УДК 004.089

Анализ зарубежной нормативной базы по идентификации и аутентификации

© А.С. Кузьмин, А.Г. Сабанов

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Приводится обзор некоторых наиболее известных работ по регулированию процессов идентификации и аутентификации пользователей систем государственных услуг, электронной коммерции и информационных систем государственных органов. Анализ рассмотренных работ показывает необходимость создания отечественной нормативной базы по вопросам идентификации и аутентификации. При разработке регулирующих документов необходимо учитывать мировой опыт. В частности, требуется нормативное введение уровней гарантий аутентификации в зависимости от результатов оценки рисков для тех или иных государственных систем. При этом необходимо учитывать технологии аутентификации, используемые или планируемые к применению в указанных информационных системах.

Ключевые слова: *идентификация, аутентификация, зарубежная нормативная база.*

Введение. Вопросам регулирования процессов идентификации и аутентификации (ИА) на Западе уделяется достаточно много внимания. В ряде развитых капиталистических стран нетрудно заметить связь темпов развития электронной коммерции и проектов по построению электронного правительства с количественным ростом нормативной базы, которая может как ускорять, так и замедлять процессы построения систем удаленного электронного взаимодействия (УЭВ) государства, бизнеса и граждан.

Актуальность анализа зарубежной нормативной базы по вопросам организации систем автоматической ИА участников УЭВ продиктована тем, что в отличие от западных стран в российской нормативной базе можно найти только один документ [1], целиком посвященный данной тематике. В большей части отечественных законов, стандартов и руководящих документов встречается лишь упоминание (или, как правило, один-два небольших абзаца) о таких сложных процессах, как ИА. В то же время в Российской Федерации идет интенсивное строительство систем электронной коммерции и оказания государственных услуг в электронной форме. Государственные информационные системы (ГИС) по требованию времени начинают обрастать системами Web-доступа, имеется насущная необходимость защищенного обмена информацией между информационными системами (ИС), все чаще требуется организация удаленного доступа к

ГИС, содержащим кроме открытой информации различные категории информации ограниченного доступа. Достаточно интенсивно начинает использоваться электронная подпись, применение которой невозможно без сервисов ИА. В этих условиях для разработки весьма актуальной отечественной нормативной базы по ИА необходимо учитывать мировой опыт.

Обзоры нормативной базы, тем более зарубежной, выполняются достаточно редко и, как правило, не являются общедоступными. Заметим, что сделать обзор работ по аутентификации — задача непростая в силу сложности этого явления и обилия вариантов реализаций систем ИА. Эту работу невозможно выполнить, не имея многолетнего опыта и не обладая знаниями в области криптографии и информационных технологий. Как правило, в опубликованных обзорах проблемы аутентификации освещены односторонне. Одной из известных попыток сделать системный обзор является работа [2]. К числу ее достоинств можно отнести обширный список литературы, простую манеру изложения и обилие примечаний. Существенными недостатками данной работы являются уникальная (не общепринятая) классификация механизмов аутентификации и явный перекос в сторону повышенного внимания к парольной аутентификации.

Наиболее полный обзор основных протоколов аутентификации представлен в классическом труде по криптографии [3]. Данная работа содержит список литературы из 1653 позиций, в ней рассмотрены основные протоколы аутентификации, возможные атаки и методы их парирования. Показано, что к середине 1990-х годов разработка теории ИА и основных протоколов аутентификации была закончена. К сожалению, в этой части изложение носит скорее исторический и всеобъемлющий по широте, чем системный, характер. К существенному недостатку работы относится отсутствие сравнения протоколов по обоснованным критериям, что, на наш взгляд, необходимо для практического проектирования и построения систем аутентификации, но является отдельной научной задачей. Заметим, что в обеих рассмотренных монографиях требования к аутентификации отсутствуют, изложены лишь определения, общие подходы, протоколы и способы построения систем аутентификации.

Данная статья посвящена обзору наиболее известных стандартов, требований и рекомендаций по ИА, находящихся в открытых источниках. Для удобства восприятия расположим рассматриваемые документы в порядке их опубликования.

Обзор зарубежной нормативной базы. Одним из первых наиболее полных стандартов по аутентификации является разработанный в 1993 г. стандарт [4], состоящий из трех частей (общий подход, использование симметричной и асимметричной криптографии). Для

данного обзора наиболее интересна третья часть указанного стандарта, пересмотренного в 1997–1998 гг. Стандарт [4] посвящен аутентификации субъектов с использованием алгоритма с открытым ключом. В стандарте определены пять различных протоколов для односторонней и двусторонней аутентификации. В документе приводится одно из первых определений понятия строгой аутентификации. Стандарт был введен в действие 15 ноября 1993 г., заменен 15 октября 1998 г. на [4].

В том же 1993 г. стандарт [5] «Аутентификация субъекта на основе криптографии с открытым ключом» был разработан NIST (американским Национальным институтом стандартов и технологий), но опубликован был четыре года спустя, 18 февраля 1997 г. Данный стандарт определяет два протокола аутентификации субъектов в компьютерной системе на основе запроса и отзыва — один для односторонней, другой для двусторонней аутентификации. Этот стандарт рекомендуется применять во всех федеральных ведомствах, использующих системы аутентификации на основе открытых ключей, для защиты несекретной информации в компьютерных системах и цифровых системах электросвязи, не подпадающих под действие секции 2315 раздела 10 или секции 3502(2) раздела 44 Кодекса США. Данный стандарт могут использовать и негосударственные организации. Остановимся на некоторых положениях этого документа подробнее.

Аутентификация на основе криптографии с открытым ключом может успешно использоваться во многих приложениях, в частности, в случаях, когда стороны аутентификации не имеют предварительных сведений о существовании друг друга. Протоколы аутентификации, приведенные в настоящем стандарте, можно использовать совместно с другими системами на основе открытого ключа, а также в прикладном и встроенном программном обеспечении, в аппаратном обеспечении и в любой их комбинации.

В стандарте определены два протокола аутентификации субъектов, использующих алгоритмы криптографических преобразований с открытым ключом для формирования и проверки электронной подписи. Один субъект может подтвердить другому субъекту свою подлинность, подписав случайный запрос. Это обеспечивает строгость аутентификации без необходимости иметь общий секрет. Если настоящий стандарт внедряется в федеральных правительственных компьютерных системах, генерация и проверка электронных подписей должны выполняться согласно требованиям FIPS (в частности, FIPS PUB 186 «Стандарт цифровой подписи»).

Вместе с тем некоторые положения настоящего стандарта сформулированы не так строго, как аналогичные положения [4], что позволяет разработчикам вводить оригинальные поля некоторых аутен-

тификаторов, а также оставляет возможность для соответствия настоящему стандарту некоторых протоколов аутентификации с открытым ключом, не подпадающих под [4]. В разделе 2 приводится обзор определенных рассматриваемым стандартом протоколов, а также критерии соответствия стандарту, краткое описание угроз, которым противостоят протоколы аутентификации, и список определений и обозначений. Протоколы аутентификации описаны в разделе 3. В приложениях к [4] приведены необязательные методы форматирования и кодирования аутентификационной информации.

В протоколах аутентификации субъектов, изложенных в рассматриваемом стандарте, для генерации аутентификаторов применяются алгоритмы электронной подписи. Протоколы аутентификации не зависят от природы субъекта (например, один и тот же протокол используется для взаимной аутентификации двух людей, человека и процесса, двух процессов). Аутентификация пользователя обычно разбивается на две стадии: на первой человек проходит аутентификацию по отношению к криптографическому модулю, а на второй криптографический модуль выполняет формирование и(или) проверку электронной подписи от имени пользователя.

Аутентификация субъекта зависит от успешности выполнения двух действий: 1) проверки принадлежности ему ключевой пары; 2) проверки подписи под отзывом. В процессе аутентификации проверяющая сторона генерирует случайное число — запрос, связывает его с идентификатором проверяемой стороны. Затем проверяемая сторона формирует электронную подпись отзыва. Проверяющая сторона находит открытый ключ проверяемой по идентификатору последней. В случае успешной проверки подписи с помощью найденного открытого ключа аутентификация считается пройденной.

Данный стандарт не предусматривает использования ни сертификатов открытого ключа, ни инфраструктуры открытых ключей. Он не требует ни синхронизации часов, ни использования штампов времени. Рассматриваемый стандарт не предъявляет требований к именованию субъектов. Он требует лишь уникальности их идентификаторов.

Одним из коротких, но интересных документов, основанных на принятом UNCITRAL в 1996 г. модельном законе развития электронной коммерции в мире, является Министерская декларация для электронной коммерции [6], в которой достаточно много внимания уделено вопросам аутентификации. В этом документе признается необходимость развития электронной аутентификации внутри стран недискриминационными методами в целях интероперабельности и развития международной электронной коммерции.

В августе 2001 г. были опубликованы рекомендации [7], в которых определяется механизм аутентификации SASL (Simple Authenti-

cation and Security Layer — простой уровень аутентификации и безопасности), основанный на стандартах аутентификации субъекта [4, 5]. Рекомендации [7] являются доработкой подготовленных в 1997 г. компанией Netscape рекомендаций RFC 2222. Механизм, описанный в [7], обеспечивает аутентификацию субъекта с использованием сертификатов формата X.509, но не обеспечивает целостность и конфиденциальность пользовательских данных. Он может применяться в тех случаях, когда целостность и конфиденциальность обеспечиваются на уровне приложения.

В асимметричных схемах (схемах с открытым ключом) аутентифицируемый субъект снабжается закрытым ключом, и затем он может проходить аутентификацию по отношению к любому серверу, поскольку его открытый ключ доступен во всей системе. Симметричные механизмы аутентификации (такие парольные механизмы, как CRAM-MD5, содержащийся в RFC 2195) не имеют такого преимущества, поскольку их использование требует предварительного распространения общего секрета между сторонами аутентификации. По сравнению с TLS описываемый механизм обладает следующими преимуществами:

• простота. Если требуются только функции, обеспечиваемые SASL (а не все функции, обеспечиваемые TLS), то SASL предпочтительнее, поскольку он проще;

• поддержка уровней. Механизм SASL характеризуется лучшей совместимостью с большинством протоколов, чем TLS;

• наличие прокси-серверов. В некоторых архитектурах TLS-сеансы не связывают конечные точки приложений. В таких ситуациях для обеспечения сквозной аутентификации может использоваться SASL;

• повышение уровня аутентификации. В некоторых приложениях при инициировании TLS-сеанса может быть еще неизвестен требуемый уровень аутентификации (анонимность, аутентификация сервера, взаимная аутентификация). Механизм SASL позволяет со временем повышать уровень аутентификации.

Механизм SASL предусматривает два режима аутентификации. Односторонняя аутентификация клиента: клиент формирует электронную подпись запроса от сервера и тем самым подтверждает серверу свою подлинность. Взаимная аутентификация: клиент формирует электронную подпись запроса от сервера и сервер формирует электронную подпись отзыва от клиента. Таким образом, и клиент, и сервер подтверждают друг другу свою подлинность.

В декабре 2001 г. был опубликован специальный выпуск NIST [8]. Этот документ является одним из немногих системных исследований компьютерной безопасности, основанных на рассмотрении главных сервисов безопасности (конфиденциальности, целостности,

доступности и мониторинга действий пользователей) с учетом рисков, относящихся к ИТ. Главным достижением этой работы является обоснование необходимости введения гарантий аутентификации для обеспечения конфиденциальности, целостности и доступности информации. Гарантии (достоверность) аутентификации — это характеристика системы, дающая уверенность в том, что система выполняет свою функцию. Гарантии, по данным работы [8], обеспечиваются:

• упрощением технических решений;

• использованием доверенного программного обеспечения;

• архитектурой, нацеленной на минимизацию вреда от вторжений либо за счет уменьшения уязвимостей, либо за счет функций обнаружения и восстановления;

• не техническими (например, организационными) мерами.

Конечно, этот подход далек от совершенства (как будет показано далее, в последующих нормативных документах было существенно доработано не только само понятие гарантий, но и пути их обеспечения), однако данное исследование было в некотором смысле пионерским и сыграло роль основы для современных требований к аутентификации. Например, впервые были введены понятия логического и физического доменов безопасности. Вторым ярким примером может служить подход к снижению рисков. Так, согласно [8], уменьшение рисков, связанных с атаками, достигается следующими техническими средствами:

• при наличии дыр — внедрение методов подстраховки;

• при наличии дыр, которые могут быть использованы, — многоуровневая защита и архитектурные решения;

• когда расходы злоумышленника оказываются меньше его выгоды от реализации атаки — использование средств защиты, повышающих стоимость атаки (например, нетехнические меры, такие как ограничение обрабатываемой информации, могут снизить выгоду злоумышленника);

• когда ущерб от реализации атаки слишком велик — применение архитектуры и принятие технических мер, ограничивающих масштабы атаки, а следовательно, и ущерб.

Исследование [8] легло в основу ряда документов, и по сей день имеющих важное значение для США и ряда других стран.

Параллельно с американским институтом NIST интенсивные работы по выпуску нормативных документов проводились в Европе. Представляет интерес группа документов CWA, опубликованных в период с 2001 по 2004 г. Аббревиатура CWA (CEN Workshop Agreement) означает документ под названием «Соглашение рабочей группы европейского комитета по стандартизации CEN (the European Committee for Standardization)».

Группа документов CWA сыграла большую роль в применении средств ИА при использовании электронной подписи в странах Евросоюза. В частности, несколько документов CWA посвящено SSCD (Secure Signature-Creation Devices) — устройствам, способным генерировать ключевые пары внутри устройства.

Приведем список из восьми документов серии CWA, связанных с регулированием ИА в части применения электронных подписей в Европе:

• CWA 14167-1/4 «Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures»;

• CWA 14168 «Secure Signature-Creation Devices "EAL 4+"»;

• CWA 14169 «Secure Signature-Creation Devices "EAL 4+"»;

• CWA 14170 «Security Requirements for Signature Creation Applications»;

• CWA 14172-1/8 «EESSI Conformity Assessment Guidance»;

• CWA 14355 «Guidelines for the implementation of Secure Signature-Creation Devices»;

• CWA 14365-1/2 «Guide of use of Electronic Signature»;

• CWA 14890-1/2 «Application Interface for smart cards used as Secure Signature-Creation Devices».

На основе стандарта [5] в 2003 г. административно-бюджетное управление (АБУ) при Президенте США разработало руководство по применению средств аутентификации для доступа к государственным системам [9], которое было закреплено Директивой 12 [10], подписанной Президентом в 2003 г. В Директиве было впервые введено понятие гарантий аутентификации для транзакций электронного правительства. При этом гарантии аутентификации были разделены на четыре уровня:

1) отсутствие требований конфиденциальности идентификационных данных;

2) некоторый уровень требований конфиденциальности идентификационных данных;

3) высокий уровень требований конфиденциальности идентификационных данных;

4) очень высокий уровень требований конфиденциальности идентификационных данных.

Директива инициировала ряд важнейших документов, нормирующих процессы аутентификации не только в Америке, но и в ряде других стран. Директива Президента США сыграла огромную роль в становлении требований безопасности и стандартов идентификации и аутентификации в США, Канаде, Австралии и других странах. До сих пор на официальном сайте Правительства США находится указанная директива для всех федеральных агентств, а

также разработанные в соответствии с ней нормативные документы, отчеты правительства и другие документы по контролю процессов ее выполнения.

Анализ, проведенный в работе [9], был дополнен исследованиями европейских специалистов в области стандартизации телекоммуникаций Международного союза электросвязи [11]. В данной работе последовательно изложены основные угрозы аутентификации, уязвимости, виды аутентификации, роль доверенной третьей стороны. В рассмотрении аутентификации сделан уклон на сетевую безопасность. Особое внимание уделено безопасности аутентификации как процесса. В частности, введены следующие классы защиты способов аутентификации по отношению к аутентифицирующей (подтверждающей подлинность предъявленного идентификатора) информации. Нулевой класс является незащищенным. Первый класс защищен от вскрытия, второй — от вскрытия и повторной передачи, третий — от вскрытия и повторной передачи со стороны одного и того же проверяющего объекта. Четвертый класс отличается от третьего тем, что проверяющие объекты могут быть различными. Впервые в международном стандарте введено понятие сертификата формата X.509, выпущенного удостоверяющим центром для аутентификации. Ценность рассматриваемого стандарта заключается в системном рассмотрении защит от атак на процесс аутентификации. Этот стандарт необходимо рассматривать как один из источников при построении систем оценки рисков ИА.

В 2006 г. в США был выпущен стандарт [12], подготовленный NIST во исполнение Директивы 12 [10]. В отличие от предыдущих руководящих документов вместо ИА в этом стандарте впервые вводится понятие PIV (Personal Identity Verification — проверка персональной идентификации). К этому времени нормативная база США достаточно развита (в частности, системы ИА уже строятся в соответствии с [5, 7–10]), а для выполнения основных положений [10] осталось не так много — достроить систему гарантий ИА. Для этого сначала физический и логический доступ разделяются по разным контурам, причем контур управления физическим доступом интегрируется со СКУД — системой контроля и управления доступом. Для управления логическим доступом вводятся разработанные в [8] четыре уровня доверия (гарантий) аутентификации. После оценки рисков и определения требуемого уровня строгости аутентификации государственные агентства и ведомства, согласно [12], могут выбирать технологию, которая обеспечивает выполнение для данного уровня строгости аутентификации хотя бы минимальных технических требований:

• к аутентификаторам (токенам);

• к процедуре подтверждения подлинности и регистрации электронных удостоверений, привязывающих пользователя к аутентификатору;

• к механизмам удаленной аутентификации, представляющим собой комбинацию электронных удостоверений, аутентификаторов и протоколов аутентификации;

• к механизмам подтверждения, используемым для передачи результатов удаленной аутентификации другим сторонам.

Особое место в рассматриваемых документах занимает руководство [13], также разработанное согласно Директиве 12 [10] и дополняющее основные теоретические положения стандарта [12]. В преамбуле данного руководства сказано, что рекомендации соответствуют требованиям циркуляра [9]. Они являются дополнением к рекомендациям АБУ по электронной аутентификации для федеральных ведомств, в которых заданы четыре уровня аутентификации в зависимости от последствий ошибок аутентификации и ненадлежащего использования электронных удостоверений. Далее приводится краткое содержание требований к каждому из четырех уровней, подробно рассмотренных в работе [14].

Заметим, что через 5 лет после выхода первой версии FIPS PUB 201-1 [12] был разработан и опубликован усовершенствованный стандарт под тем же названием [15]. В версии 201-2 учтены отзывы и правки, поступившие от ведомств за 5 лет. Приведем некоторые отличия [15] от [12]. Введено понятие «цепочки доверия», поддерживаемой издателем смарт-карты — удостоверения. «Цепочка доверия» позволяет владельцу карты после прохождения биометрической аутентификации получить новую карту взамен скомпрометированной, потерянной, украденной или поврежденной. Максимальный срок действия смарт-карты увеличен с 5 до 6 лет. Аутентификация с помощью карты на основе асимметричных алгоритмов сделана обязательной, а на основе симметричных алгоритмов — необязательной. Добавлено необязательное сравнение биометрических параметров на карте как средство активации карты и механизм аутентификации.

Краткий анализ зарубежной нормативной базы. Наиболее многочисленные и проработанные с научной точки зрения нормативные документы по регламентации средств и методов аутентификации были созданы в США. На наш взгляд, этому в немалой степени способствовало то, что на проведение таких объемных работ существовал бизнес-заказчик в лице АБУ при Президенте США. В 2003 г. АБУ, проанализировав информацию, обрабатываемую и хранимую в своих ИС, решило упорядочить доступ к открытой информации и информации ограниченного доступа. Известно, что аутентификация является одним из важнейших инструментов организации доступа

при электронном взаимодействии. Поэтому, с одной стороны, при разделении механизмов аутентификации на уровни гарантий АБУ стремилось обеспечить конфиденциальность, доступность и целостность этой информации. С другой стороны, на государство при этом возлагалась функция обеспечения этих гарантий путем инспектирования используемых средств ИА. Такой подход стал возможен при наличии развитой теории ИА и проверенных протоколов аутентификации, рассмотренных в [3].

Инициатива АБУ закреплена в Директиве 12 Президента [10]. На ее основе были начаты научно-исследовательские работы, примерами которых являются [8, 14]. Это позволило в короткие сроки создать достаточно полную, действующую до сих пор и постоянно совершенствующуюся базу руководящих документов по ИА.

Действующую в США государственную систему идентификации, электронных удостоверений (ЭУ) и контроля доступа ICAM (Identity, Credential, and Access Management) трудно сравнивать с российской. В США уже более 8 лет действуют обязательные к выполнению стандарты FIPS, развита система регистрации, оформления и проверки ЭУ и т. п.

Документы, лежащие в основе системы ICAM, легко можно найти на сайте правительства США. Главными из них являются [8, 10, 13, 15]. Заметим, что переносить американский опыт на российскую почву и пользоваться опубликованными на этом же сайте документами надо весьма осторожно, с научным обоснованием, доработками и разумными ограничениями.

Кратко рассмотрим некоторые нормативные документы по ИА в других странах.

В 2009 г. в Австралии было опубликовано «Национальное руководство по электронной аутентификации [16]. В основу этого документа положены разработки [8, 12, 13]. В отличие от США введены пять уровней угроз и соответствующих им уровней доверия аутентификации. Подчеркивается значение стойкости к атакам процесса регистрации пользователей открытых ИС по доступу к государственным услугам.

Из множества документов АТЭС можно выделить для внимательного рассмотрения вышедшие в 2002 г. рекомендации «Электронная аутентификация» и более позднюю работу [17]. Заметим, что документы АТЭС — это только рекомендации правительствам. В них подчеркивается необходимость развивать систему ИА для электронной коммерции на основе криптографии с открытыми ключами. В мягких формах декларируются «правильные» американские подходы, интероперабельность, применение к национальным системам ИА недискриминационных методов.

В Канаде действует национальная система ИА, базирующаяся на принципах [18]. В Европейских странах наиболее часто применяется упрощенный трехуровневый подход к оценке рисков (низкий, средний и высокий риск) и соответственно три уровня гарантий аутентификации. Этот подход наиболее полно изложен в [18].

Заключение. Выполнен обзор некоторых наиболее известных работ по регулированию процессов идентификации и аутентификации пользователей систем государственных услуг, электронной коммерции и информационных систем государственных органов. Анализ зарубежного опыта показывает, что первые требования к аутентификации разработаны в США. Канада, Австралия и ряд других стран повторяют подходы и лишь локализуют американские требования, которые являются наиболее проработанными. Также анализ рассмотренных работ показывает необходимость создания отечественной нормативной базы по вопросам идентификации и аутентификации. При разработке регулирующих документов необходимо учитывать мировой опыт. В частности, требуется нормативное введение уровней гарантий аутентификации в зависимости от результатов оценки рисков для тех или иных государственных систем. При этом следует учитывать технологии аутентификации, используемые или планируемые к применению в указанных информационных системах.

Необходимость нормативного 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 указанной Концепции отмечается, что информационное взаимодействие государственных органов между собой, с организациями и гражданами осуществляется с помощью использования современных средств идентификации и электронной цифровой подписи. В результате такого взаимодействия можно однозначно определить (идентифицировать) участников информационного взаимодействия, правомочность должностных лиц органов государственной власти, осуществляющих информационное взаимодействие, дату и время его осуществления, а также гарантировать идентичность информации, отправленной одним участником и полученной другим участником информационного взаимодействия. В рамках формирования электронного правительства необходимо использовать различные механизмы ИА в соответствии с целями и задачами идентификации и аутентификации.

На основе представленного анализа можно сделать вывод о том, что российская нормативная база по ИА существенно отстает от руководящих документов развитых стран. Следовательно, необходимо интенсивно поработать, чтобы сократить указанное отставание.

ЛИТЕРАТУРА

[1] Постановление Правительства РФ 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”». *Российская газета*, 2011, 6 декабря.

[2] Смит Р.Э. *Аутентификация: от паролей до открытых ключей*. Москва, Вильямс, 2002, 432 с.

[3] Шнайер Б. *Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си*. Москва, Триумф, 2003, 816 с.

[4] *ISO/IEC 9798-3. Information technology — Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques*, 1997. URL: http://webstore.eic.ch/preview/info_isoiec9798-3%7Bed2.0%7Den.pdf (дата обращения 01.11.2013).

[5] *FIPS 196. Entity authentication using public key cryptography.* N.I.S.T., National Technical Information Service, Springfield, Virginia, 1997. URL: http://csrc.nist.gov/publications/fips/fips196/fips196.pdf (дата обращения 01.11.2013).

[6] *Ministerial Declaration on Authentication for Electronic Commerce,* 7–9 October 1998. URL: http://www.oecd.org/internet/ieconomy/35842032.pdf (дата обращения 01.11.2013).

[7] Zuccherato R. Nystrom M. *ISO/IEC 9798-3. Authentication SASL Mechanism. RFC 3163,* August 2001. URL: http://www.rfc-editor.org/rfc/rfc3163.txt (дата обращения 01.11.2013).

[8] Stoneburger G. Unerlying Technical Models for Information Technology Security. *NIST SP-800-33*, 2001. URL: http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf (дата обращения 01.11.2013).

[9] *OMB Memorandum M-04-04 E-Authentication Guidance for Federal Agencies.* December 16, 2003 & OMB Circular A-130 2003. URL: http://csrc.nist.gov/drivers/documents/m04-04.pdf (дата обращения 01.11.2013).

[10] *Homeland Security Presidential Directive 12 (HSPD-12). Policy for a Common Identification Standard for Federal Employees and Contractors*, 2004. URL: http://www.dhs.gov/homeland-security-presidential-directive-12 (дата обращения 01.11.2013). URL: http://www.idmanagement.gov/hspd-12-purchasing (дата обращения 19.06.2013).

[11] *ISO/IEC 10181-1/2, ITU-T Rec/x.810 &811. Information technology — Open Systems Interconnection — Security frameworks for open systems — Part 2: Authentication framework,* 2004. URL: http://www.itu.int/rec/T-REC/en (дата обращения 01.11.2013).

[12] *FIPS PUB 201-1. Personal Identity Verification (PIV) of Federal Employees and Contractors,* March 2006. URL: http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1chng1.pdf (дата обращения 01.11.2013).

[13] *NIST SP 800-63. Electronic Authentication Guideline*, 2006. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublicaions/NIST.SP.800-63-2.pdf (дата обращения 01.11.2013).

[14] Сабанов А.Г. Об уровнях строгости аутентификации. *Докл. Томского гос. ун-та систем управления и радиоэлектроники*, 2012, № 2 (26), с. 134–139.

[15] *FIPS PUB 201-2. Personal Identity Verification (PIV) of Federal Employees and Contractors,* March 2011. URL: http://csrc.nist.gov/publications/drafts/fips201-2/Draft_NIST-FIPS-20102.pdf (дата обращения 01.11.2013).

[16] *National e-Authentication Framework*, January 2009. URL: http://agimo.gov.au/files/2012/04/NeAFFramework.pdf (дата обращения 19.06.2013).

[17] *APEC. Guiding Principles for PKI-Based Approaches to Electronic Authentication. Ministerial Statements*. Lima, Peru, 2005. URL: http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2005_tel/annex_d.aspx (дата обращения 19.06.2013).

[18] *OECD Recommendation on Electronic Authentication,* 2007. URL: http://www.oecd.org/dataoecd/32/45/38921342.pdf (дата обращения 23.05.2013).

Статья поступила в редакцию 28.06.2013

Ссылку на эту статью просим оформлять следующим образом:
Кузьмин А.С., Сабанов А.Г. Анализ зарубежной нормативной базы по идентификации и аутентификации. *Инженерный журнал: наука и инновации,* 2013, вып. 11. URL: http://engjournal.ru/catalog/it/security/1021.html

Кузьмин Алексей Сергеевич — д-р физ.-мат. наук, профессор МГТУ им. Н.Э. Баумана, действительный член академии криптографии РФ. Автор более 100 работ в области проблем прикладной математики. e-mail: Kzmn@mail.ru

Сабанов Алексей Геннадьевич — канд. техн. наук, доцент МГТУ им. Н.Э. Баумана. Автор более 20 работ в области проблем идентификации и аутентификации. e-mail: Asabanov@mail.ru