность выбора одного поставщика (разработчика) технологии с учетом его репутации и опыта работы, стоимости проекта, функциональности и ряда других факторов. В том случае, когда комплексная безопасность организации базируется на функциях безопасности отдельных приложений или устройств (от разных поставщиков), которые приобретались

организацией исключительно в целях бизнеса, сложно вообще говорить об инфраструктуре безопасности.

Перечисленные возможности составляют далеко не все аргументы в пользу всеобъемлющей инфраструктуры безопасности. Однако стандартность решения, которая обеспечивает функциональную совместимость и значительно сокращает затраты администрирования, и предлагаемые функции безопасности являются главными преимуществами комплексного решения (в масштабе полной инфраструктуры) во многих средах. Обладающая всеми этими качествами инфраструктура безопасности способна быть фундаментом доверия взаимодействующих сторон в сфере электронных коммуникаций.

Инфраструктура обеспечения юридической значимости информации, представленной в электронном виде

Для организации электронных взаимодействий между органами власти и гражданами и организациями в процессе предоставления государственных и муниципальных услуг требуется создание общественных институтов, эквивалентных используемым в традиционном очно-бумажном взаимодействии. При этом электронные учетные системы являются аналогом систем бумажного учета. Инфраструктура обеспечения юридической значимости информации, представленной в электронном виде, соответствует традиционным институтам обеспечения доверия к документам на бумажном носителе, к которым относятся собственноручная подпись, печати и штампы, официальные бланки, бланки строгой отчетности, гербовая бумага, публикации в официальных изданиях и др.

Правовые условия признания электронного документа юридически значимым

Несмотря на функциональную тождественность бумажных и электронных документов, между ними существуют принципиальные различия в способах обеспечения их аутентичности, адресности и неотказуемости, обусловленные техническими и культурными причинами.

Участники взаимодействия, а также иные заинтересованные лица должны быть уверены, что документы, направляемые органам публичной власти и получаемые от них, доставлены адресату вовремя и без искажений, а также в том, что существует способ фиксации и представления письменных и иных доказательств факта и содержания взаимодействия.

Качество юридической значимости в рамках очно-бумажного документооборота реализуется через систему реквизитов (неотъемлемых составляющих документа), обеспечивающих фиксацию и сохранность юридических фактов, сведения о которых зафиксированы в документах, а

также возможности их использования в качестве доказательств. Состав реквизитов документов без конкретизации сферы их применения зафиксирован в России в ГОСТ Р 6.30-2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов», в котором описано 30 реквизитов. Применительно к сфере государственного управления установлен перечень из 24 реквизитов, которые зафиксированы в Правилах делопроизводства в федеральных органах исполнительной власти, утвержденных постановлением Правительства Российской Федерации от 15 июня 2009 г. № 477.

Признание документа в качестве юридически значимого, независимо от того, какими техническими, правовыми и организационными средствами это сделано, обеспечивается следующими факторами:

Подтверждение волеизъявления субъекта правоотношений. Как правило, подтверждение волеизъявления реализуется собственноручной подписью или цифровой подписью (далее – ЦП) как ее аналогом. Технология ЦП, обеспечивая надежную идентификацию отправителя сообщения и неотказуемость авторства, решает также задачи надежной защиты содержания сообщения (документа) от третьих лиц и надежного контроля целостности содержимого сообщения (документа).

Фиксация и проверка полномочий должностных лиц. Должностные лица не могут исполнять свои обязанности неограниченное время, состав их полномочий может изменяться. Для исключения ситуаций, когда неполномочные должностные лица скрепляют своей подписью документы, необходимо ведение электронных реестров уполномоченных лиц, которым выдан сертификат ключа цифровой подписи, а также своевременный отзыв сертификатов. Такая норма в отношении уполномоченных лиц федеральных органов исполнительной власти установлена в Федеральном законе от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» (далее – Федеральный закон об электронной цифровой подписи).

Фиксация правового статуса органов власти. Состав и сферы деятельности (полномочия, функции) федеральных и региональных органов власти, органов местного самоуправления претерпевают изменения. В бумажных документах реквизит правового статуса реализуется, например, в форме углового штампа с гербом Российской Федерации, указанием контактных данных, проставлением штампа или гербовой печати ведомства. В электронной форме адекватной реализацией подобного правового содержания является ведение электронных реестров органов государственного и муниципального управления, что должно быть функцией соответствующих уполномоченных органов.

Подтверждение места и времени издания документа. Эти реквизиты являются обязательными атрибутами качества юридической значимости не всех документов, однако многие категории документов могут быть

признаны ничтожными в случае отсутствия таких реквизитов. Особая проблема удостоверения места возникает в случае, если стороны договора находятся в разных юрисдикциях (например, в свободной экономической зоне или в разных странах). Для подтверждения места и времени издания документа в электронном виде необходимо использование доверенной третьей стороны для формирования меток доверенного времени, прилагаемых к электронным документам, и для привязки электронного документа к определенной территории или юрисдикции.

Для обеспечения всех атрибутов юридической значимости зафиксированного в установленном порядке юридического факта (электронного документа или записи в электронной базе данных) в целях взаимодействия неопределенного круга лиц, необходимы следующие взаимодополняющие общественные институты, часть которых относится к ведомственному, часть к инфраструктурному уровню, а часть реализуется с помощью общественных институтов:

1. Общенациональная инфраструктура удостоверения открытых ключей цифровой подписи (инфраструктура цифрового доверия), обеспечивающая идентификацию субъектов информационного взаимодействия и целостность содержания электронного документа. Инфраструктура цифрового доверия включает в себя удостоверяющие центры, входящие в единый домен цифрового доверия, и обеспечивает единое пространство использования цифровой подписи. Инфраструктура цифрового доверия обеспечивает наивысшую степень защищенности электронных форм взаимодействия и при определенных условиях (использование доверенных защищенных устройств) подходит для всех случаев волеизъявления, однако имеет ограниченное применение вследствие сложности и низкой доступности. Описана в подразделе «Инфраструктура цифрового доверия».

2. Иные инструменты удаленной идентификации участников электронного взаимодействия, применимые для ограниченного набора волеизъявлений ввиду меньшей степени защищенности в сравнении с инфраструктурой удостоверения открытых ключей цифровой подписи. описаны в подразделе «Идентификация при удаленном взаимодействии».

3. Инфраструктура доверенной третьей стороны (электронный нотариат), предназначенная для удостоверения доверенного времени, а также иных существенных для юридической значимости документа фактов (места издания документа, сделки, контракта, договора, соглашения), а также апостильного и нотариального заверения. Инфраструктура доверенной третьей стороны, как правило, реализовывается на основе инфраструктуры цифрового доверия.

4. Электронные учетные системы участников информационного взаимодействия (органов и организаций, уполномоченных лиц органов и организаций, физических и юридических лиц), обеспечивающие

подтверждение их правового статуса, правомочий, полномочий, права подписи и др., в электронном правительстве реализуются, как правило, на ведомственном уровне, что соответствует современной практике учета правовых статусов.

КОНТРОЛЬНЫЕ ВОПРОСЫ

Тест

К инфраструктурным институтам электронного правительства обычно НЕ относят:

а) Инфраструктура обеспечения доверия для цифровых подписей

б) Инфраструктура обеспечения доверия к органам власти

в) Инфраструктура обеспечения юридической значимости информации, представленной в электронном виде

Политики доверия должны обеспечивать:

а) Конфиденциальность

б) Компетентность пользователей

в) Эффективное использование информации

Инфраструктура, отвечающая целям безопасности не обязана:

а) Быть доступной для всех приложений

б) Иметь унифицированные «точки входа»

в) Обеспечивать защищенность одного объекта

Программное обеспечение превентивного действия используется для защиты инфраструктуры

а) Физического уровня

б) Системного уровня

в) Уровня приложений

Технология ЭЦП НЕ обеспечивает

а) Надежную идентификацию отправителя сообщения

б) Истинность содержания сообщения

в) Неотказуемость авторства сообщения

Глава 3.
Электронная цифровая подпись

Сегодня трудно представить работу любой организации, особенно органа государственной власти или местного самоуправления, без компьютерных сетей и баз данных, следовательно, вопросы информационной безопасности и в частности, кто и на каком основании получает доступ к ее получению, обработке и распространению приобретают всё большее значение.

Особенности идентификации и использования подписи в цифровом мире и пространстве доверия

Корнем решения вопросов управления правами доступа к информационным системам являются понятия идентификации и аутентификации.

Идентификация (*лат. identifico – отождествлять*) — это процесс сообщения субъектом своего имени или идентификатора, с целью отличить себя от других субъектов.

Аутентификация (*англ. Authentication*) или подтверждение подлинности – это процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации, в простейшем случае – с помощью имени и пароля.

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. Можно сказать, что идентификация и аутентификация – это первая линия обороны, интересно её сравнение с «проходной» информационного пространства организации. И если идентификация – это получение ответа на вопросы «кто вы?» и «что вы?», то аутентификация служит доказательством того, что вы являетесь именно тем, за кого себя выдаете.

Идентификация позволяет субъекту – пользователю или процессу, действующему от имени определенного пользователя, назвать себя, сообщив свое имя. Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого себя выдает. В качестве синонима слова «аутентификация» иногда используют сочетание «проверка подлинности». Субъект может подтвердить свою подлинность, если предъявит по крайней мере одну из следующих сущностей:

- нечто, что он знает: пароль, личный идентификационный номер, криптографический ключ и т.п.;
- нечто, чем он владеет: личную электронную карточку или иное устройство аналогичного назначения;

- нечто, что является частью его самого: голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики (Рис. 2);
- нечто, ассоциированное с ним, например, номер и дата выдачи паспорта, домашний адрес или телефонный номер.

Рис. 2. **Пример устройства с биометрической аутентификацией (по отпечатку пальца)**

Идентификация и аутентификация являются взаимосвязанными составляющими проверки подлинности пользователей. На практике идентификация и аутентификация часто логически объединяются в рамках единого процесса (пример - схема «логин-пароль»), а понятие идентификация используется для обозначения обеих процедур.

На основании идентификации и аутентификации производится авторизация участников – определение их полномочий по доступу к сервисам или данным электронного правительства. Авторизация производится, исходя из требований нормативных правовых актов, определяющих эксплуатацию конкретной информационной системы государственного учета и полномочия (правомочия) участников взаимодействия.

Авторизация – это режим, который ассоциирован с каждым пользователем, в котором прописаны права доступа (и модификации) пользователя к тем или иным информационным ресурсам системы. Процесс передачи электронных данных между информационными системами также может быть зашифрован для того, чтобы ограничить доступ какой-либо третьей стороны. На сегодня уже разработаны и внедрены сложные механизмы шифрования данных.

Необходимость решения задачи правового регулирования вопросов идентификации и аутентификации участников электронного взаимодействия обозначена в Концепции формирования в Российской Федерации электронного правительства до 2010 года, одобренной распоряжением Правительства Российской Федерации от 6 мая 2008 г. № 632-р.

В Концепции формирования в Российской Федерации электронного правительства до 2010 года отмечалось, что информационное взаимодействие государственных органов между собой, с организациями и гражданами осуществляется с помощью использования современных средств идентификации участников информационного взаимодействия и электронной цифровой подписи. В результате такого взаимодействия можно однозначно определить (идентифицировать) участников информационного взаимодействия, правомочность уполномоченных должностных лиц органов государственной власти, осуществляющих информационное взаимодействие, дату и время осуществления информационного взаимодействия, а также гарантировать идентичность информации, отправленной одним участником информационного взаимодействия и полученной другим участником информационного взаимодействия.

Действующее законодательство регламентирует вопросы идентификации и аутентификации участников электронного взаимодействия исключительно в контексте использования электронной цифровой подписи. Вместе с тем в мировой практике используются различные механизмы идентификации и аутентификации участников электронного взаимодействия (система штрих-кодирования, цифровые сертификаты, архитектуры открытых ключей и т.д.). В рамках формирования электронного правительства необходимо легализовать использование всех, в том числе несложных и малозатратных механизмов.

По мнению ряда экспертов, реализацию механизмов идентификации в приложениях электронного правительства необходимо вести на основе следующих базовых принципов:

1. *Адекватность метода идентификации ее целям*

Надежность, сложность и стоимость используемого метода идентификации должна соответствовать цели его применения. Чем меньше значимость взаимодействия с точки зрения правовых последствий, тем более простые способы идентификации следует применять.

Конкретные методы идентификации, применяемые на различных этапах предоставления услуги (получение информации, выражение волеизъявления, отслеживания хода предоставления услуги и др.), должны выбираться на этапе перевода услуги в электронный вид, исходя из содержания этапа и состава передаваемых сведений, и требований законодательства.

2. *Децентрализация процедур идентификации*

Для сокращения рисков и ввиду отсутствия постоянных соединений с функциональными ведомственными и региональными информационными системами создание обязательного для использования органами власти и получателями государственных и муниципальных услуг единого идентификационного шлюза на федеральном уровне нецелесообразно.

Создание такого шлюза возможно после появления государственных и муниципальных услуг, реализованных в электронном виде и носящих межведомственный или межуровневый характер. После появления значительного числа приложений электронного правительства и формирования в стране единого домена цифрового доверия следует рассмотреть вопрос о целесообразности создания единого идентификационного шлюза. Его создание в среднесрочной перспективе не должно исключать возможность идентификации пользователей на иных уровнях (ведомственном, региональном, на уровне функциональных ИС).

3. *Минимальность и подконтрольность предоставляемых пользователем сведений*

Процедура идентификации должна требовать от пользователя минимально возможный состав информации о его личности.

Система идентификации должна обеспечивать пользователю средства контроля над идентификационными данными, которые он предоставляет органам власти при удаленном взаимодействии.

4. *Минимальное раскрытие сведений о пользователе*

Проверка подлинности пользователя должна производиться однократно в пределах единой службы аутентификации. В конкретное приложение допустимо передавать только частный (сеансовый) идентификатор, используемый в данном приложении. Не допускается использование единого идентификатора пользователя, на основе которого можно установить связь между данными, имеющими отношение к пользователю, в различных учетных системах. Установление связи между данными допускается в случае предписания нормативного правового акта или при наличии информированного согласия пользователя.

5. *Диверсификация вариантов идентификации*

Для обеспечения гибкости, масштабируемости и надежности, а также снижения рисков неэффективных инвестиций информационные системы электронного правительства должны предусматривать возможность применения различных способов идентификации, которые не должны быть привязаны к конкретным организационно-технологическим решениям, в том числе к универсальной электронной карте, единому реестру идентификаторов, регистру граждан и иным средствам.

Пользователь должен иметь возможность выбирать наиболее удобный для него идентификатор и способ его предоставления, в том числе в зависимости от используемого устройства доступа или канала связи.

Информационные системы электронного правительства должны предусматривать возможность выполнения единой с правовой точки зрения транзакции (подача заявления, выражение волеизъявления и т.п.) в рамках последовательных сессий, в которых могут использоваться различные механизмы идентификации.

6. *Независимость способов идентификации и иных характеристик предоставления услуги*

Выбранные органом власти способы идентификации пользователей не должны ограничивать их в способах выполнения обязанностей, связанных с предоставлением государственной или муниципальной услуги. Например, использование универсальной электронной карты со встроенными банковскими приложениями для идентификации пользователя не должно ограничивать его право совершения платежей, предусмотренных законодательством, с помощью иных удобных ему способов (платежных систем в сети Интернет, банковских карт, скретч-карт).

7. *Информированность пользователей*

Пользователи должны информироваться о том, какие их идентификационных данных для каких целей будут использованы. Перед регистрацией пользователи должны быть уведомлены о:

- целях, сроке и способах использования идентификационных данных;
- возможности передачи данных третьим лицам;
- порядке использования и порядке корректировке данных;
- технологии предоставления и обработки данных.

Пользователям должны предоставляться ссылки на применимые правовые акты и даваться пояснения, доступные гражданам, не имеющим специального образования.

Постановлением Правительства Российской Федерации от 28 ноября 2011г. № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (ЕСИА) утверждено создание федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (единая система идентификации и аутентификации).

В соответствии с указанным постановлением федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» должна обеспечивать санкционированный доступ участников информационного взаимодействия

в единой системе идентификации и аутентификации к информации, содержащейся в государственных информационных системах, муниципальных информационных системах и иных информационных системах, в следующих целях:

- предоставление государственных и муниципальных услуг, в том числе услуг, предоставляемых государственными и муниципальными учреждениями и другими организациями, в которых размещается государственное задание (заказ) или муниципальное задание (заказ);
- исполнение государственных и муниципальных функций;
- формирование базовых государственных информационных ресурсов, определяемых Правительством Российской Федерации;
- межведомственное электронное взаимодействие;
- иные цели, предусмотренные федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации.

В свою очередь, санкционированный доступ к указанной информации должен предоставляться с использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, то есть при помощи СМЭВ.

В единой системе идентификации и аутентификации санкционированный доступ к информации должен осуществляться посредством использования простых электронных подписей и усиленных квалифицированных электронных подписей следующими участниками информационного взаимодействия:

- должностными лицами федеральных органов исполнительной власти, государственных внебюджетных фондов, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, государственных и муниципальных учреждений, многофункциональных центров, а также иных организаций в случаях, предусмотренных федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации;
- заявителями — физическими и юридическими лицами.

Постановлением Правительства Российской Федерации № 977 определен также состав единой системы идентификации и аутентификации, которая должна включать в себя следующие регистры:

- регистр физических лиц;
- регистр юридических лиц;
- регистр должностных лиц органов и организаций;
- регистр органов и организаций;
- регистр информационных систем.

Таким образом, единая система идентификации и аутентификации является важным звеном в системе электронного взаимодействия, обеспечивая как взаимодействие органов государственной власти и местного самоуправления, так и взаимодействие таких органов и заявителей.

К сожалению, надежная идентификация и аутентификация затруднена по ряду принципиальных причин.

Во-первых, компьютерная система основывается на информации в том виде, в каком она была получена; строго говоря, источник информации остается неизвестным. Например, злоумышленник мог воспроизвести ранее перехваченные данные. Следовательно, необходимо принять меры для безопасного ввода и передачи идентификационной и аутентификационной информации; в сетевой среде это сопряжено с особыми трудностями.

Во-вторых, почти все аутентификационные сущности можно узнать, украсть или подделать.

В-третьих, имеется противоречие между надежностью аутентификации с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это не только хлопотно, но и повышает вероятность подглядывания за вводом.

В-четвертых, чем надежнее средство защиты, тем оно дороже.

Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств идентификации и аутентификации. Обычно компромисс достигается за счет комбинирования двух первых из перечисленных базовых механизмов проверки подлинности.

В настоящее время наиболее распространенным средством аутентификации являются пароли. Система сравнивает введенный и ранее заданный для данного пользователя пароль; в случае совпадения подлинность пользователя считается доказанной. Другое средство, постепенно набирающее популярность, - секретные криптографические ключи пользователей.

Обратим внимание на то, что процесс идентификации и аутентификации может идти не только между пользователем и системой - его целесообразно применять и к равноправным партнерам по общению, а также для проверки подлинности источника данных. Когда аутентификации подвергаются процесс или данные, а не человек, выбор допустимых средств сужается. Компьютерные сущности не могут чем-то обладать, у них нет биометрических характеристик. Единственное, что у

них есть, это информация; значит, проверка подлинности может основываться только на том, что процесс или данные знают. С другой стороны, память и терпение у компьютерных сущностей не в пример лучше человеческих, они в состоянии помнить или извлекать из соответствующих устройств и многократно применять длинные криптографические ключи, поэтому в распределенных средах методы криптографии выходят на первый план; по существу, им нет альтернативы.

Любопытно отметить, что иногда фаза аутентификации отсутствует совсем - партнеру верят на слово, или носит чисто символический характер. Так, при получении письма по электронной почте вторая сторона описывается строкой «От:» и подделать ее не составляет большого труда. Порой в качестве свидетельства подлинности выступает только сетевой адрес или имя компьютера - вещь явно недостаточная для подлинного доверия. Только использование криптографии поможет навести здесь порядок.

Главное достоинство парольной аутентификации - простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности. Надежность паролей основывается на способности помнить их и хранить в тайне. Чтобы пароль был запоминающимся, его зачастую делают простым, однако простой пароль нетрудно угадать, особенно если знать пристрастия данного пользователя. Иногда пароли с самого начала не являются тайной, так как имеют стандартные значения, указанные в документации, и далеко не всегда после установки системы производится их смена. Правда, это можно считать аспектом простоты использования программного продукта.

Следующий после аутентификации шаг - **авторизация** (authorization - санкционирование, разрешение, уполномочивание) пользователя для выполнения определенных задач. Авторизация - это процесс определения набора прав, которыми обладает пользователь - т.е. к каким типам действий, ресурсов и служб он допускается.

В обычной жизни, при деловом и административном взаимодействии, для того, чтобы мы доверяли информации и документам, получаемым нами из внешних источников, необходимо применение инструментов, обеспечивающих:

- гарантии того, что личность автора или источника документа установлена и мы можем быть уверены, что именно он отвечает за достоверность документа;
- гарантии того, что этот человек не сможет отказаться от авторства документа или того, что именно он предоставил нам этот документ;

– гарантии того, что документ, который мы получили именно тот, который нам предоставил отправитель и что он не был изменен в процессе передачи.

При традиционном документообороте мы используем для этих целей собственноручную подпись, которая является одним из важнейших реквизитов документа.

В ряде стран документ становится легитимным лишь при наличии подписи уполномоченного лица, без проставления на нем печати организации. Нечто подобное встречается и в нашей стране. Например, при оформлении счета-фактуры законодатель не требует заверять подписи лиц печатью выдавшей организации или индивидуального предпринимателя.

Развитие современных технологий вносит свои коррективы и в эту сферу отношений. 8 апреля 2011 года в России вступил в силу новый Федеральный Закон «Об электронной подписи» (63-ФЗ от 6 апреля 2011 г.), который позволяет обращаться за услугами органов власти через интернет, используя документы, заверенные электронной подписью. В силу закон вступил с 2011 года, и уже сейчас ряд государственных служб активно принимают документы с такой подписью.

С одной стороны, такие нововведения призваны облегчить процесс подписания документов и расширить возможности применения подписи для удостоверения, например, электронных документов. С другой стороны, очень важно при этом действовать в соответствии с законодательством, дабы избежать ситуаций, когда юридическая сила документа может быть оспорена в силу неправомерного использования того или иного аналога собственноручной подписи.

Согласно Гражданскому кодексу для удостоверения любых сделок требуется личная подпись гражданина. Перечень случаев, когда документ может быть подписан другим лицом, является исчерпывающим: наличие у гражданина физических недостатков, тяжелой болезни или его неграмотность. При этом подпись другого лица удостоверяется нотариусом. Однако Гражданский кодекс оговаривает ситуации, когда подпись документа возможна только лицом, от которого он исходит. Так, закрытое завещание должно быть собственноручно написано, причем подписано именно завещателем. Несоблюдение этих правил влечет недействительность завещания. Его подписание каким-либо другим, даже уполномоченным завещателем лицом, не допускается.

В организации правом подписи документов наделены лишь руководитель и главный бухгалтер. Этот перечень может быть расширен по решению руководителя, которое оформляется в виде соответствующего приказа или доверенности в зависимости от того, состоит ли лицо, наделяемое правом подписи, в штате организации. Поскольку приказ является внутренним документом, то передать право подписи по нему

можно лишь работнику организации. Доверенность же предполагает такую возможность и применительно к лицу, не связанному с организацией трудовыми отношениями. Доверенность от имени юридического лица может быть выдана только руководителем или лицом, уполномоченным на это учредительными документами.

В деятельности любой организации возможна ситуация, когда руководитель (или другое уполномоченное лицо) отсутствует на месте, а подписать документы надо немедленно. В этом случае на помощь может прийти факсимиле. Не исключена и необходимость передачи документа по электронным каналам связи. При этом сканирование не способно обеспечить его безопасность. В этом случае, чтобы сохранить первоначальный смысл и реквизиты документа и исключить вероятность прочтения его третьими лицами, следует воспользоваться электронной цифровой подписью (ЭЦП). Только факсимиле и ЭЦП являются на настоящий момент закрепленными в российском законодательстве аналогами собственноручной подписи.

Факсимильное воспроизведение подписи с помощью средств механического или иного копирования упоминается в Гражданском кодексе. Но, как сказано в письме МНС РФ от 01.04.2004 г. «Об использовании факсимиле подписи», поскольку в действующем законодательстве отсутствует регламентация данного вопроса, то применение факсимиле допускается только при взаимном соглашении сторон, которое может быть выражено либо непосредственно в договоре (оговоркой, что документы, заверенные подобным образом, имеют юридическую силу), либо путем направления соответствующих писем. Но даже тогда применение факсимиле весьма ограничено: согласно тому же письму МНС оно не допускается на доверенностях, платежных и других документах, имеющих финансовые последствия.

Правомерность использования ЭЦП на тех или иных документах на сегодняшний день остается достаточно спорным вопросом. Можно сказать, что законодатель без должного внимания отнесся к решению этого вопроса. Он ограничился лишь принятием закона, содержащего общие положения. В этой ситуации каждый орган вправе самостоятельно решать, разрешать ли использование ЭЦП в документах, касающихся его сферы деятельности, или нет. Отсутствие единой правовой позиции делает использование ЭЦП крайне проблематичным. А это не в последней степени влияет на вхождение российских компаний в мировую экономику в качестве полноправных участников.

Не секрет, что в российском, как, впрочем, и в любом другом законодательстве, доказательством проведения той или иной операции признается наличие соответствующих документов.

И если раньше речь шла исключительно о документах в бумажном виде, то в настоящее время развитие информационных технологий привело

к тому, что электронные документы в своих правах уравниваются с бумажными.

В мае 2007 года Россия подписала Конвенцию ООН об использовании электронных сообщений в международных договорах, став тем самым десятой страной, признающей документы в электронной форме наравне с традиционной бумажной формой.

Ситуация с ЭЦП в Российской Федерации на сегодняшний день обстоит таким образом, что любому пользователю для работы с информационными системами, требующими применения электронно-цифровой подписи, приходится практически для каждой из них заводить отдельную ЭЦП.

Электронная цифровая подпись

Согласно закону, электронной цифровой подписью признается реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

В настоящее время идет постепенная смена регулирования, введенного Федеральным законом от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» (утрачивающего силу с 1 июля 2012 г.) на новое, вводимое Федеральным законом № 63-ФЗ «Об электронной подписи».

В соответствии с новым законом ранее действовавшее понятие «электронная цифровая подпись» заменено понятием «электронная подпись».

Электронная подпись — информация в электронной форме, присоединенная к другой информации в электронной форме (подписываемой информации) или иным образом связанная с такой информацией и использующаяся для определения лица, подписывающего информацию.

Таким образом, использование электронной подписи позволяет идентифицировать лицо, подписывающее какую-либо информацию, с как минимум не меньшей степенью надежности, что и традиционные собственноручная подпись или печать.

Суть ЭЦП можно выразить в нескольких словах: если пересылаемый документ будет каким-либо образом изменен, то проверка подписи будет неудачной и, следовательно, будет сделан вывод о том, что документ

подвергался изменениям и не может быть признан заслуживающим доверия.

Для понимания принципов работы ЭЦП нужно познакомиться с некоторыми основами криптографии.

Криптофункция — функция, позволяющая из текста и ключа сделать шифр, такого типа, что даже имея несколько пар «текст-шифр» невозможно угадать ключ, и такой, что воссоздать текст из шифра можно только с помощью ключа (Рис. 3). «Ключ» более адекватное название и более ёмкое, чем «пароль» - ключ похож на обычный железный ключ - мы можем иметь много открытых и закрытых замков, но открыть данный конкретный замок мы можем только имея данный конкретный (подходящий к этому замку) ключ.

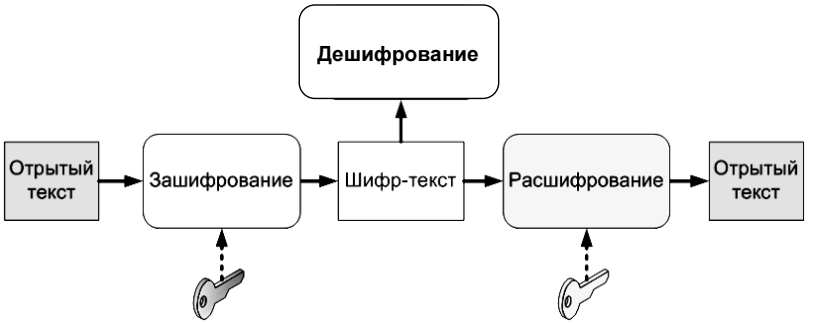

Рис. 3. **Основные операции использования криптографических ключей**

Криптография (использование криптофункций) бывает двух видов: симметричная и несимметричная (или ассиметричная - т.е. с открытыми и закрытыми ключами). В симметричной криптографии ключ, используемый для расшифровки такой же, как для шифровки (Рис. 4).

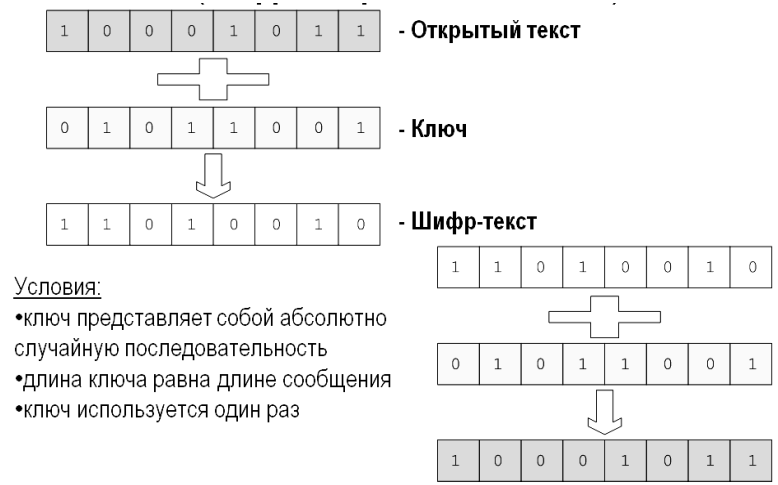

Рис. 4. **Совершенно секретное симметричное шифрование с использованием одноразовых ключей**

Один из основных постулатов криптографии (правило Керкхоффса) гласит, что стойкость алгоритма шифрования основана только на незнании ключа противником. Длинна ключа - основная характеристика, определяющая класс стойкости шифра. Управление ключами, т.е. их генерирование, распространение и т.п. - одна из наиболее сложных задач в практической криптографии.

Этот тип криптографии нас не будет интересовать, поскольку, при необходимости распространения ключа для расшифровки сообщения, пропадает уверенность в том, кто это сообщение зашифровал, ведь для шифрования и расшифрования всеми используется один и тот же ключ.

Технологии реализации электронной цифровой подписи

Как уже было указано во введении, задачи формирования «электронного правительства» предполагают решение вопросов обеспечения легитимности административных процессов в электронной среде и надежной идентификации участников информационного обмена, в том числе граждан. Электронная цифровая подпись (ЭЦП) в инфраструктуре электронного правительства предназначена для обеспечения юридической значимости взаимодействия в электронном виде. ЭЦП является фундаментальной технологией, лежащей в основе межведомственного электронного взаимодействия.

Электронная подпись используется для:

– установления авторства электронного документа;
– проверки целостности (отсутствия искажений) в подписанном документе.

Для этого, используется пара ключей: электронная подпись формируется с использованием сертификата ключа электронной подписи (закрытого ключа), а проверка значений электронной подписи осуществляется с помощью сертификата ключа проверки электронной подписи (открытого ключа).

Методические рекомендации по разработке электронных сервисов и применению технологии электронной подписи[19] рассматривают следующие виды подписи:

Электронная подпись физического лица:

– электронная подпись, формируемая от имени пользователя Единого портала государственных услуг (функций), осуществляющего заказ услуг в электронном виде (далее – пользователя ЕПГУ, ЭП-П);
– электронная подпись, формируемая от имени должностного лица органа власти, участвующего в межведомственном взаимодействии при оказании государственных услуг (далее – служебного пользования, ЭП-СП).

Электронная подпись информационных систем:

– электронная подпись, формируемая от имени органа государственной власти и органа местного самоуправления (далее – органа власти, ЭП-ОВ), участвующего в межведомственном взаимодействии при оказании государственных услуг;
– электронная подпись, формируемая системой межведомственного электронного взаимодействия (далее – СМЭВ) при обработке электронных сообщений, передаваемых через нее (далее – ЭП-СМЭВ);
– электронная подпись, формируемая ЕПГУ при формировании электронных сообщений, передаваемых в информационные системы органов власти (далее – ЭП-ПГУ).

[19] Методические рекомендации по разработке электронных сервисов и применению технологии электронной подписи при межведомственном электронном взаимодействии. Версия 2.3.3. [Опубликовано 06.08.2011 на Портале методической поддержки реализации 210-ФЗ - доступ авторизованный]. Версия 2.3.3 одобрена Протоколом заседания Подкомиссии по использованию информационных технологий при предоставлении государственных и муниципальных услуг Правительственной комиссии по внедрению информационных технологий в деятельность государственных органов и органов местного самоуправления от 29 июля 2011 г. № 9 // http://210fz.ru/mdx/assets/files/documents/smev_i_rsmeb/Prilogenie_mp_v2_3_3.doc

Необходимо отметить, что в указанных методических рекомендациях выделяются различные виды и форматы электронной подписи (см. табл. 1).

Таблица 2. Виды и форматы электронной подписи

№ п.п.	Название электронной подписи	Описание, назначение электронной подписи
1.	**Виды электронной подписи**	
1.1.	Электронная подпись физического лица	▪ электронная подпись, формируемая от имени пользователя Единого портала государственных услуг (ЕПГУ), осуществляющего заказ услуг в электронном виде (ЭП-П) ▪ электронная подпись, формируемая от имени должностного лица органа власти, участвующего в межведомственном взаимодействии при оказании государственных услуг (электронная подпись служебного пользования, ЭП-СП)
1.2.	Электронная подпись информационных систем	▪ электронная подпись, формируемая от имени органа государственной власти и органа местного самоуправления (электронная подпись органа власти, ЭП-ОВ), участвующего в межведомственном взаимодействии при оказании государственных услуг ▪ электронная подпись, формируемая СМЭВ при обработке электронных сообщений, передаваемых через нее (ЭП-СМЭВ) ▪ электронная подпись, формируемая ЕПГУ при формировании электронных сообщений, передаваемых в информационные системы органов власти (ЭП-ПГУ)
2.	**Форматы электронной подписи**	
2.1.	Электронная подпись в заявлениях с ЕПГУ	▪ в электронных сообщениях, формируемых при заказе услуг в электронном виде, используется специальный формат передачи электронных документов - архив документов, содержащий файлы заявления и сопутствующих вложений, а также для каждого из соответствующих файлов подписей в формате PKCS#7 detached
2.2.	Электронная подпись уполномоченного лица органа власти при межведомственном взаимодействии	▪ в электронных сообщениях без вложений для передачи электронной подписи уполномоченного лица органа власти при межведомственном взаимодействии используется формат XML Digital Signature ▪ в электронных сообщениях с вложениями электронная подпись передается для каждого электронного документа в виде отдельного файла в формате PKCS#7 detached в составе архива вложений
2.3.	Электронная подпись информационных систем	▪ информационные системы при формировании подписи в электронных сообщениях используют формат XML Digital Signature в связке со стандартом WS-Security
2.4.	Электронная подпись в XML	▪ формат XML Digital Signature базируется на стандарте языка XML, являющегося основой электронного взаимодействия ИС ▪ подпись в формате XMLDSig не является легко отчуждаемой от инфраструктуры электронного правительства, потому предлагается использовать его только для взаимодействия с использованием XML форматов
2.5.	Электронная подпись для файлов	▪ подпись в формате PKCS#7 является легко отчуждаемой и может быть проверена физическим лицом с помощью ПО, не входящего в инфраструктуру электронного правительства ▪ предлагается его использование для подачи заявлений на услуги с ЕПГУ и межведомственного взаимодействия, предполагающего передачу вложений (текстовых, графических, картографических) в электронных сообщениях.

Примечание: Таблица сформирована в соответствии с Методическими рекомендациями по разработке электронных сервисов и применению технологии электронной подписи при межведомственном электронном взаимодействии, 2011 г.

По видам электронные подписи, в соответствии с Федеральным законом № 63-ФЗ, делятся на:

– простую электронную подпись;
– усиленную электронную подпись.

В свою очередь, усиленная электронная подпись также бывает двух видов:

– неквалифицированная электронная подпись;
– квалифицированная электронная подпись.

В соответствии с Федеральным законом № 63-ФЗ, простая электронная подпись — это электронная подпись, которая посредством

использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Неквалифицированной электронной подписью является электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

Квалифицированная электронная подпись — это электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- ключ проверки электронной подписи указан в квалифицированном сертификате;
- для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

Отличия между разными видами электронных подписей состоят в степени защищенности, а следовательно, и в возможности применения того или иного вида электронной подписи для удостоверения различных видов информации. Сфера действия разных видов электронных подписей также прямо установлена в законе:

Федеральным законом № 63-ФЗ прямо установлено, что информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

В свою очередь, информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных неквалифицированной электронной подписью, равнозначными документам на бумажных носителях, подписанным

собственноручной подписью, должны предусматривать порядок проверки электронной подписи.

При этом если в соответствии с федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или обычаем делового оборота, документ должен быть заверен печатью, электронный документ, подписанный усиленной электронной подписью и признаваемый равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью. Федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия могут быть предусмотрены дополнительные требования к электронному документу в целях признания его равнозначным документу на бумажном носителе, заверенному печатью.

В качестве примера нормативного акта, устанавливающего обязательность использования конкретного вида электронных подписей, можно привести Постановление Правительства Российской Федерации № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи», в котором сказано, что при организации межведомственного взаимодействия, осуществляемого в электронном виде органами исполнительной власти и органами местного самоуправления при предоставлении государственных или муниципальных услуг и исполнении государственных или муниципальных функций, применяется усиленная квалифицированная электронная подпись.

Проверка электронной подписи осуществляется с применением ключа проверки электронной подписи. В свою очередь, сертификат ключа электронной подписи представляет собой электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи. Сертификаты ключей проверки электронных подписей выдаются особыми юридическими лицами — удостоверяющими центрами.

При создании электронной подписи средства электронной подписи должны:

- показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

– создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи;
– однозначно показывать, что электронная подпись создана.

В свою очередь, при проверке электронной подписи средства электронной подписи должны:

– показывать содержание электронного документа, подписанного электронной подписью;
– показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;
– указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

Кроме того следует учитывать, что одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании электронной подписью пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным электронной подписью того вида, которой подписан пакет электронных документов. Соответственно, в таком пакете электронных документов не могут находиться документы, подписанные разными электронными подписями.

Общее регулирование применения электронных подписей осуществляет уполномоченный федеральный орган исполнительной власти, которым, в соответствии с постановлением Правительства Российской Федерации № 976 «О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи, является Минкомсвязи России.

Уполномоченный федеральный орган:

– осуществляет аккредитацию удостоверяющих центров, проводит проверки соблюдения аккредитованными удостоверяющими центрами требований, которые установлены настоящим Федеральным законом и на соответствие которым эти удостоверяющие центры были аккредитованы, и в случае выявления их несоблюдения выдает предписания об устранении выявленных нарушений;
– осуществляет функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров.

Уполномоченный федеральный орган обязан обеспечить хранение следующей указанной в настоящей части информации и круглосуточный беспрепятственный доступ к ней с использованием информационно-телекоммуникационных сетей:

– наименования, адреса аккредитованных удостоверяющих центров;

– реестр выданных и аннулированных уполномоченным федеральным органом квалифицированных сертификатов;
– перечень удостоверяющих центров, аккредитация которых аннулирована;
– перечень аккредитованных удостоверяющих центров, аккредитация которых приостановлена;
– перечень аккредитованных удостоверяющих центров, деятельность которых прекращена;
– реестры квалифицированных сертификатов, переданные в уполномоченный федеральный орган.

Безусловно, говоря об электронной подписи невозможно не затронуть проблему защиты информации. Минкомсвязью России формируется единое пространство доверия (ЕПД) – совокупность удостоверяющих центов, прошедших процедуру добровольного подтверждения соответствия требованиям по присоединению к этому пространству. ЕПД обеспечивает информационно-технологическую поддержку при использовании ЭЦП в процессах оказания электронных государственных и муниципальных услуг с помощью инфраструктуры электронного правительства.

Согласно Методическим рекомендациям по применению технологии электронной подписи в СМЭВ, все ЭЦП используемые в рамках взаимодействия при оказании госуслуг, должны быть выданы удостоверяющими центрами, входящими в ЕПД (более подробно об этом изложено в следующей главе).

С практической точки зрения, можно говорить об ЭЦП как удобном средстве заверения документов, которое, при обеспечении юридической значимости и ее защищенности, позволяет заявителям сэкономить время и освобождает их от необходимости очного посещения того или иного ведомства.

Главным преимуществом сценария цифрового удостоверения личности является универсальность использования цифровой подписи. Однако данный сценарий имеет ряд недостатков:

– Концентрация рисков информационной безопасности для добросовестных пользователей и рост стимулов злоумышленников к противоправным действиям. Умышленное или неумышленное разглашение закрытого ключа подписи приводит к тому, что злоумышленник может выступать от имени законного обладателя закрытого ключа во всем спектре правовых отношений.
– Высокие требования к информационной безопасности, вызванные концентрацией рисков. Необходимо обеспечить полный контроль со стороны гражданина над жизненным циклом закрытого ключа подписи, достигаемый только применением безопасных устройств

его формирования, хранения и применения на сегодня дорогостоящих вычислительных устройств, управляемых доверенной операционной системой с защищенной памятью.

- Организационная сложность, связанная с необходимостью централизованного управления большим числом ключей цифровой подписи. Требует формирования повсеместной и дорогостоящей инфраструктуры выдачи и приема электронных удостоверений личности. Мировой опыт на сегодня не предоставляет примеров реализации такого рода сценариев для крупных стран, имеющих сложную структуру государственного управления и значительное число граждан.
- Большие требования к культуре использования цифровых методов идентификации. Значительные бюджетные расходы.

КОНТРОЛЬНЫЕ ВОПРОСЫ

Тест

Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации это:

а) Идентификация

б) Аутентификация

в) Авторизация

Главное достоинство парольной аутентификации:

а) Надежность

б) Простота

в) Распространенность

На настоящий момент закрепленными в российском законодательстве аналогами собственноручной подписи НЕ является:

а) ЭЦП

б) Факсимиле

в) Печать

Глава 4.
Инфраструктура открытых ключей и развитие системы удостоверяющих центров

Инфраструктура открытых ключей

PKI (*англ. public key infrastructure*) — инфраструктура открытых ключей. Помимо криптографии в PKI используются два очень важных понятия (они не относятся к криптографии, это понятия из «реального мира»): идентичность и доверие.

Идентичность — набор данных о субъекте (не обязательно человеке), позволяющий отличить субъекта от всех остальных возможных субъектов. Это может быть набор паспортных данных, реквизиты юридического лица (для организаций), другие позиции. А ещё это может быть адрес электронной почты. Не вполне надежно, но зато удобно. В суде такое не примут, а вот в большинстве других случаев (например, при шифровке переписки) – такого адреса вполне достаточно.

Собственно, те, кто выступает в качестве субъектов криптографии (т.е. тех, кто что-то подписывает, шифрует и т.д.), так и называют *субъект криптографии.*

Доверие - это фундаментальная идея всей инфраструктуры открытых ключей. Все связи внутри инфраструктуры - это указание на то, кто кому что и как доверяет. Точно определить термин «доверие» сложно, и для практических нужд PKI используется следующая: «XXX доверяет YYY, если поведение YYY соответствует ожидаемому XXX». Другими словами, если мы кому-то доверяем, то мы уверены, что этот человек будет себя вести так, как мы ожидаем (в хорошем смысле).

Заметим, что доверие редко бывает всеобщим. Обычно мы доверяем в каком-то конкретном вопросе (или наборе вопросов).

Эти два понятия «идентичность» и «доверие» являются основой для построения PKI.

Следует отметить, что суть PKI состоит в том, что задачи идентичности и доверия не могут быть решены только средствами криптографии. Необходима некая договорённость между использующими ключи людьми о том, как именно доказывать связь ключа и пользователя. Решение этого вопроса - и есть основа PKI. Дополнительно же, помимо «главной задачи» решается ещё несколько очень важных задач, позволяющих обеспечить множество видов дополнительного криптографического сервиса.

Ассиметричная криптография (являющаяся основой PKI) использует разные половинки ключа для шифровки и расшифровки (Рис. 5).

Половинки равноценны: если мы ключ разделили на две половинки A и B, то зашифровав с помощью A, мы можем расшифровать с помощью B. Зашифровав с помощью B мы можем расшифровать с помощью A (и только). Мы не можем расшифровать шифр, созданный с помощью A, используя A. И наоборот, зашифрованное B не может быть расшифровано с помощью B. Более того (и это есть основа криптографии), ничем, кроме соответствующей половинки ключа, шифр не может быть расшифрован. Если B - шифровало, то ТОЛЬКО A может расшифровать. Если A шифровало, то ТОЛЬКО B может расшифровать.

Более того, процесс создания половинок A и B таков, что они могут быть созданы только вместе, одновременно. Нельзя сначала сделать A, а потом B. И наоборот - точно так же (т.е., если мы утеряли одну половинку ключа, то вторую не удастся восстановить).

Мы своим административным решением (не имеющим под собой технического обоснования) объявляем одну половинку ключа открытым ключом, а вторую, ей соответствующую, закрытым ключом. Комбинацию открытого и закрытого ключа мы назовём ключевой парой. С точки зрения математики не имеет разницы кто есть кто. С административной же важно не то "кто есть кто", а чтобы использование (хранение и т.д.) открытых/закрытых ключей было разным. На самом деле, именно это - идея, что открытый и закрытый ключ используются с разными целями, и есть истинная цель ассиметричной криптографии. Термины «закрытый» и «открытый» ключи немного неудачны. Им соответствуют более точные английские термины: *private key* (личный ключ) и *public key* (общественный ключ).

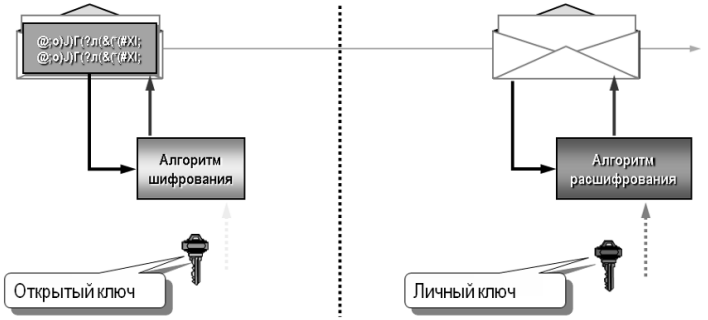

Рис. 5. **Асимметричная криптография**

Как понятно из английских названий, публичный (*public key* - общественный, открытый) ключ мы предоставляем публике, а приватный (*private key* -личный, закрытый) храним в секрете от всех остальных. Любой желающий может зашифровать некий текст (публично известным)

открытым ключом и послать его нам. НИКТО, у кого нет закрытого ключа НЕ МОЖЕТ расшифровать это сообщение. А владелец закрытого ключа (получатель) - может.

Таким образом, используя пары ключей, мы получаем защищённый канал связи, который можно прослушивать, но невозможно ничего понять (кроме факта шифрованной переписки).

Подпись. Из криптографии мы возьмём ещё одну важный термин: криптохэш. Хэш это функция, которая из произвольного набора данных исходного документа по определенному алгоритму формирует данные заданного размера. Например, путем побайтного сложения всех символов документа, мы получим один байт результирующего хэша, по мере возможности, различающийся в зависимости от входных данных. Понятно, что будут совпадения (например, данные №1 и данные №2 могут дать одинаковый хэш), но, чем больше (2, 4, 8 и т.д. байт) длинна хэша, тем реже это будет происходить. Такие совпадения называются колллизией. Что коллизии есть у каждого хэша легко показать: если у нас хэш длинной N-бит из любого набора данных, то всего есть 2^N различных значений хэша. Очевидно, что если мы на вход дадим 2^N+1 данных, то хотя бы для двух значений хэш будет одинаковым (т.е. будет как минимум, одна коллизия).

Криптохэш - это такой хэш, который трудно подобрать. На самом деле требований к хэшу много. Процитируем Википедию[20].

Требования к криптохэшу:

- *Стойкость к коллизиям первого рода*: для заданного сообщения должно быть практически невозможно подобрать другое сообщение, имеющее такой же хэш. Это свойство также называется необратимостью хэш-функции.
- *Стойкость к коллизиям второго рода*: должно быть практически невозможно подобрать пару сообщений, имеющих одинаковый хэш.

Для криптографических хэш-функций также важно, чтобы при малейшем изменении аргумента значение функции сильно изменялось. В частности, значение хэша не должно давать утечки информации даже при изменении отдельных битов аргумента. Это требование является залогом криптостойкости алгоритмов шифрования, хэширующих пользовательский пароль для получения ключа.

Теперь, предположим, что отправитель для заданного сообщения вычислит криптохэш, зашифрует только его своим ЗАКРЫТЫМ ключом, положит результат в подпись письма и перешлет получателю, у которого есть соответствующий открытый ключ. Как уже было пояснено ранее, открытый ключ и закрытый строго обратны друг для друга (открытым

[20] http://ru.wikibooks.org/wiki/Введение_в_PKI

можно расшифровать то, что зашифровано закрытым). Получатель, приняв сообщение, вычислит ту же самую хэш-функцию. После чего он расшифрует хэш из подписи письма. Если присланное значение хэш-функции совпало с вычисленным получателем, то можно быть уверенным в том, что полученное сообщение именно то, которое было подписано отправителем (Рис. 6).

Т.е. подписанное таким образом сообщение невозможно подделать.

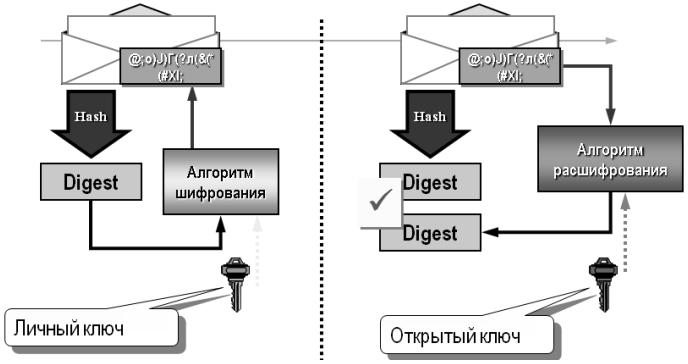

Рис. 6. **Использование подписи - асимметричное шифрование хэша**

Таким образом, корреспонденты могут переписываться не только скрыв текст писем от окружающих, но и точно проверяя, что сообщение не было подделано (но это не может исключить пропажу сообщения, потому что в этом случае не будет ни письма, ни хэша). Это не исключает возможности повторной передачи того же самого сообщения.

Основная функция, которую берёт PKI из криптографии, это функция подписи. Для выполнения этой функции создаётся пара ключей: открытый и закрытый, при этом открытый публикуется, а закрытый держится в секрете. Заметим, что с точки зрения инфраструктуры шифрование сообщения является второстепенной функцией. Отношения доверия выстраиваются, в первую очередь, основываясь на подписях. В то же самое время, область применения PKI очень тесно связана с шифрованием (раз в распоряжении пользователей уже есть ключи, пригодные для шифрования, то ими можно пользоваться).

Например, на практике часто используется комбинация из симметричных и несимметричных методов шифрования, как описано далее:

1. Для обеспечения аутентификации и неотказуемости отправителя, производится создание хэша и его шифрация с использованием закрытого ключа отправителя;
2. Для обеспечения конфиденциальности, сообщение шифруется одноразовым симметричным ключом;
3. Для обеспечения возможности последующей авторизации получателя, зашифрованное сообщение шифруется еще раз открытым ключом получателя
4. Результат пересылается получателю по открытым каналам (Рис. 7).

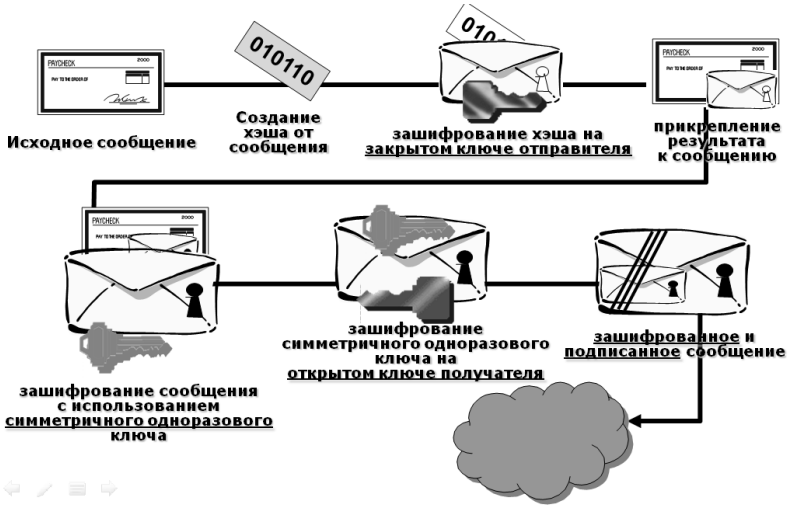

Рис. 7. **Отправка подписанного и зашифрованного сообщения**

Получатель сообщения проделывает процедуры в обратном порядке:

1. С помощью закрытого ключа получателя (своего) восстанавливает зашифрованное сообщение и одноразовый симметричный ключ.
2. Расшифровывает сообщение с использованием одноразового симметричного ключа.
3. Восстанавливается приложенное отправителем значение хэша с помощью открытого ключа отправителя.
4. Вычисляется значение хэша принятого сообщения и сравнивается с принятым значением хэша.
5. Если значения хэш-функций совпадают, и все операции расшифрования прошли успешно, значит можно гарантировать, что

сообщение было отправлено конкретным отправителем, оно не подвергалось изменениям, и оно не могло быть прочитано теми, у кого нет закрытого ключа (Рис. 8).

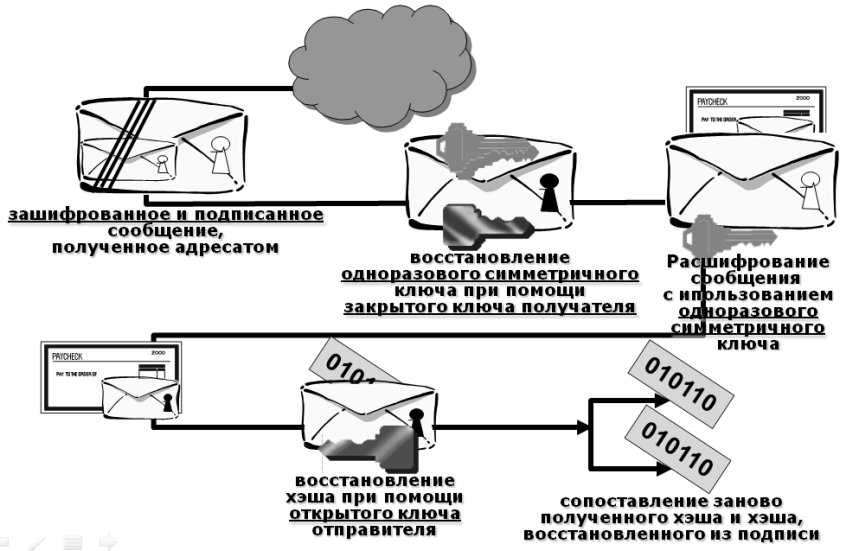

Рис. 8. **Получение подписанного и зашифрованного сообщения**

В любом случае, пожалуй, основным документом, который позволит упорядочить отношения, связанные с использованием ЭЦП, и, как следствие, в дальнейшем позволит использовать документы, подписанные ЭЦП для решения спорных ситуаций, в том числе и в суде, является **регламент использования ЭЦП**. Причем в разработке этого документа должны принимать участие не только разработчики программных средств, необходимых для реализации ЭЦП, но и будущие их пользователи и юристы, поскольку имеется целый ряд вопросов, решение которых невозможно без согласования с действующими и планируемыми регламентами и процессами деятельности организации, а также, с действующим законодательством.

На что же следует обратить внимание в первую очередь при подготовке подобного регламента?

Во-первых, регламент должен четко определять сферы применения ЭЦП и ее место в документообороте организации. Необходимо четко определить, при подписании каких именно документов будет использоваться ЭЦП. Несомненно, наибольший эффект от

использования ЭЦП возможен при ее максимальном применении в организации. Однако тут стоит исходить из требований законодательства – определенные документы до сих пор признаются юридически значимыми только в бумажном виде.

Во-вторых, как и в случае с документами, необходимо определить круг лиц, полномочных использовать ЭЦП. Лицам, наделенным правом использования ЭЦП, следует помнить о том, что нельзя просто взять и передать свой сертификат ключа другому лицу в случае, например, своей болезни или отпуска. Во-первых, сертификат ключа содержит данные о фамилии, имени и отчестве своего владельца и при его использовании кем-либо другим документ все равно окажется подписанным владельцем сертификата. А, во-вторых, сертификат содержит информацию о ключах ЭЦП, что является конфиденциальной информацией. Поэтому передача полномочий по использованию ЭЦП должна быть четко прописана в регламенте. Например, необходимо предусмотреть, что сертификат ключа может быть передан определенному лицу, а сама передача должна оформляться соответствующим распорядительным актом.

В третьих, оба вышеперечисленных условия (определение сферы применения и круга лиц) должны быть взаимосвязаны – необходимо определить, кто и на какие документы вправе ставить свою ЭЦП. Это также поможет избежать ситуаций с одновременным подписанием одного и того же документа с использованием ЭЦП различными лицами.

Итак, использование электронной цифровой подписи требует соблюдения ряда правил, игнорирование которых может повлечь недействительность документов с подобными реквизитами.

Однако, имеются проблемы использования открытых/закрытых ключей. Как было показано ранее, использование несимметричных алгоритмов шифрования и криптохэшей позволяет защитить передаваемую информацию от подслушивания и изменения.

Важным условием этого процесса является обмен открытыми ключами между сторонами (участвующими в обмене информацией). А как пользователь XXX сможет проверить, что полученный ключ - это ключ YYY, а не зловредного ZZZ (который перехватил оригинальное письмо YYY, а вместо него отправил письмо со своим открытым ключом, и получая все сообщения от YYY, он их расшифровывает/меняет, шифрует/подписывает своим ключом и отправляет дальше к XXX)? Каким образом мы можем узнать, что данный ключ принадлежит данному пользователю? Опять шифроблокноты, личные встречи и бумаги с печатями?

Следует подчеркнуть, что это не самый сложный метод: люди обмениваются нотариально заверенными бумагами с распечатанными открытыми ключами - и никакой «зловредный ZZZ» не сможет притвориться одним из них. Главная проблема подобного метода - плохое

масштабирование. Если 300 человек решат так сделать со всеми остальными 299 партнерами, то потребуется 300*299=89700 нотариально заверенных распечаток открытых ключей.

Проблема получения правильного открытого ключа - это первая проблема. Вторая проблема: предположим, что закрытый ключ у пользователя украли. Как ему оповестить всех людей, с кем у него защищённый обмен информацией о краже? А об утрате? Если он это сделает с помощью незащищённых каналов связи, то и злоумышленник может заявить (якобы от лица пользователя): «ключ украли, компьютер сломали, не слушайте больше писем с этим ключом». Т.е. вся защита держится на личном доверии, каких-то других каналах связи? Или вообще ни на чём не держится?

Главная проблема, которую можно выделить из этих примеров: пользователь не имеет возможности проверить, что ключ YYY принадлежит пользователю YYY. Любой другой пользователь (злоумышленник) может сделать то же самое, что пользователь YYY, и назвать себя пользователем YYY.

Система удостоверяющих центров

Для сообщества потенциальных пользователей, объединяющего сотни тысяч или миллионов субъектов, наиболее практичным способом связывания открытых ключей и их владельцев является организация доверенных центров. Этим центрам большая часть сообщества или, возможно, все сообщество доверяет выполнение функций связывания ключей и идентификационных данных (идентичности) пользователей.

Такие доверенные центры в терминологии PKI называются ***удостоверяющими центрами (УЦ)***; они сертифицируют связывание пары ключей с идентичностью, заверяя цифровой подписью структуру данных, которая содержит некоторое представление идентичности и соответствующего открытого ключа. Эта структура данных называется ***сертификатом открытого ключа*** (или просто сертификатом). По сути сертификат представляет собой некое зарегистрированное удостоверение, которое хранится в цифровом формате и признается сообществом пользователей PKI законным и надежным. Для заверения электронного сертификата используется электронная цифровая подпись. Выпуская сертификат открытого ключа некоторого пользователя, УЦ подтверждает и берет на себя ответственность за то, что он установил принадлежность данного открытого ключа именно указанному в сертификате пользователю. В этом смысле *удостоверяющий центр* уподобляется нотариальной конторе, так как подтверждает подлинность сторон, участвующих в обмене электронными сообщениями или документами (Рис. 9).

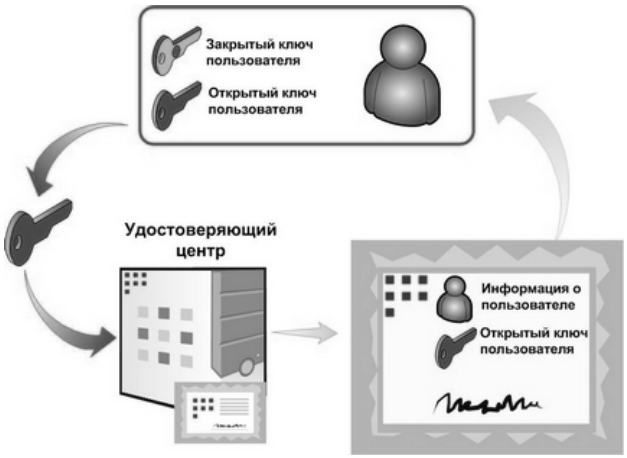

Рис. 9. **Принципиальная схема функционирования удостоверяющего центра**

Хотя УЦ не всегда входит в состав PKI (особенно небольших инфраструктур или тех, которые оперируют в закрытых средах, где пользователи могут сами эффективно выполнять функции управления сертификатами), он является критически важным компонентом многих крупномасштабных PKI (особенно, реализуемых в рамках программ формирования электронного правительства). Непосредственное использование открытых ключей требует дополнительной их защиты и идентификации для установления связи с секретным ключом. Без такой дополнительной защиты злоумышленник может выдавать себя как за отправителя подписанных данных, так и за получателя зашифрованных данных, заменив значение открытого ключа или нарушив его идентификацию. Все это приводит к необходимости проверки подлинности, то есть ***верификации открытого ключа***.

Удостоверяющий центр объединяет людей, процессы, программные и аппаратные средства, вовлеченные в безопасное связывание имен пользователей и их открытых ключей. *Удостоверяющий центр* известен субъектам PKI по двум атрибутам: названию и открытому ключу. *УЦ* включает свое имя в каждый выпущенный им сертификат и в список аннулированных сертификатов (CAC) и подписывает их при помощи собственного секретного ключа. Пользователи могут легко идентифицировать сертификаты по имени *УЦ* и убедиться в их подлинности, используя его *открытый ключ (Рис. 10)*.

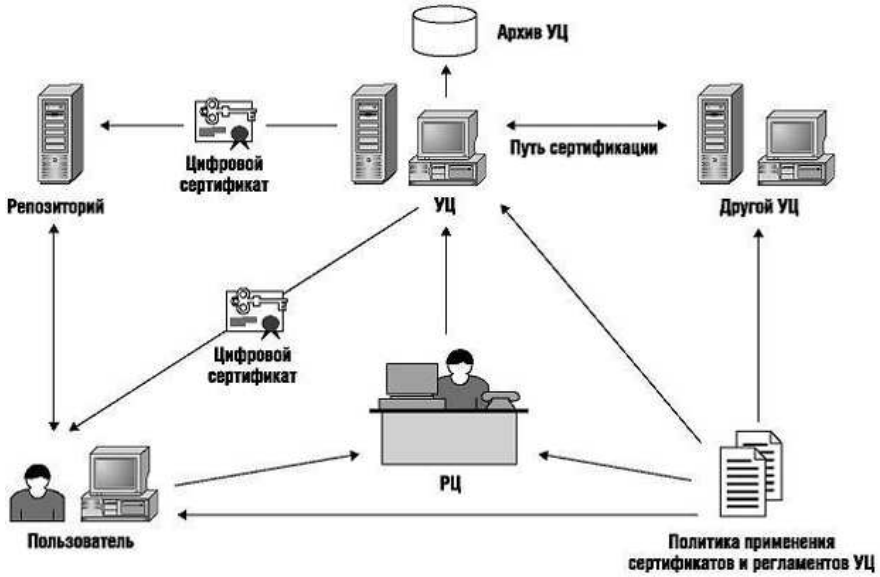

Рис. 10. **Схема маршрутов сертификации в рамках удостоверяющего центра**

Удостоверяющий центр - главный управляющий компонент PKI - выполняет следующие основные функции:

- формирует собственный секретный ключ; если является головным УЦ, то издает и подписывает свой сертификат, называемый самоизданным или самоподписанным;
- выпускает (то есть создает и подписывает) сертификаты открытых ключей подчиненных удостоверяющих центров и конечных субъектов PKI; может выпускать кросс-сертификаты, если связан отношениями доверия с другими PKI;
- поддерживает **реестр сертификатов** (базу всех изданных сертификатов) и формирует списки CAC с регулярностью, определенной регламентом УЦ;
- публикует информацию о статусе сертификатов и списков CAC.

При необходимости *УЦ* может делегировать некоторые функции другим компонентам PKI (Рис. 11). Выпуская *сертификат открытого ключа*, *УЦ* тем самым подтверждает, что лицо, указанное в сертификате, владеет секретным ключом, который соответствует этому открытому ключу. Включая в сертификат дополнительную информацию, *УЦ* подтверждает ее принадлежность этому субъекту. Дополнительная информация может быть контактной (например, адрес электронной почты)

или содержать сведения о типах приложений, которые могут работать с данным сертификатом. Когда субъектом сертификата является другой *УЦ*, издатель подтверждает надежность выпущенных этим центром сертификатов.

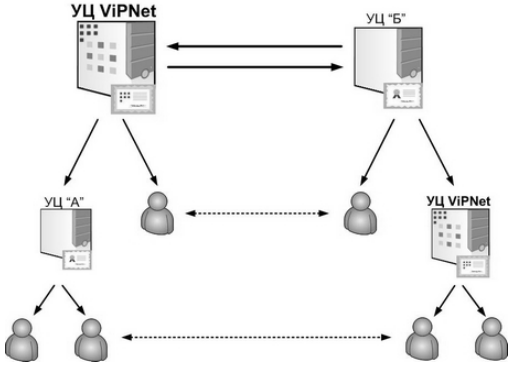

Рис. 11. **Делегирование функций УЦ**

Для организации взаимодействия различных информационных систем и распространения в них доверия часто требуется совместная работа различных PKI. Например, это требуется при межведомственном информационном обмене (Рис. 12). Обычно используется одна архитектура или комбинация нескольких архитектур взаимодействия PKI: иерархическая (подчинение нескольких УЦ вышестоящему головному УЦ), сетевая (объединение одноранговых инфраструктур с перекрестной (кросс-) сертификацией головных УЦ), мостовая (кросс-сертификация каждого УЦ с одним выделенным УЦ-мостом).

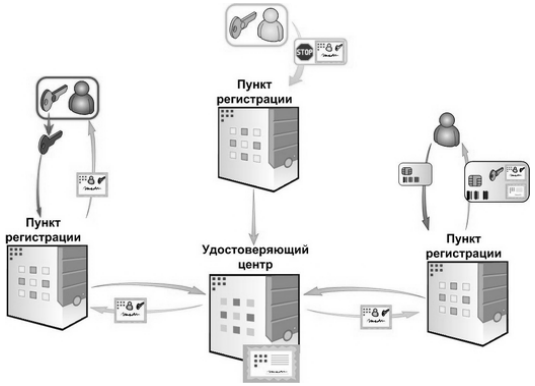

Рис. 12. **Взаимодействие УЦ с пунктами регистрации**

В крупных территориально распределенных PKI взаимодействие УЦ с пользователями обычно производится через пункты регистрации. Пункт регистрации, выступая в качестве филиала УЦ, проводит идентификацию пользователей, генерирует для них ключевые пары или устанавливает факт владения закрытым ключом по предъявленному открытому ключу, после чего формирует и передает запрос на сертификацию в УЦ. Также через пункт регистрации в УЦ передаются запросы пользователей на изменение статуса уже выпущенных сертификатов. Результаты обработки запросов из УЦ пользователи тоже получают в пункте регистрации.

Сеть пунктов регистрации позволяет создать более эффективную PKI. Для обеспечения высокого уровня безопасности операций по выпуску и обслуживанию сертификатов к УЦ предъявляются специальные требования по организационной, физической и информационной безопасности. Перенос части функций УЦ в пункт регистрации позволяет снизить эти требования, что уменьшает расходы на создание УЦ. Пункты регистрации снижают нагрузку на УЦ по обработке запросов пользователей, вплоть до полного исключения непосредственного взаимодействия пользователей и УЦ. Это также ведет к снижению эксплуатационных расходов на содержание УЦ. Кроме того, чем разветвленнее сеть пунктов регистрации, тем ниже расходы пользователей, связанные с процедурой регистрации.

Действия *УЦ* ограничены ***политикой применения сертификатов (ППС)***, которая определяет назначение и содержание сертификатов. *УЦ* выполняет адекватную защиту своего секретного ключа и открыто публикует свою политику, чтобы пользователи могли ознакомиться с назначением и правилами использования сертификатов. Ознакомившись с *политикой применения сертификатов* и решив, что доверяют *УЦ* и его деловым операциям, пользователи могут полагаться на сертификаты, выпущенные этим центром. Таким образом, в PKI *удостоверяющие центры* выступают как доверенная третья сторона.

Нельзя утверждать, что PKI сама по себе является *инфраструктурой безопасности*, но она может быть основой всеобъемлющей инфраструктуры безопасности. Инфраструктура открытых ключей представляет собой комплексную систему, сервисы которой реализуются и предоставляются с использованием технологии открытых ключей. Цель PKI состоит в управлении ключами и сертификатами, посредством которого организация может поддерживать надежную и доверенную сетевую среду. PKI позволяет использовать сервисы шифрования и выработки цифровой подписи согласованно используемой широким кругом приложений, функционирующих в среде открытых ключей.

Таким образом, Инфраструктура открытых ключей (PKI) - это современная технология аутентификации, использующая для

идентификации субъектов криптографию с открытыми ключами вместе со следующими механизмами:

- механизмом установления доверия на базе определенной модели доверия;
- механизмом присваивания субъектам имен, уникальных в данной среде;
- механизмом распространения информации, характеризующей правильность связывания определенной пары ключей (*открытого* и секретного) с определенным именем субъекта в данной среде (такая информация фиксируется и предоставляется центром, которому доверяет верификатор информации).

Строго говоря, *PKI* обеспечивает аутентификацию - не больше и не меньше; вопреки широко распространенному мнению о возможностях *PKI*, она не реализует:

- авторизацию (хотя может применяться с целью защиты информации, используемой для авторизации);
- доверие (хотя и способствует установлению отношений доверия, подтверждая принадлежность данного *открытого ключа* определенному субъекту);
- именование субъектов (а только связывает известные имена субъектов с их *открытыми ключами*);
- защиту компьютерных систем и сетей (служит базисом сервисов безопасности, но не заменяет собой другие средства и методы защиты).

Конечно, аутентификация - это только один из необходимых сервисов безопасности. Многие приложения также требуют конфиденциальности, целостности и невозможности отказаться от участия в обмене информацией. Технология *PKI* обеспечивает поддержку всех этих сервисов.

КОНТРОЛЬНЫЕ ВОПРОСЫ

Тест

Одним из основных достоинств несимметричного шифрования является:

а) Стойкость к дешифрованию

б) Низкие требования к вычислительным ресурсам

в) Безопасность распространения ключей для расшифровки

Если длина хэша 1 байт, то при каком минимальном количестве документов обязательно возникнет коллизия их хэшей:

а) 19

б) 300

в) 1025

Основная используемая функция ЭЦП:

а) Подпись

б) Шифрование

Для обеспечения идентичности и доверия достаточно:

а) Шифрования

б) Договоренностей

в) Наличие организационно-технологической инфраструктуры

Удостоверяющий центр известен субъектам PKI по атрибутам:

а) название и открытый ключ

б) название и закрытый ключ

в) IP-адрес и открытый ключ

Политика применения сертификатов определяет:

а) порядок выпуска сертификатов

б) назначение и содержание сертификатов

в) политику защиты конфиденциальной информации

Глава 5.
Идентификация личности с использованием электронных карт

Идентификационные карты

Для решения таких задач построения инфраструктуры доверия, как идентификация личности, возможность использования ЭЦП, получение услуг в электронном виде и т.д., во многих странах переходят от традиционных удостоверений личности (паспорт и другие документы) к их электронным аналогам – ID-картам (в России утверждено название «Универсальная электронная карта» - или УЭК).

ID-карта во многих европейских странах уже является первичным удостоверением личности и признается всеми членами Евросоюза и государствами-членами Шенгенского соглашения, не входящими в Европейский Союз, в качестве официального удостоверения для путешествующего лица.

Такая карта обычно хранит информацию о своем владельце, чаще всего это: полное имя владельца, пол, национальный идентификационный номер, криптографические ключи и сертификаты.

Чтобы использовать электронные возможности ID-карты, необходимо иметь:

- ID-карту вместе с PIN-кодами;
- терминал или компьютер;
- считывающее устройство (Рис. 13);
- программное обеспечение для ID-карты

Рис. 13. **ID-карта в считывающем устройстве**

Карту необходимо вставить в считывающее устройство (или поднести к бесконтактному) и ввести PIN-коды. ID-карта должна оставаться в считывающем устройстве в течение всего времени доступа.

Большинство ID-карт поддерживает стандарт X.509, что делает возможным их использование в государственных электронных сервисах других стран. Все крупные банки, большинство финансовых и других сервисов поддерживают аутентификацию с помощью ID-карты.

Чип в карте содержит криптографическую пару (общедоступный и личный ключи), которая позволяет пользователям подписывать электронные документы с использованием публичных ключей. Также, существует возможность шифровать документы, используя публичный ключ держателя карты, но она редко используется, поскольку при утере или повреждении карты расшифровать документы будет невозможно.

По законам стран, использующих ID-карту, электронная цифровая подпись юридически эквивалентна подписи от руки.

Для нас интересен опыт Эстонии, недавно, но активно внедрившей ID-карту (Рис. 14), как инструмент доверия, во многие сферы жизни:

Рис. 14. **Пример ID-карты используемой в Эстонии**

Во многих газетах Эстонии (например, Eesti Päevaleht) есть возможность оставлять комментарии к web-колонкам, используя ID-карту для аутентификации.

В больших городах Эстонии, таких как Таллин и Тарту, разрешено пользоваться виртуальным проездным билетом, который связан с ID-картой.

Владелец такого билета может так же заказать услугу напоминания по SMS или на e-mail о том, когда истекает срок действия билета, или автоматически купить следующий, пользуясь банковским платёжным поручением.

Чтобы использовать «виртуальный» проездной билет, пассажир должен иметь при себе ID-карту. При проверке контролёр вставляет ID-карту в специальное устройство — считыватель ID-карт, которое определяет наличие билета, а также напоминает об окончании срока его действия. В исключительных случаях наличие билета можно проверить по личному коду пассажира, ID-карта в таком случае не обязательна. Проверка билета такими способами занимает всего пару секунд.

ID-карта Эстонии также используется для идентификации на интернет-выборах.

В феврале 2007 года Эстония была первой страной в мире, которая ввела электронное голосование на парламентских выборах. Более 30 тыс. человек приняло участие в электронном голосовании.

На муниципальных выборах 2009 года возможностью проголосовать с помощью ID-карты воспользовались уже более 100 тыс. человек — 9,5 % населения, имеющего право голоса.

ID-карта используется для аутентификации и авторизации на государственном портале eesti.ee и в общегосударственной базе данных X-tee. Также планируется использовать ID-карту как основное средство аутентификации в ныне внедряемой электронной системе здравоохранения E-tervis.

В настоящее время граждане Эстонии и граждане других государств-членов Европейского Союза, получившие в Эстонии идентификационную карту на правах резидента Эстонии, имеют право использовать ID-карту в качестве удостоверения личности в поездках по территории Евросоюза и для пересечения его внешних границ как на въезд, так и на выезд из стран Евросоюза, Европейского экономического пространства, в том числе Исландии и Норвегии, а также Швейцарии. При этом на оборотной стороне ID-карты должна быть машиносчитываемая информация о владельце ID-карты, а кроме того, содержаться двуязычная запись на эстонском и английском языках: «EL kodanik / EU citizen». Трёхстрочная машиносчитываемая информация включает в себя данные о номере идентификационной карты и контрольную цифру в первой строке, дату окончания срока действия этого документа с контрольным числом и трёхбуквенным международным кодом страны гражданской принадлежности во второй строке, фамилию и имена держателя карты - в третьей строке.

Идентификационными картами по сути являются все виды платёжных банковских пластиковых карт, а также удостоверения личности (пропуска), выполненные в формате контактных и бесконтактных пластиковых карт.

Существует ряд международных стандартов, определяющих практически все свойства пластиковых карточек, начиная от физических свойств пластика, размеров карточки, и заканчивая содержанием информации, размещаемой на карточке тем или иным способом:

- ISO 7810 - «Идентификационные карты — физические характеристики»;
- ISO 7811 - «Идентификационные карты — методы записи»;
- ISO 7812 - «Идентификационные карты — система нумерации и процедура регистрации идентификаторов эмитентов» (5 частей);
- ISO 7813 - «Идентификационные карты — карты для финансовых транзакций»;
- ISO 4909 - «Банковские карты — содержание третьей дорожки магнитной полосы»;
- ISO 7816 - «Идентификационные карты — карты с микросхемой с контактами» (6 частей)

В Германии, начиная с ноября 2010 года вводится новое удостоверение личности, содержащее функцию электронного удостоверения (ID-карта). Наряду с электронными паспортами других европейских стран оно сделает возможным оказание трансграничных интероперабельных услуг. Основой для этого является спецификация CEN/TS 15480 «Система идентификационных карт – Европейская Гражданская Карта» Европейского комитета по стандартизации (CEN). Институт Fraunhofer FOKUS совместно с партнёром SagemOrga исследует, насколько европейские карты удостоверения личности могут быть усовершенствованы в плане удобной для пользователя интеграции с электронными сетевым приложениями. Технология Match-on-card-Technology (MoC) фирмы SagemOrga поддерживает использование биометрических признаков, таких как отпечатки пальцев, в качестве альтернативы личному коду (PIN) в целях получения доступа к функциям карты.

Fraunhofer FOKUS в своей лаборатории Secure eldenity Lab разработал демонстрационный сценарий аутентификации пользователей на основе применения технологии MoC. На примере прототипного портала совместных исследовательских проектов в сценарии «ECC 2.0» демонстрируется возможность аутентификации при помощи электронного удостоверения личности в сочетании с основанной на биометрии технологией MoC. Инновативные функции, такие как удобный пользователю отказ от шестизначного личного кода, могли бы, при

сохранении высокого уровня безопасности, в будущем применяться в электронных удостоверениях личности.

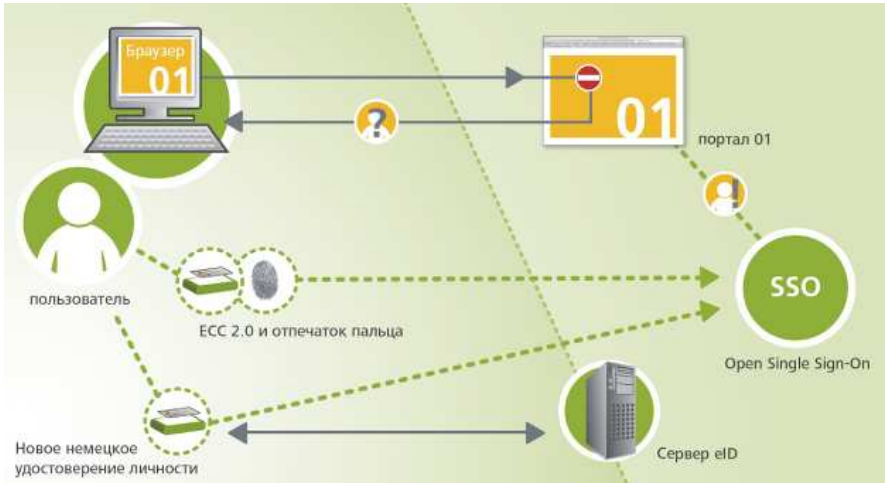

Рис. 15. **Пример взаимодействия с использованием ID-карты в Германии**

Универсальная электронная карта

Универсальная электронная карта (УЭК) планируется как основное средство идентификации личности при предоставлении государственных и муниципальных услуг населению в Российской Федерации. Универсальная электронная карта призвана упростить бюрократические процедуры, улучшить качество государственных услуг, повысить информированность граждан о своих правах, а также способствовать развитию безналичных расчётов. УЭК можно будет использовать в качестве банковской карты как полноценное платёжное средство (обязательное по законодательству к приёму). УЭК сократит нагрузку на подразделения организаций, которые занимаются расчетами с персоналом и ведением личных дел сотрудников (бухгалтерия, отдел кадров).

УЭК станет единой для жителей всех регионов страны и заменит существующие социальные карты, объединив в себе ряд функций — полиса обязательного медицинского и пенсионного страхования, полиса ОСАГО, студенческого билета, читательского билета, средства оплаты

школьного питания, средства контроля посещения школ учащимися, проездных документов и банковских карт.

1	Прием заявок на прием к врачу
2	Заполнение и направление в аптеки электронных рецептов
3	Информирование о предоставлении гос. соцпомощи в виде набора социальных льгот
4	Выплаты по безработице
5	Техосмотр транспортных средств
6	Прием экзаменов и выдача водительских удостоверений
7	Регистрация автотранспорта и прицепов
8	Сведения об автомобильных правонарушениях
9	Сведения из ЕГРП о недвижимом имуществе и сделках с ним
10	Сведения из Государственного кадастра недвижимости
11	Оформление, выдача, замена и учет паспортов и других документов
12	Информирование о задолженностях по налогам, пеням и штрафам
13	Сведения о состоянии ИЛС в системе обязательного пенсионного страхования
14	Медуслуги, включая взаиморасчеты ОМС
15	Выплата пенсий, пособий, субсидий

ИСТОЧНИК: ПРАВИТЕЛЬСТВО РФ

Рис. 16. **Сферы применения УЭК**

В феврале 2011 года Президент Дмитрий Медведев высказал пожелание интегрировать водительское удостоверение в УЭК.

С 1 сентября 2010 г. в трех российских регионах началась реализация пилотного проекта по внедрению универсальных электронных карт. Выбор регионов и категорий населения объяснялся тем, что здесь уже существуют развитые системы социальных карт. В Астраханской области такой проект реализует Сбербанк, в Башкортостане — банк «Уралсиб», в Татарстане — банк «Ак Барс» Правда, последние отменять пока не будут: на первом этапе системы социальных и универсальных карт будут действовать параллельно. И так будет до тех пор, пока универсальные карты не обеспечат аналогичную функциональность. Социальные карты будут обслуживаться до завершения их срока действия.

До запуска пилотных проектов по УЭК спектр услуг по социальным картам в опытных регионах был весьма ограничен. В Татарстане, например, по ним доступен только льготный проезд в общественном транспорте. В Астраханской области и Башкортостане карты предоставляют более широкий перечень услуг, в том числе медицинских и банковских. В Башкирии помимо прочего по социальной карте можно получать сведения о размере пенсионных накоплений, налогов, а также различные скидки и бонусы.

В программе пилотного проекта было предусмотрено 15 видов государственных услуг. Предполагалось, что помимо стандартного набора в рамках УЭК по карте можно будет проводить регистрацию автомобилей

и техосмотр, на ней будут отражаться данные из ЕГРП и единого кадастра недвижимости, информацию об административных правонарушениях в области дорожного движения; о состоянии пенсионного счета, ОМС; необходимой для оформления, выдачи, замены паспорта и других документов и т. д.

К концу 2010 года был завершен первый этап тестирования системы в 3-х пилотных регионах. Согласно Федеральному закону №210 ФЗ «О предоставлении государственных и муниципальных услуг» предполагалось что УЭК можно будет получить начиная с 1 января 2012 г.

В марте 2011 г. Президент Дмитрий Медведев дал поручения, касающиеся внедрения в России УЭК. Список поручений охватывал срок до конца 2011 г.

Из списка поручений следовало, что в истории внедрения российских УЭК 2011 год останется подготовительным периодом, во время которого будет составлена смета проекта, подготовлена его нормативная и законодательная база, разработаны регламенты, начнется обучение граждан пользованию электронными госуслугами и подготовка инфраструктуры.

Кроме законотворческой стороны проблемы, мероприятия 2011 г. коснулись технологий, связанных с внедрением УЭК. Предполагалось, что в 2011 году должна была начаться разработка персональных терминалов для считывания универсальной карты и соответствующего ПО. К концу 2011 года в регионах должны были быть созданы базы данных содержащие цифровые фотографии граждан, основываясь на которых должен был производиться выпуск карт.

К сожалению, эти поручения не были выполнены в полном объеме и сроки внедрения УЭК были перенесены на год.

Министр связи Татарстана Николай Никифоров рассказал CNews, что в госорганах региона установлено около 10 тыс. считывающих устройств, стоимость каждого из которых он оценивает «примерно в 200 руб.». По его словам, в Татарстане активно используются 180 тыс. региональных электронных карт при их общем тираже 250 тыс.

В своих поручениях Медведев предусмотрел стимулирование граждан к пользованию универсальными электронными картами. Так одним из побудительных мотивов к их получению может стать снижение госпошлин и других обязательных платежей для потребителей госуслуг с помощью карт.

Наконец, Президент России дал поручение разрешить один из самых болезненных вопросов внедрения УЭК — финансирование всего проекта. До марта 2011 г. внедрение инфраструктуры карт в пилотных регионах

происходило за счет участников ОАО «Универсальная электронная карта» - Сбербанка (34%), банка «Уралсиб» (33%) и банка «АК БАРС» (33%). При этом, по словам главы Сбербанка Германа Грефа, «пока ни один из инвесторов не смог окупить затраты на инфраструктуру УЭК, а первые надежды на окупаемость относятся ко времени через 2-3 года». Отчасти, по этой причине, как утверждает глава Сбербанка, от участия в проекте уклонились «Банк Москвы» и ВТБ.

В конце 2010 ОАО «УЭК» объявило тендер для определения исполнителя работ по разработке, внедрению и сопровождению системы управления проектом «Организация предоставления государственных и муниципальных услуг с использованием универсальной электронной карты». Победу в тендере одержала компания ЗАО «Проектная Практика».

В течение 2011 года, специалисты ГК «Проектная Практика» должны были:

- разработать нормативно-методическую базу и календарные планы проекта;
- создать проектный офис;
- разработать информационную систему для управления проектом;
- провести обучение сотрудников ОАО «УЭК» в области управления проектами;
- осуществлять мониторинг реализации проекта и техническую поддержку информационной системы.

В марте 2011 года Правительство РФ утвердило **технические требования** к универсальной электронной карте. Карта будет содержать сведения о ее владельце, представленные как в визуальной, так и в электронной форме. В перечень требований также входит оснащение карты интегральной схемой отечественного производства с криптографическим ядром. Объем памяти схемы должен составлять не менее 72 Кбайт, и она должна содержать области, защищенные от несанкционированного доступа. Постоянная и энергонезависимая перезаписываемая память интегральной схемы универсальной электронной карты должна обеспечивать хранение записанной информации не менее 5 лет.

Внешний вид УЭК (не прошедший ещё официального утверждения) приведен на официальном сайте карты http://www.uecard.ru/ (рис. 17).

11 февраля 2011 г. на портале CNews по инициативе Минкомсвязи был проведен интернет-опрос, посвященный трем вариантам дизайна карты. Более половины голосов (5 тыс. человек) было отдано за вариант, представленный ниже.

1 Индивидуальный номер карты
2 Логотип банка-эмитента банковского приложения
3 Логотип платежного продукта
4 Микропроцессор
5 Элементы защитного комплекса (трехзначный код проверки подлинности карты)
6 Логотип «УЭК»
7 Контактная информация уполномоченной организации субъекта РФ, выдавшей карту
8 Фотография (в случае выдачи карты по заявлению гражданина)
9 Фамилия держателя карты
10 Имя держателя карты
11 Отчество держателя карты (если имеется)
12 Пол
13 Дата рождения
14 Срок действия универсальной электронной карты
15 Образец подписи
16 Логотип дополнительного платежного продукта (если имеется)
17 Номер банковской карты
18 Страховой номер индивидуального лицевого счета в системе обязательного пенсионного страхования (СНИЛС)
19 Номер полиса обязательного медицинского страхования (ОМС)

Рис. 17. **Внешний вид УЭК**

Для граждан получение первой такой карты будет бесплатным, а за перевыпуск придется заплатить, но не более 300 рублей. Возможно, гражданам придется платить за сопровождение приложений, которые есть на карте. Стоимость сопровождения четырех обязательных федеральных приложений (в том числе идентификационные данные, медицинское, пенсионное приложения) будет устанавливать государство. Оно будет либо бесплатным, либо обойдется в незначительную сумму.

Для реализации возможностей универсальных электронных карт с целью получения государственных услуг в электронном виде создается Единая платежно-сервисная система «Универсальная электронная карта» (ЕПСС УЭК).

В зависимости от вида услуги процесс ее предоставления может быть мгновенным, когда услуга предоставляется в момент обращения, или длительным, когда предоставление услуги требует определенного времени.

В результате среди всего множества услуг выделяются длительные и мгновенные услуги.

Предоставление длительных услуг включает в себя следующие последовательно выполняемые стадии:

- стадия заказа услуги (оформление и направление поставщику услуги (ПУ) запроса на ее оказание и получение от ПУ ответа с результатом приема запроса к исполнению);
- стадия оказания услуги (выполнение ПУ действий, предусмотренных сценарием оказания услуги);
- стадия уведомления гражданина о результате оказания услуги.

Инфраструктура ЕПСС УЭК призвана обеспечить поддержку процесса оказания длительной услуги только на ее первой стадии. Вторая и третья стадии процесса оказания длительной услуги реализуются поставщиком услуги самостоятельно без использования инфраструктуры ЕПСС УЭК.

При оказании мгновенных услуг все три перечисленные выше стадии процесса объединяются вместе путем включения второй и третьей стадии внутрь первой. В результате гражданин, запросивший услугу, в рамках первой и единственной стадии процесса (стадии заказа услуги) получает в ответе на свой запрос результат оказания услуги Поставщиком.

Под процессом оказания услуги в рамках ЕПСС УЭК понимается совокупность действий, выполняемых участниками ЕПСС УЭК в рамках стадии заказа услуги – процесс заказа услуги.

Началом процесса заказа услуги является обращение гражданина за услугой с использованием терминала, подключенного к инфраструктуре ЕПСС УЭК, с целью подготовки и направления Поставщику услуги запроса на оказание услуги. Окончанием процесса заказа услуги является получение гражданином на том же терминале ответа от Поставщика услуги, содержащего информацию о результате обработки запроса на оказание услуги (для мгновенных услуг – информацию о результате оказания услуги Поставщиком). Процесс заказа услуги от его начала до окончания осуществляется в рамках одного сеанса взаимодействия гражданина с Поставщиком услуги с использованием терминала.

Услуги, заказ которых может осуществляться с использованием карт УЭК, содержатся в сводном реестре услуг ЕПСС УЭК, ведение и распространение которого в рамках ЕПСС УЭК обеспечивает Оператор ЕПСС УЭК. Сводный реестр услуг ЕПСС УЭК содержит описание следующих категорий услуг:

- государственные услуги (федеральные, региональные, муниципальные);
- коммерческие услуги;
- услуги по автономному обслуживанию карты УЭК на терминале.

Описание процесса ведения и распространения сводного реестра услуг в рамках ЕПСС УЭК, а также описание состава информации по каждой услуге, включенной в состав реестра, приведены в документе «Операционные правила сервисной части ЕПСС УЭК. Порядок ведения реестра услуг ЕПСС УЭК».

Цель реализации процесса заказа услуги с использованием карты УЭК - обеспечить для гражданина – держателя карты УЭК возможность дистанционного обращения к различным организациям, предоставляющим услуги (Поставщикам услуг) в электронной форме, независимо от места территориального расположения поставщика услуги и места территориального расположения гражданина, обратившегося за услугой.

Для достижения этой цели в рамках сервисной части ЕПСС УЭК создается инфраструктура, призванная решить следующие основные задачи, связанные с обеспечением унифицированного процесса заказа услуг с использованием карт УЭК:

- Обеспечить унификацию схем заказа услуг с использованием карт УЭК для множества поставщиков, предоставляющих услуги в электронной форме, сделав их доступными повсеместно, независимо от места обращения гражданина за услугой и места расположения поставщика услуги.
- Обеспечить развитие участниками ЕПСС УЭК терминальной сети для массового обращения граждан за любыми услугами, предоставляемыми в электронной форме различными поставщиками услуг в рамках ЕПСС УЭК.
- Создать условия для массового включения в процесс оказания услуг в электронной форме различных организаций - поставщиков услуг, заинтересованных в расширении инфраструктуры доступа к своим услугам.

В рамках ЕПСС УЭК можно выделить три схемы заказа услуги:

- Внутрирегиональная схема заказа услуги реализуется в том случае, когда участник ЕПСС УЭК, в терминале которого запрашивается услуга (Оператор каналов обслуживания), может напрямую обратиться к поставщику запрошенной услуги, то есть выступает в схеме заказа услуги также в роли Оператора поставщиков услуг.
- Внутриведомственная схема заказа услуги реализуется в том случае, когда участник ЕПСС УЭК, в терминале которого запрашивается услуга (Оператор каналов обслуживания), сам же осуществляет оказание запрошенной услуги, то есть, выступает в схеме заказа услуги также в роли Поставщика услуг.

- Трансрегиональная схема заказа услуги реализуется в том случае, когда участник ЕПСС УЭК, в терминале которого запрашивается услуга (Оператор каналов обслуживания), для передачи запроса на оказание услуги обращается к Оператору ЕПСС УЭК.

В процессе заказа услуги задействованы следующие участники:

N п/п	Участник процесса	Комментарий
1	Банк-эквайрер	Организация, осуществляющая перечисление в адрес Поставщика услуг денежных средств по платежам граждан, сделанным в процессе заказа платных услуг
2	Банк-эмитент	Организация, осуществляющая авторизацию платежных операций, связанных с оплатой услуг, заказ которых осуществляется с использованием карты УЭК.
3	Гражданин	Держатель карты УЭК, обращающийся в терминал, подключенный к Оператору каналов обслуживания с целью заказа услуги.
4	Оператор ЕПСС УЭК	Организация, обеспечивающая взаимодействие в рамках ЕПСС УЭК всех ее участников. Оператором ЕПСС УЭК является федеральная уполномоченная организация (ФУО).
5	Оператор каналов обслуживания	Оператор каналов обслуживания (ОКО) - участник ЕПСС УЭК, управляющий сетью терминалов, на которых инициируются действия по заказу услуг гражданами с использованием карт УЭК. В качестве Оператора каналов обслуживания могут выступать следующие категории участников ЕПСС УЭК: • Уполномоченные организации субъектов (УОС); • ФУО; • Банк-участник; • Сервис-партнер.
6	Оператор поставщиков услуг	Оператор поставщиков услуг (ОПУ) - организация, непосредственно осуществляющее взаимодействие с Поставщиками услуг с целью передачи ПУ запроса гражданина на оказание услуги и получения ответа на запрос. В качестве Оператора поставщиков услуг могут выступать следующие категории участников ЕПСС УЭК:

		• Уполномоченные организации субъектов (УОС); • ФУО; • Банк-участник; • Сервис-партнер.
7	Поставщик услуг	Поставщик услуг (ПУ) - организация, непосредственно осуществляющая предоставление услуг гражданам по их запросам, сформированным с использованием карт УЭК. В качестве Поставщика услуг могут выступать: • УОС; • ФУО; • Банк-участник; • Сервис-партнер; • прочие организации, не являющиеся Участниками ЕПСС УЭК.

Краткое описание взаимодействия участников

При заказе услуги по внутрирегиональной схеме роль Оператора каналов обслуживания и роль Оператора поставщиков услуг исполняется одним участником ЕПСС УЭК, который:

- обеспечивает подготовку Гражданином на терминале с использованием карты УЭК данных запроса на оказание услуги;
- подготавливает запрос на оказание услуги для направления его Поставщику услуги (по итогам успешной авторизации заказа услуги Оператором ЕПСС УЭК);
- обращается к Поставщику услуги с запросом на оказание услуги и получает ответ с результатом приема заказа Поставщиком услуг;
- предоставляет Гражданину ответ Поставщика услуги с результатом приема заказа (на экране терминала и, если требуется, в печатной форме).

Заказ услуги по внутриведомственной схеме производится аналогично, с той разницей, что роль Поставщика услуг такой схеме исполняется тем же участником ЕПСС УЭК, который исполняет роли Оператора каналов обслуживания и Оператора поставщиков услуг.

В случае совмещения нескольких ролей одним участником ЕПСС УЭК, показанное на диаграмме взаимодействие между этими ролями рассматривается как вырожденное.

Процесс заказа услуги по внутрирегиональной (внутриведомственной) схеме включает в себя следующие основные действия:

1. Процесс заказа услуги с использованием карты УЭК инициируется Гражданином после выбора требуемой ему услуги из перечня услуг, предложенного на терминале Оператора каналов обслуживания (предполагается, что выбрана услуга, заказ которой осуществляется по внутрирегиональной (внутриведомственной) схеме).

2. Оператор каналов обслуживания, с использованием метаинформации по выбранной услуге, обеспечивает подготовку Гражданином на терминале с использованием карты УЭК данных запроса на оказание услуги (данные запроса защищаются криптограммой, сформированной картой УЭК гражданина, обратившегося за услугой). Процесс подготовки данных предусматривает взаимодействие с Гражданином и картой УЭК. Для отдельных услуг в процессе подготовки запроса возможно обращение к Поставщику услуг с целью получения специальных данных по услуге и/или проверке правильности задания параметров запроса на оказание услуги. Детальные требования к порядку подготовки данных запроса на оказание услуги приведены в документе «Спецификация терминалов».

3. Оператор каналов обслуживания обращается к Оператору ЕПСС УЭК с целью авторизации заказа услуги, направляя ему запрос на авторизацию заказа услуги, включающий необходимые данные запроса на оказание услуги, подготовленные на терминале с участием гражданина, и получает ответ с результатом авторизации и, в случае предоставления авторизации заказа, дополнительной информацией, которая должна быть включена в запрос на оказание услуги, направляемый в адрес Поставщика услуги.

4. Оператор ЕПСС УЭК получает от Оператора каналов обслуживания запрос на авторизацию заказа услуги, осуществляет авторизацию заказа услуги и направляет ответное сообщение инициатору запроса, включая в него результат авторизации, и, в случае предоставления авторизации, необходимую дополнительную информацию: идентификатор заказа, присвоенный оператором ЕПСС, ЭЦП оператора ЕПСС УЭК, заверяющая определенный набор данных заказа, и др. В том случае, если в сообщении-запросе, полученном от ОКО, присутствует поручение держателя карты по оплате услуги с его счета, привязанного к карте УЭК, Оператор ЕПСС УЭК инициирует авторизацию платежной операции. В случае отказа в авторизации ответное сообщение содержит причину отказа. По результатам авторизации Оператором ЕПСС УЭК фиксируется операционный документ по заказу услуги (см. глоссарий), который будет использоваться им в процессе осуществления расчетов.

5. На основании полученного от Оператора ЕПСС УЭК ответа Оператор каналов обслуживания принимает решение о продолжении или

прекращении обработки заказа в зависимости от полученного в ответе результата.

6. В случае получения отказа в авторизации Оператор каналов обслуживания подготавливает с использованием метаинформации по запрошенной услуге ответ для отображения гражданину на экране терминала. В ответе должна содержаться причина, по которой запрошенная услуга не может быть предоставлена.

7. В случае получения подтверждения авторизации Оператор каналов обслуживания подготавливает запрос на оказание услуги для направления его Поставщику услуги. В ходе подготовки запроса на оказание услуги в него включаются данные, подготовленные в рамках диалога с гражданином на терминале, и дополнительная информация по заказу, полученная в ответе от Оператора ЕПСС УЭК (ЭЦП Оператора ЕПСС, присвоенный оператором ЕПСС идентификатор заказа и др.).

В случае заказа услуги по внутрирегиональной схеме взаимодействие, связанное с передачей подготовленного Оператором каналов обслуживания запроса на оказание услуги Оператору поставщиков услуг в рамках данной схемы является вырожденным и в действительности отсутствует, поскольку роли Оператора каналов обслуживания и Оператора поставщиков услуг исполняются одним Участником ЕПСС УЭК.

В случае заказа услуги по внутриведомственной схеме взаимодействие, связанное с передачей подготовленного Оператором каналов обслуживания запроса на оказание услуги Оператору поставщиков услуг и далее Поставщику услуги в рамках данной схемы является вырожденным и в действительности отсутствует, поскольку в таком случае все три роли: Оператора каналов обслуживания, Оператора поставщиков услуги и Поставщика услуги исполняются одним участником ЕПСС УЭК.

8. Участник ЕПСС УЭК, совмещающий в себе роли Оператора поставщиков услуг и Оператора каналов обслуживания, обращается к Поставщику региональной услуги, направляя ему подготовленный запрос на оказание услуги, и получает от Поставщика услуги ответ по заказу услуги.

9. Поставщик услуги обрабатывает полученный запрос на оказание услуги, используя данные, содержащиеся в составе имеющейся у него метаинформации (метаинформация для обработки запроса) по услуге, указанной в запросе, и, с использованием той же метаинформации (метаинформация для формирования ответа на запрос), формирует по итогам обработки ответ по заказу услуги и направляет его источнику получения запроса. По итогам обработки Поставщик услуги фиксирует у себя операционный документ по заказу услуги, который будет использоваться им в процессе осуществления расчетов.

10. Оператор каналов обслуживания с использованием метаинформации по услуге (метаинформация для визуализации ответа) отображает содержащийся в ответе результат заказа услуги на экране терминала для гражданина. При необходимости (в случае наличия в метаинформации по услуге соответствующих данных) результат заказа услуги выводится на печать.

11. После отображения результата заказа услуги гражданину процесс заказа услуги считается завершенным.

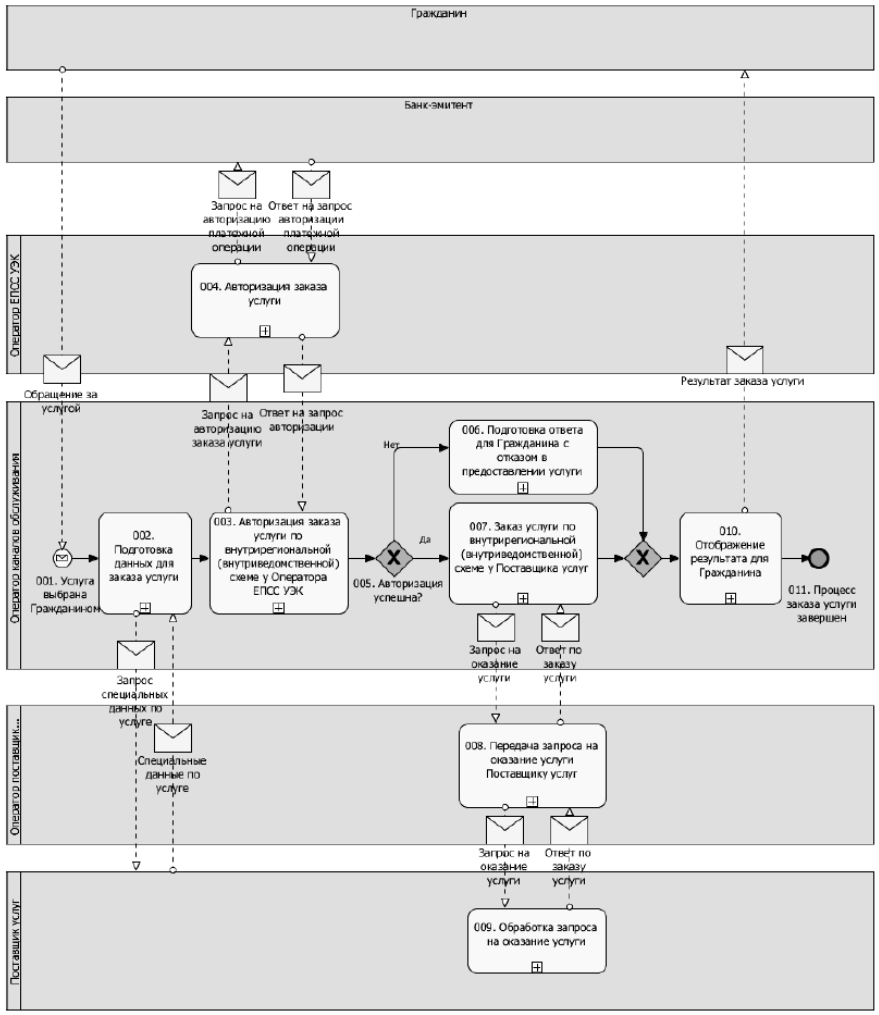

Рис. 18. **Взаимодействие участников**

Эксперты отмечают, что проектом УЭК не предусмотрено обязательного размещения на карте электронной цифровой подписи (ЭЦП), что безусловно окажет негативное влияние на реализацию программы доступа граждан к дистанционным госуслугам, реализуемым в рамках электронного правительства. Кроме того, карты УЭК невозможно будет использовать для электронного голосования.

Планируется, что первые универсальные карты начнут выдавать россиянам в 2012 г. (в пилотных регионах), с 2013 г. по всей России в заявительном порядке, а с 2014 г. в уведомительном. Планируется, что функции выдачи будут возложены на работодателей, учебные заведения, органы соцзащиты и, возможно, на банки. Обеспечить картами всех граждан России предполагается к 2017 г. Срок действия карты составит пять лет.

КОНТРОЛЬНЫЕ ВОПРОСЫ

Тест

ID-карта:

а) не требует для своего использования специального оборудования

б) используется на территории одного государства

в) хранит информацию о своем владельце

ID-карта:

а) не заменяет собственноручную подпись

б) не противоречит законодательству всех стран Евросоюза

в) не позволяет подписывать документы ЭЦП

Эстонская ID-карта не позволяет:

а) оплачивать покупки в магазинах

б) участвовать в парламентских выборах

в) оплачивать проезд

Универсальная электронная карта предназначена для :

а) электронной подписи документов

б) использования в качестве заграничного паспорта

в) упрощения бюрократических процедур

Универсальная электронная карта позволит :

а) заменить все идентификационные документы гражданина

б) использовать ее в качестве банковской карты

в) подписывать документы ЭЦП

К маю 2011 года уже официально утверждены:

а) технические требования к УЭК

б) законодательные акты, гарантирующие получение государственных услуг на основе УЭК

в) внешний вид УЭК

Заключение

Электронная подпись, сервисы PKI и универсальная электронная карта на современном технологическом этапе оправданно рассматриваются как эффективное решение для обеспечения пространства доверия в информационной среде при оказании электронных государственных услуг.

Перечень решений, обеспечивающих пространство доверия информационного общества, электронного государства, электронного правительства, которые могут быть реализованы только посредством комплексного применения сервисов на основе инфраструктуры открытых ключей, рассмотренных в учебном пособии, можно продолжить, однако представленного перечня достаточно для того, чтобы утверждать, что эти технологии занимают ключевое место среди элементов электронного правительства и информационного общества. Далее слово за специалистами, которые должны предложить эффективные способы развертывания данных технологических решений и за гражданами, которые будут готовы их использовать в повседневной жизни.

Глоссарий

Владелец сертификата ключа подписи (владелец СКП) - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Валидный СКП - сертификат, положительно прошедший все необходимые операции проверки валидности.

Доверенный удостоверяющий центр (ДУЦ) - удостоверяющий центр, аккредитованный в сети доверенных УЦ ФНС России.

Закрытый ключ ЭЦП - уникальная последовательность символов, известная владельцу СКП и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств ЭЦП.

Единое пространство доверия - структура, определяющая организационные границы, в пределах которых находятся только заслуживающие доверия удостоверяющие центры, а сертификаты ключей подписей, изготовленные ими, признаются всеми участниками информационного взаимодействия в границах структуры и на равных условиях.

Идентификация - действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Идентификатор пользователя - уникальный в рамках Удостоверяющего центра (УЦ) код пользователя (последовательность символов), позволяющий провести авторизацию пользователя. В УЦ идентификаторы пользователя генерируются на основе данных, взятых из заявления пользователя на регистрацию.

Информационная система должна рассматриваться как среда, обеспечивающая целенаправленную деятельность органов государственной власти. Т.е. она представляет собой совокупность таких компонентов как информация, регламенты, персонал, аппаратное и программное обеспечение, объединенных регулируемыми взаимоотношениями для формирования организации как единого целого и обеспечения её целенаправленной деятельности.

Информационная безопасность (безопасность информации) - состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного

уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п.

Информационно-коммуникационные технологии (ИКТ) – совокупность методов, производственных процессов и программно-технических средств, интегрированных с целью сбора, обработки, хранения, распространения, отображения и использования информации в интересах ее пользователей.

Информация – сведения об окружающем мире (объектах, явлениях, событиях, процессах, закономерностях…), которые уменьшают имеющуюся степень неопределенности, неполноты знаний, отчужденные от их создателя и ставшие сообщениями (выраженными на определенном языке в виде знаков, в том числе и записанными на материальном носителе), которые можно воспроизводить путем передачи устным, письменным или другим способом (с помощью условных сигналов, технических средств, и т.д.).

Информационный обмен - обмен сведениями о лицах, предметах, фактах, событиях и процессах, независимо от формы их представления.

Информационный ресурс Организатора сети ДУЦ ФНС России (ИРУЦ) - автоматизированная система, позволяющая проводить автоматическую регистрацию и актуализацию регистрационных данных (включая СКП) участников юридически значимого электронного документооборота.

Инфраструктура открытых ключей - PKI – Public Key Infrastructure –технология аутентификации с помощью открытых ключей.

Ключевой носитель - электронный носитель ключевой информации, содержащий один или несколько ключей.

Компрометация ключа - утрата доверия к тому, что используемые закрытые ключи недоступны посторонним лицам. К событиям, связанным с компрометацией ключей, относятся, в том числе, следующие:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение целостности печатей на сейфах с ключевыми носителями, если используется процедура опечатывания сейфов;
- утрата ключей от сейфов в момент нахождения в них ключевых носителей;
- утрата ключей от сейфов в момент нахождения в них ключевых носителей с последующим обнаружением;

- доступ посторонних лиц к ключевой информации.

Конфликтная ситуация - противоречивые позиции сторон по какому-либо поводу; стремление к противоположным целям или использование различных средств для их достижения; несовпадение интересов, желаний сторон. В ходе обмена ЮЗЭД возможно возникновение спорных ситуаций, связанных с реализацией прав пользователей СКП.

Конфиденциальная информация - любая информация, доступ к которой ограничен законодательством Российской Федерации, не содержащая сведений, составляющих государственную тайну.

Кросс-сертификат - СКП уполномоченного лица Доверенного УЦ, подписанный ЭЦП уполномоченного лица Организатора сети ДУЦ.

Объект доступа - единица ресурса автоматизированной информационной системы, доступ к которой регламентируется правилами разграничения **доступа.**

Организатор сети доверенных УЦ ФНС России (Организатор сети ДУЦ) - удостоверяющий центр, приказом ФНС России назначенный головным УЦ в сети доверенных удостоверяющих центров ФНС России.

Открытый ключ ЭЦП - уникальная последовательность символов, соответствующая закрытому ключу ЭЦП, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств ЭЦП подлинности ЭЦП в электронном документе.

Пользователь СКЗИ - физическое или юридическое лицо, обладающее правом пользования средством криптографической защиты информации. Право пользования подтверждается лицензией производителя СКЗИ, выданной пользователю.

Проверка валидности сертификата ключа подписи - это действия, производимые над проверяемым сертификатом ключа подписи для того, чтобы убедиться в возможности его использования, а именно:

- проверка целостности сертификата ключа подписи;

- проверка срока действия сертификата ключа подписи;

- проверка отсутствия сертификата ключа подписи в актуальном списке отозванных сертификатов ключей подписей;

- проверка области действия сертификата ключа подписи.

Сертификат ключа подписи (СКП) - (сертификат открытого ключа) - документ на бумажном носителе и электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной

цифровой подписи и идентификации владельца сертификата ключа подписи.

Система - система юридически значимого электронного документооборота Федеральной налоговой службы Российской Федерации (далее - ФНС России) при информационном взаимодействии с хозяйствующими субъектами.

Список отозванных сертификатов (СОС) - файл, подписанный УЦ, содержащий серийные номера СКП, прекративших свое действие (отозванных) раньше установленного срока, причину прекращения действия, информацию об УЦ, отозвавшем сертификаты, и другую служебную информацию.

Средства криптографической защиты информации (СКЗИ) - средства шифрования, средства имитозащиты, средства электронной цифровой подписи, средства кодирования, средства изготовления ключевых документов и ключевые документы (независимо от вида носителя ключевой информации).

Средства электронной цифровой подписи (средства ЭЦП) - аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи.

Удостоверяющий центр (УЦ) - организация (юридическое лицо), оказывающая услуги по управлению жизненным циклом СКП, в соответствии с законодательством Российской Федерации.

Уполномоченное лицо УЦ - сотрудник, назначенный приказом, либо распоряжением руководителя УЦ, на имя (псевдоним) которого выдан сертификат ключа подписи центра сертификации УЦ.

Электронная цифровая подпись (ЭЦП) - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электронное правительство — использование в практике органов государственной власти современных информационно-коммуникационных технологий (ИКТ) для осуществления всего спектра правительственных функций, нацеленное на обеспечение доступа граждан к достоверной официальной информации, на создание новых возможностей для

взаимодействия органов власти между собой, с населением, бизнесом и институтами гражданского общества, а также на повышение эффективности и прозрачности государственного управления.

Электронный документ (ЭД) - документ, в котором информация представлена в электронно-цифровой форме.

Юридически значимый электронный документ (ЮЗЭД) - электронный документ, подписанный ЭЦП уполномоченного лица Участника Системы.

Рекомендуемая литература и информационные материалы

Основная литература

1. Беззубцев О.А., Мартынов В.Н., Мартынов В.М. Некоторые вопросы правового обеспечения использования ЭЦП - http://www.cio-world.ru/offline/2002/6/21492/.
2. Борохович Л., Монастырская А., Трохова М. Ваша интеллектуальная собственность. СПб: Питер, 2007. С. 287.
3. Никитов В.А. и др. Информационное обеспечение государственного управления. М., 2008. С. 82-116.
4. Полянская О.Ю. , Горбатов В.С. Инфраструктуры открытых ключей, Бином, 2007, ISBN: 978-5-9556-0081-9
5. Семилетов С. И. Проблемы электронного документа (глава 4) // Информационное право: актуальные проблемы теории и практики. Коллективная монография./ под общ. ред. И.Л. Бачило – М. : Юрайт. 2009. – 530 с.
6. Ткачев А.В. Законодательное регулирование правового статуса ЭЦП. Основные положения - http://www.confident.ru/magazine/new/18.html.
7. Чубукова С.Г., Элькин В.Д. Основы правовой информатики (юридические и математические вопросы информатики). Учебное пособие / Под ред. М.М. Рассолова. М.: Контракт, 2007.
8. Электронный документ и документооборот: правовые аспекты: сб. научн. тр. / РАН. ИНИОН, ИГП. Сектор информационного права– М., 2003. – 208 с.

Дополнительная литература и ссылки на интернет-ресурсы

1. Кристальный Б.В., Якушев М.В. Концепция российского законодательства в области Интернета - http://www.vic.spb.ru/law/doc/a84.htm.
2. Фатьянов А.А. Правовое регулирование электронного документооборота : учеб.-практ. пособ. http://www.logistics.ru/9/4/6/i20_27304p0.htm
3. В тридевятом царстве, в электронном государстве. // Пресс-релиз «Фонда Общественное Мнение». 13 июля 2011 г. [Электронный ресурс]. Режим доступа: http://bd.fom.ru/report/cat/smi/smi_int/pressr_080711.
4. Задирако И.Н. Портал государственных услуг: личный опыт // Проект G2C «Содействие электронному правительству в Российской Федерации», финансируемый ЕС. Портал знаний ЭП. Июнь 2011 г. [Электронный ресурс]. Режим доступа: http://www.rusg2c.ru/system/files/Zadirako%20June%202011.pdf.
5. Проценко, Л. «Чиновник с айпадом»: Станет ли лучше жизнь москвичей в электронном городе? // «Российская газета». Столичный выпуск № 5538. 27 июля 2011 г. [Электронный ресурс]. Режим доступа: http://www.rg.ru/2011/07/27/infograd.html.
6. Трахтенберг, А.Д. Переход к электронному правительству: государственное предложение и общественный запрос (по материалам социологических исследований) // Материалы XIII Всероссийской конференции «Интернет и современное общество», Санкт-Петербург, 19 – 21 октября 2010 г.
7. Carter, L. The Utilization of E-Government Services: Citizen Trust, Innovation and Acceptance Factor / Carter L., Belanger F. // Information System Journal. 2005. V 1. P. 5 – 25.
8. Carter, L. E-government Adoption: A Cultural Comparison / Carter L., Weerakkody V. // Information Systems Frontiers. 2008. V. 10. P. 473-482.
9. Davis, F.D. Perceived Usefulness, Perceived Ease of Use, and User Accepatance of Information Technology // MIS Quarterly. 1989. V. 13. № 3. P. 319 – 339.
10. Gauld, D. Do They Want It? Do They Use It? The ‘Demand-Side’ of E-Government in Australia and New Zealand / Gauld D., Goldfinch Sh., Horsburgh S. // Government Information Quarterly. 2010. V. 27. P. 177 – 186.
11. Horst, M. Perceived Usefulness, Personal Experience, Risk Perception and Trust as Determinants of Adoption of E-Government Services in The Netherlands / Horst M., Kuttschreuter M., Gutteling J.M. // Computers in Human Behavior. 2007. V. 23. P. 1838 – 1852.

Нормативные правовые акты

1. Федеральный закон Российской Федерации от 25 июля 2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»» // http://www.rg.ru/2011/07/27/dannye-dok.html
2. Федеральный закон от 11 июля 2011 г. № 200-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «Об информации, информационных технологиях и о защите информации»» // http://www.rg.ru/2011/07/15/smi-dok.html
3. Федеральный закон Российской Федерации от 1 июля 2011 г. № 169-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // http://www.rg.ru/2011/07/02/uslugi-site-dok.html
4. Федеральный закон Российской Федерации от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // http://www.rg.ru/2011/04/08/podpis-dok.html
5. Федеральный закон Российской Федерации от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // http://www.rg.ru/2010/07/30/gosusl-dok.html
6. Федеральный закон Российской Федерации от 27 июля 2010 г. № 227-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием ФЗ «Об организации предоставления государственных и муниципальных услуг»» // http://www.rg.ru/2010/08/02/uslugi-dok.html
7. Постановление Правительства Российской Федерации от 28 декабря 2011 г. №1184 «О мерах по обеспечению перехода федеральных органов исполнительной власти и органов государственных внебюджетных фондов на межведомственное информационное взаимодействие в электронном виде»
8. Правила представления в регистрирующий орган иными государственными органами сведений в электронной форме, необходимых для осуществления государственной регистрации юридических лиц и индивидуальных предпринимателей, а также для ведения единых государственных реестров юридических лиц и индивидуальных предпринимателей. Утверждены Постановлением Правительства РФ от 22 декабря 2011 года № 1092
9. Распоряжение Правительства Российской Федерации от 2 декабря 2011 г. №2161-р «О внесении изменений в государственную программу Российской Федерации "Информационное общество (2011 - 2020 годы)»

10. Постановление Правительства Российской Федерации от 28 ноября 2011 г. № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»»
11. Приказ Федеральной налоговой службы от 7 ноября 2011 г. № ММВ-7-6/735 «Об утверждении Порядка представления заявлений, уведомлений и запросов в налоговые органы в электронном виде для целей учета в налоговых органах организаций и физических лиц»
12. Постановление Правительства Российской Федерации от 24 октября 2011 г. № 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)» // http://government.ru/gov/results/16910/
13. Постановление Правительства Российской Федерации от 24 октября 2011 г. № 860 «Об утверждении Правил взимания платы за предоставление информации о деятельности государственных органов и органов местного самоуправления» // http://government.ru/gov/results/16909/
14. Постановление Правительства Российской Федерации от 8 сентября 2011 г. №759 «О внесении изменений в Постановление Правительства Российской Федерации от 25 декабря 2009 г. № 1088» // http://government.consultant.ru/page.aspx?1572112
15. Постановление Правительства Российской Федерации от 7 сентября 2011 г. №751 «О внесении изменений в Правила делопроизводства в федеральных органах исполнительной власти» // http://government.ru/gov/results/16456/
16. Приказ Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) от 2 сентября 2011 г. № 221 «Об утверждении Требований к информационным системам электронного документооборота федеральных органов исполнительной власти, учитывающих, в том числе, необходимость обработки посредством данных систем служебной информации ограниченного распространения»
17. Постановление Правительства Российской Федерации от 19 августа 2011 г. № 705 «О внесении изменений в некоторые акты правительства Российской Федерации в связи с необходимостью перехода на межведомственное электронное взаимодействие» // http://government.consultant.ru/page.aspx?1570542

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена Программа развития государственного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет информационных технологий, механики и оптики» на 2009–2018 годы.

КАФЕДРА УПРАВЛЕНИЯ ГОСУДАРСТВЕННЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

Кафедра УГИС создана в 2011 году на Магистерском корпоративном факультете НИУ ИТМО.

Обучение на магистерской программе «Управление государственными информационными системами» направлено на приобретение теоретических знаний и практических навыков в сфере создания и развития ИТ-систем для нужд государственной власти и местного самоуправления.

Практическая часть обучения проходит на базе Центра технологий электронного правительства НИУ ИТМО, Санкт-Петербургского информационно-аналитического центра и других партнерских структур под руководством опытных экспертов и представителей органов власти.

Дмитрий Родиславович Трутнев

ИНФРАСТРУКТУРА ДОВЕРИЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Учебное пособие

В авторской редакции
Дизайн обложки С.Н. Ушаков
Верстка Ю.В. Байкеева
Редакционно-издательский отдел Санкт-Петербургского государственного университета информационных технологий, механики и оптики
Зав. РИО Н.Ф. Гусарова
Лицензия ИД № 00408 от 05.11.99
Подписано к печати
Заказ №
Тираж 100 экз.
Отпечатано на ризографе