УДК 004.089

А.Г. Сабанов

Об уровнях строгости аутентификации

Рассмотрены зарубежные подходы к построению уровней строгости аутентификации. Предложен способ формирования уровней строгости аутентификации.
Ключевые слова: удаленная аутентификация, идентификация, электронная подпись.

В связи с выходом Постановления Правительства РФ от 28 ноября 2011 г. № 977 [1], которое предписывает в весьма сжатые сроки (до 15 апреля 2012 г.) ввести в эксплуатацию единую систему идентификации и аутентификации (ЕСИА), актуальным становится вопрос о том, какие базовые принципы защиты будут заложены в основу создания национальной универсальной платформы защищенного доступа к различным информационным системам (ИС), используемым для предоставления государственных услуг. Создание систем управления удаленным доступом к информации, содержащей конфиденциальные данные, является одной из самых сложных задач даже в масштабе одного отдельно взятого предприятия, для ее решения в масштабах страны требуется разработка нестандартного подхода. Проблема осложняется тем, что речь идет об управлении доступом корпоративных пользователей и физических лиц к сервисам в публичном облаке. Фактически это означает, что необходимо в кратчайшие сроки решить задачу предоставления транссистемного доступа к облачным сервисам. Решение такой задачи возможно только при введении определенных требований к построению системы управления доступом на основе облачной инфраструктуры, построенной на базе инфраструктуры открытых ключей. Корректность решения задач идентификации и аутентификации (ИА) и создание пространства доверия в таких системах начинает играть ключевую роль.

Исходя из анализа зарубежного опыта создания подобных систем, одним из ключевых принципов является введение требований выполнения определенных уровней доверия (в данном случае это совпадает с требованиями к строгости) аутентификации для различных групп пользователей и уровней доверия (в данном случае и защищенности) информационных систем (ИС), к которым соответствующие группы пользователей имеют права доступа. Фактически речь идет об уровнях доверия или уровнях гарантий (level of assurance), которые будут рассмотрены в данной статье. Введение уровней строгости аутентификации лежит в основе самого распространенного в странах Европы и США метода решения технически сложной задачи электронной аутентификации удалённых пользователей по сети в государственных информационных системах (ГИС).

В отличие от развитых западных стран, имеющих достаточно долгую историю решения данных вопросов и развитую нормативную базу [2–10], в России вопросам стандартизации процессов ИА не уделялось должного внимания. В российской нормативной базе отсутствуют какие-либо технические требования и даже рекомендации к построению уровней строгости аутентификации.

В данной статье рассматриваются подходы к решению данной задачи, принятые в США и Европе. На основе анализа и обобщения зарубежного опыта [4–10] предложен способ построения уровней строгости аутентификации.

С выработкой единого подхода к решению такой сложной задачи определения уровней, правил и технических требований к аутентификации для разных условий к ресурсам ограниченного доступа сталкиваются все страны, строящие информационное общество и использующие облачные вычисления. Сначала рассмотрим опыт одной из самых первых стран, начавшей строительство E-Government и E-Commerce.

Обзор уровней требования к аутентификации, разработанных за рубежом. История развития рекомендаций, технических требований и стандартов на разделение по уровням строгости аутентификации насчитывает в США почти десятилетие [4]. Первым документом, основывающимся на принятом UNCITRAL модельном законе развития электронной коммерции в мире, принятым в 1996 г. в Оттаве, является Директива административно-бюджетного управления Администрации Президента [5]. В Директиве на основе определения степени конфиденциальности процесса проверки идентификации личности гражданина и степени конфиденциальности, с которой гражданин

должен использовать и хранить изданное для него электронное удостоверение личности, было впервые введено понятие гарантий аутентификации для транзакций электронного правительства. При этом гарантии аутентификации были разделены на 4 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.

Указанные требования были проведены на основе анализа рисков ошибок аутентификации и возможных атак. Этот анализ был дополнен и более тщательно исследован в работе [6].

После оценки рисков и определения требуемого уровня строгости аутентификации ведомства могут выбирать технологию, которая обеспечивает выполнение хотя бы минимальных технических требований для данного уровня строгости аутентификации:

• требований к аутентификаторам (токенам);

• требования к подтверждению подлинности, регистрации и передаче электронных удостоверений, привязывающих пользователя к аутентификатору;

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

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

Ниже приводится краткое содержание требований к каждому из четырёх уровней.

Уровень 1. На этом уровне нет требований к подтверждению подлинности, но механизм аутентификации предоставляет некоторую долю уверенности в том, что заявитель, обращающийся к транзакции или данным, – тот, за кого себя выдаёт. Аутентификация признаётся успешной, если заявитель предоставляет по протоколу безопасной аутентификации доказательство владения аутентификатором. Пароли или секреты не передаются по сети в открытом виде. Но этот уровень не требует применения криптографических методов защиты. Во многих случаях злоумышленник, имеющий доступ к каналу связи, имеет возможность восстановить пароль, используя атаку со словарём.

Уровень 2 предполагает использование однофакторной аутентификации в удалённой сети. Вводятся требования к подтверждению подлинности. При использовании аутентификационных секретов длительного хранения таковые не доверяются никакой из сторон, за исключением заявителя, а проверяющие стороны подчиняются поставщику службы электронных удостоверений (Credentials Service Provider, CSP); однако CSP может предоставлять независимым проверяющим сторонам сеансовые (временные) общие секреты. Обязательно должны использоваться разрешённые криптографические методы. Подтверждения подлинности заявителей, выпускаемые в результате их успешной аутентификации, аутентифицируются криптографически (разрешёнными методами) либо получаются напрямую от доверенной стороны по безопасному протоколу аутентификации.

Уровень 3 предоставляет многофакторную (не менее 2) аутентификацию в удалённой сети. Процедуры подтверждения подлинности требуют проверки идентифицирующих материалов и информации. Аутентификация основана на доказательстве владения ключом или одноразовым паролем по криптографическому протоколу, требуется наличие механизмов обеспечения строгости криптографии, защищающих первичные аутентификаторы (секретный ключ, закрытый ключ или одноразовый пароль) от компрометации методами прослушивания, воспроизведения, онлайн-угадывания, имитации проверяющей стороны и «человек посередине». Могут использоваться три вида аутентификаторов – программные криптографические аутентификаторы, аппаратные криптографические аутентификаторы и аппаратные генераторы одноразовых паролей. При использовании аутентификационных секретов длительного хранения таковые не доверяются никакой из сторон, за исключением заявителя, а проверяющие стороны подчиняются CSP; однако CSP может предоставлять независимым проверяющим сторонам сеансовые (временные) общие секреты. Для всех операций используются легитимные криптографические методы. Подтверждения подлинности заявителей, выпускаемые в результате их успешной аутентификации, аутентифицируются криптографически либо получаются напрямую от доверенной стороны по безопасному протоколу аутентификации.

Уровень 4 предназначен для обеспечения самой строгой аутентификации на основе доказательства владения закрытым ключом по криптографическому протоколу. Уровень 4 аналогичен уровню 3, за исключением того, что на нём допускается использование только аппаратных криптографиче-

ских аутентификаторов, усилены требования FIPS 140-2 к оценке криптографических модулей и требуется, чтобы в дальнейшем подлинность передаваемых конфиденциальных данных подтверждалась с использованием ключа, привязанного к процессу аутентификации. Аутентификатор должен быть аппаратным криптографическим модулем, имеющим сертификат соответствия FIPS 140-2 уровня 2 или выше с обеспечением физической безопасности на уровне не ниже FIPS 140-2 уровня 3. Требуется строгая криптографическая аутентификация всех сторон и при всякой передаче конфиденциальных данных между сторонами. Могут использоваться как симметричные, так и асимметричные криптографические алгоритмы. Аутентификация требует подтверждения заявителем владения аутентификатором по безопасному протоколу аутентификации. Должны предотвращаться атаки прослушивания, воспроизведения, онлайн-угадывания, имитации проверяющей стороны и «человек посередине». При использовании аутентификационных секретов длительного хранения они не доверяются никакой из сторон, за исключением заявителя, а проверяющие стороны подчиняются CSP; однако CSP может предоставлять независимым проверяющим сторонам сеансовые (временные) общие секреты. Для всех операций должны использоваться стойкие одобренные криптографические методы. При всякой передаче конфиденциальной информации осуществляется криптографическая аутентификация с использованием ключей, привязанных к процессу аутентификации.

Данный подход нашел свое развитие в работах [7–10]. Например, в стандарте [8] для сотрудников федеральных агентств однозначно предписано использование строгой аутентификации уровня 4 с применением интеллектуальных смарт-карт SSCD (Secure Signature Creation Device, токены с неизвлекаемым закрытым ключом). Точно такие же требования присутствуют в драфтах американских и европейских нормативных актов, разработанных в 2011 г. [9, 10].

Предлагаемый способ построения уровней строгости аутентификации. В отличие от развитых стран мира, использующих 4-уровневую иерархию строгости аутентификации, в настоящей работе предлагается простая и понятная трехуровневая модель ИА. Такая модель наиболее полно согласовывается с текущим состоянием нормативной базы как в части оценки состояния защищенности ИС, обрабатывающих информацию ограниченного доступа, не содержащую гостайну, так и в части законодательства по защите персональных данных и электронной подписи. Так, в соответствии с №63-ФЗ на территории РФ с 1 июля 2012 г. вводится 3 вида электронной подписи: простая, усиленная неквалифицированная, усиленная квалифицированная. Условно можно ассоциировать массовое применение простой подписи с гражданами, усиленной неквалифицированной и квалифицированной – с предприятиями и организациями, а усиленной квалифицированной – с государственными структурами различного уровня. Этот подход согласуется с основными положениями №149-ФЗ, где сказано, что участниками электронного взаимодействия и обладателями информации могут являться 3 уровня пользователей: граждане (физические лица), организации (юридические лица), государство (государственные органы и органы местного самоуправления). Деление на три большие группы приемлемо как с точки зрения грубой оценки рисков (низкий, средний, высокий), так и для оценки надежности, а также последствий от ошибок ИА и атак (уровни: низкий, средний, высокий). В сложившейся за период с 2002 г. практике применения аутентификаторов (токенов) также массово используется всего 3 распространенных типа: многоразовый пароль, технология одноразовых паролей OTP (One Time Password) и технология строгой двухфакторной аутентификации с применением смарт-карт, содержащих неизвлекаемый ключ электронной подписи, применение которого невозможно без ввода PIN-кода (по сути, в этом случае используется технология электронной подписи). Таким образом, основываясь на приведенных рассуждениях и исследованиях, проведенных автором в работах [11–13], можно выделить три уровня строгости аутентификации.

Уровень 1. Разрешенным токеном при удаленной аутентификации является многоразовый пароль без требований контроля целостности. Аутентификация признается успешной при доказательстве владения токеном по одному из безопасных протоколов аутентификации, подробно рассмотренных в [13]. Пароль не должен в открытом виде передаваться по сети. Желательно соблюдать требования по длине пароля (не менее 6 символов). Разрешается использовать простую электронную подпись. Нет требований по надежности ИА. Основными обладателями информационных ресурсов на этом уровне предполагаются граждане, которые определяют риски проникновения на их ресурсы мошенников самостоятельно. Также на их ответственности лежит возможное производство электронных удостоверений (ЭУ) и передача прав доверительным сторонам. Безусловно, приветствуется использование на этом уровне аутентификаторов и ЭУ с уровней 2 и 3.

Уровень 2. Рекомендуется применение двухфакторной аутентификации (смарт-карта плюс PIN-код) или технологии OTP при использовании двух независимых каналов для доставки парольной информации пользователю. Издание ЭУ разрешено не только аккредитованным УЦ. Передача прав доверия третьим сторонам производится на основе двухсторонних соглашений (договоров) или на основе кросс-сертификации. Разрешено применение технологии многоразовых паролей при условии защиты канала и проверки целостности. Также разрешено использовать программный криптографический аутентификатор. Приветствуется использование технологий уровня 3. Основными обладателями информационных ресурсов предполагаются предприятия с развитой инфраструктурой открытых ключей. Для аутентификации и взаимодействия с государственными органами обязательно применение аутентификации уровня 3 и криптоалгоритмов ГОСТ 34.10–2001 и ГОСТ 34.11–2001.

Уровень 3. Рекомендуется использование только строгой, как минимум, двухфакторной взаимной (информационный ресурс – претендент) аутентификации с применением аутентификаторов с неизвлекаемым ключом электронной подписи (устройства класса SSCD). Это позволит обеспечить защиту ключа подписи от воспроизведения, он-лайн угадывания, имитации проверяющей стороны и атак класса «человек посредине». Согласно исследованию [11] биометрия может использоваться как дополнительный (но не основной) фактор аутентификации. Это позволит эффективно противостоять фишингу. Особое внимание следует уделять строгости процесса регистрации заявителей, изданию ЭУ и передаче прав доверительным сторонам. Рекомендуется использование только российских криптографических алгоритмов при издании ЭУ для электронной подписи и шифрования. При этом УЦ, издающий ЭУ, должен быть аккредитован в Минкомсвязи РФ.

Соответственно для предложенных трех уровней строгости аутентификации в дополнение к таблицам работы [12] можно привести соответствующие аутентификаторы, лежащие в основе системы аутентификации (табл. 1).

Таблица 1

Типы аутентификаторов, которые можно использовать на различных уровнях строгости

Тип аутентификатора	Уровень 1	Уровень 2	Уровень 3
Аппаратный криптографический аутентификатор	√	√	√
Устройство одноразовых паролей	√	√	
Программный криптографический аутентификатор	√	√	
Пароли и PIN-коды	√		

На основе предложенного подхода можно выделить требования к взаимодействию основных групп участников. Например, гражданин при запросе государственной услуги со своего уровня 1 может аутентифицироваться и пользоваться своей простой подписью, а уполномоченный сотрудник госоргана при ответах на запросы граждан будет скреплять ответ своей квалифицированной подписью, при этом подлинность автора и валидность подписи можно легко проверить. Для основных групп участников электронного взаимодействия соответствие уровней строгости аутентификации представлено в табл. 2.

Таблица 2

Соответствие уровней строгости аутентификации группам участников электронного взаимодействия

Участники электронного взаимодействия	Уровень 1	Уровень 2	Уровень 3
Граждане	√	√	√
Сотрудники негосударственных предприятий и организаций		√	√
Сотрудники государственных предприятий и учреждений			√

Также можно рассмотреть и требования к уровням строгости аутентификации при доступе на информационные ресурсы. Например, для доступа на информационный ресурс организации (к комплексной информационной системе – КИС) гражданину надо «играть по правилам» данной организации и получить легальное ЭУ, а также предъявить принятый для данной организации аутентификатор. Возможные комбинации требований к уровню строгости аутентификации для основных участников электронного взаимодействия для данной задачи представлены в табл. 3.

Таблица 3

Рекомендуемое соответствие уровней строгости аутентификации группам участников электронного взаимодействия при доступе в информационные системы (ИС)

Участники электронного взаимодействия/ИС	Граждане	КИС	ГИС
Граждане	1	2	3
Сотрудники негосударственных предприятий и организаций	1–2	2	3
Сотрудники государственных предприятий и учреждений	1–3	2–3	3

Основные защитные меры для различных уровней строгости аутентификации представлены в табл. 4.

Таблица 4

Защитные меры для удаленного доступа через открытые сети связи

Защита от	Уровень 1	Уровень 2	Уровень 3
Угадывания	√	√	√
Воспроизведения (повтор)		√	√
Перехвата		√	√
Имитации проверяющей стороны			√
Атак класса «Человек посередине»			√

Весьма полезным при построении системы аутентификации может оказаться использование различных типов протоколов аутентификации, подробно рассмотренных в [13]. Применительно к уровням строгости аутентификации результаты анализа представлены в табл. 5.

Таблица 5

Типы протоколов аутентификации при удаленном доступе

Тип протокола	Уровень 1	Уровень 2	Уровень 3
Доказательство владения закрытым ключом	√	√	√
Доказательство владения симметричным ключом	√	√	√
Доказательство знания пароля	√		

Заключение. Рассмотрен зарубежный опыт разработки требований и рекомендаций к уровням гарантий аутентификации.

Предложен способ построения уровней строгости аутентификации в зависимости от групп участников электронного взаимодействия. Способ основан на текущем состоянии отечественной нормативной базы, учитывает сложившуюся практику применения технологий идентификации и аутентификации при организации доступа к личным, корпоративным и государственным информационным ресурсам, а также учитывает десятилетний опыт применения электронных подписей.

Результаты данной работы могут использоваться для построения единой государственной системы идентификации и аутентификации. В развитие данной работы планируется исследование рисков и разработка рекомендаций по одним из самых критичных к атакам процессов аутентификации – регистрации заявителей, изданию электронных удостоверений и делегированию прав доступа третьим доверенным сторонам. Также не исследованным, но очень важным вопросом при построении государственной системы идентификации и аутентификации представляется проблема надежности процессов аутентификации.

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» [Электронный ресурс]. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=122455 свободный (дата обращения: 01.08.2012).

2. Ministerial Declaration on Authentication for Electronic Commerce 7-9 October 1998 [Электронный ресурс]. – Режим доступа: http://itlaw.wikia.com/wiki/Ottawa_Declaration_on_Authentication_for_Electronic_Commerce, свободный (дата обращения: 01.08.2012).

3. CWA 14365. Guide of use of Electronic Signature. Jan. 2003 [Электронный ресурс]. – Режим доступа: http://www.sigillum.pl/sig-cmsws/page/GetFile.aspx?cfid=187&fn=wses_n0202.pdf, свободный (дата обращения: 01.08.2012).

4. OMB Memorandum M-04-04 E-Authentication Guidance for Federal Agencies December 16, 2003 [Электронный ресурс]. – Режим доступа:http://csrc.nist.gov/drivers/documents/m04-04.pdf, свободный (дата обращения: 01.08.2012).

5. Homeland Security Presidential Directive 12 (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors. August 27, 2004 [Электронный ресурс]. – Режим доступа: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf, свободный (дата обращения: 01.08.2012).

6. NIST SpecialPublication 800-63 April 2006 [Электронный ресурс]. – Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf, свободный (дата обращения: 01.08.2012).

7. OECD Recommendation on Electronic Authentication. June 12, 2007 [Электронный ресурс]. – Режим доступа: http://www.oecd.org/dataoecd/32/45/38921342.pdf, свободный (дата обращения: 23.02.2012).

8. FIPS PUB 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors. March 2006 [Электронный ресурс]. – Режим доступа: http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf, свободный (дата обращения: 01.08.2012).

9. FIPS PUB 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors. March 2011 [Электронный ресурс]. – Режим доступа: http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf, свободный (дата обращения: 01.08.2012).

10. ETSI draft SR 000 000 v0.0.2 Rationalized Framework for Electronic Signature Standardization August 2011 & ETSI TS 1, 103173 [Электронный ресурс]. – Режим доступа: http://www.epractice.eu/files/Rationalised%20Framework%20for%20Electronic%20Signature%20Standardisation.pdf, свободный (дата обращения: 01.08.2012).

11. Сабанов А.Г. Технологии идентификации и аутентификации / А.Г. Сабанов // ВКСС Connect! – М., 2006. – № 1. – С. 65–79.

12. Сабанов А.Г. Аутентификация при электронном обмене документами // Доклады Том. гос. ун-та систем управления и радиоэлектроники. – 2011. – № 2(24). – С. 263–266.

13. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учеб. пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др.; под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. – М.: Горячая линия-Телеком, 2009. – 552 с.

Сабанов Алексей Геннадьевич
Канд. техн. наук, заместитель генерального директора ЗАО «Аладдин Р.Д.», Москва
Тел.: 8-985-924-52-09
Эл. почта: asabanov@mail.ru; a.sabanov@aladdin-rd.ru

Sabanov A.G.
Severity levels of authentication

In this article there is an observation of severity levels of authentication abroad. A method of forming severity levels of authentication is suggested.
Keywords: remote authentication, identification, electronic signature.