Р А Д И О Ф И З И К А

УДК 004.089

ОСОБЕННОСТИ АУТЕНТИФИКАЦИИ ПРИ ДОСТУПЕ К ОБЛАЧНЫМ СЕРВИСАМ

А.Г. Сабанов

ЗАО «Аладдин Р.Д.», Москва

a.sabanov@aladdin-rd.ru

Поступила в редакцию 23.01.2013

Рассмотрены особенности аутентификации для облачных вычислений. Показано, что применение парольной защиты и одноразовых паролей оправданно для частного облака, но не обеспечит требований информационной безопасности и текущего законодательства для публичного облака. Для организации безопасного доступа к облачным сервисам рекомендуется применять технологии строгой взаимной аутентификации на основе применения механизма квалифицированной электронной подписи.

Ключевые слова: удаленная аутентификация, идентификация, риски, электронная подпись, облачные вычисления, облачные сервисы.

Введение

Управление доступом пользователей к информационным ресурсам традиционно является одной из самых сложных задач в сфере информационных технологий. При переходе к облачным вычислениям и сервисам эта задача становится еще более сложной и актуальной. В условиях интенсивного строительства электронного правительства и развития государственных услуг в электронном виде переход к облачным сервисам является одним из высокоэффективных способов быстрого выхода на необходимый уровень производительности для массового оказания услуг. С учетом сложившейся неравномерности уровней информатизации некоторых отраслей (примерами отстающих отраслей являются медицина, образование и т.д.) при строительстве информационного общества переход к облачным сервисам может существенно выровнять возможности оказания услуг по отраслевому признаку.

При всех достоинствах облачных сервисов (в первую очередь, отсутствие необходимости содержать развитую инфраструктуру из аппаратных и программных компонентов на местах, закупки и содержания дорогих компьютеров и ПО, а также отказоустойчивость, экономичность и эффективность, простота использования, гибкость и масштабируемость) организация безопасного доступа к ним является далеко не тривиальной задачей.

1. При переходе к облакам для использования облачных сервисов применительно к оказанию государственных услуг создается новый тип информационных систем (ИС) – ИС общего пользования (ИСОП), «участниками электронного взаимодействия в которых является неопределенный круг лиц и в использовании которых этим лицам не может быть отказано» (ст. 2 п. 13 Федерального закона [1]). В отличие от хорошо изученных корпоративных систем, в которых участники информационного взаимодействия становятся легальными пользователями системы после заключения трудового договора, обязывающего их выполнять определенные правила работы с вычислительной техникой и информацией, пользователи ИСОП, как правило, не связаны столь строгими договорными отношениями и вытекающими из них регламентами. С другой стороны, в ИСОП для внешних пользователей системы, как правило, невозможно осуществлять хорошо развитые к настоящему времени корпоративные политики безопасности, включающие в себя кроме нормативной базы и организационных мер необходимые настройки легального (и, как правило, сертифицированного) корпоративного системного, прикладного и специального программного обеспечения. Поэтому пользователи ИСОП априори должны получать доступ к облачным сервисам из так называемой «недоверенной» среды.

2. В связи с выходом Постановления Правительства РФ от 28 ноября 2011 г. № 977 [2], которое предписывает в весьма сжатые сроки 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. Согласно международной классификации фактически строится общедоступное облако в государственном масштабе. Создание систем управления удаленным доступом к информации, содержащей конфиденциальные данные, в частности, персональные данные граждан (ПДн), является одной из самых сложных задач даже в масштабе одного отдельно взятого предприятия, не говоря уже о масштабах страны. При создании ЕСИА аспекты безопасности и интегрирования их в единое пространство доверия не принимались во внимание.

3. Исходя из анализа зарубежного опыта создания подобных систем одним из ключевых принципов является введение требований выполнения определенных уровней строгости аутентификации для различных групп пользователей и уровней защищенности ИС, к которым соответствующие группы пользователей имеют права доступа. Фактически речь идет об уровнях доверия, или уровнях гарантий (levelofassurance), которые подробно рассмотрены в работе [3]. Введение уровней строгости аутентификации лежит в основе самого распространенного в странах Европы и в 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 [4–12], в России вопросам стандартизации процессов идентификации и аутентификации не уделялось должного внимания. До выхода в свет [2] проблемам аутентификации не был посвящен ни один нормативный акт. Также в российской нормативной базе отсутствуют какие-либо технические требования и даже рекомендации к построению уровней доверия аутентификации вообще и к облачным сервисам в частности.

С целью устранения этого пробела сначала введем некоторые термины и определения. Для решения задачи изучения вопросов аутентификации при доступе к облачным сервисам рассмотрим некоторые наиболее существенные особенности аутентификации при облачных вычислениях с точки зрения оценки общих рисков и уязвимостей. Затем на основе анализа основных процессов и процедур аутентификации сформулируем некоторые рекомендации для организации аутентификации с целью обеспечения безопасного доступа к облачным сервисам.

Определение основных понятий удаленной аутентификации и облачных вычислений

Поскольку удаленная аутентификация отличается от хорошо изученной аутентификации в локальной сети [13, 14], сначала введем определение некоторых понятий.

Процесс аутентификации – процесс подтверждения подлинности субъекта. Производится с помощью подтверждения владения секретом, изданным и выданным субъекту в процессе регистрации после полной идентификации, состоящей в тщательной проверке предъявленных субъектом идентификаторов.

Идентификатор – уникальная метка, присвоенная субъекту для того, чтобы отличить его от других.

Процесс идентификации – сравнение предъявленного субъектом идентификатора с эталонным, занесенным в базу при присвоении уникальной метки данному субъекту.

Токен (аутентификатор) – секрет, изданный и выданный субъекту в процессе регистрации после тщательной проверки его идентификаторов. Токеном владеет и управляет заявитель (субъект). Токен (обычно секретный ключ, в простейшем случае – пароль) используется при аутентификации заявителя.

Подтверждение подлинности — процесс, в рамках которого доверяющая сторона или центр регистрации проверяет достаточную для уникальной идентификации пользователя информацию.

Электронное удостоверение (ЭУ) – объект, достоверно привязывающий аутентификатор (а чаще всего и некоторые идентификаторы) к субъекту, и, возможно, дополнительные атрибуты идентификации – к аутентификатору (токену), которым владеет и который контролирует субъект.

Облачные вычисления – модель, предоставляющая удобный сетевой доступ по требованию к общей совокупности настраиваемых вычислительных ресурсов (например, сетям, серверам, хранилищам, приложениям и службам), которые могут быстро выделяться и освобождаться с минимальными организационными усилиями и минимальным участием поставщика услуг.

Облачные услуги предоставляются по трём моделям, в зависимости от уровня контроля со стороны клиента: программное обеспечение как услуга (SoftwareasaService, SaaS), платформа как

услуга (PlatformasaService, PaaS); инфраструктура как услуга (InfrastructureasaService, IaaS).

Основные риски, возникающие при переходе к облачным вычислениям

Если подходить к вопросу классификации рисков с классических позиций, то для основных участников процессов при переходе к облачным вычислениям (пользователи, провайдеры, поставщики услуг) следует рассмотреть, по крайней мере, три категории рисков: организационные, юридические, технические.

Наибольшие риски ожидаются со стороны пользователей. Они наиболее уязвимы при переходе к облачным вычислениям.

В качестве примеров организационных рисков могут рассматриваться:

- риск потери управления, который может привести к невозможности соблюдения требований обеспечения конфиденциальности, доступности и целостности данных;
- привязка к поставщику облачных услуг, что может повлечь финансовые потери вследствие повышения стоимости услуг или попытки перейти к другому провайдеру;
- неполный перечень всех условий и уровней обслуживания (SLA) вследствие отсутствия опыта или навязывания текста провайдером, что может отразиться, например, в виде неполного предоставления оплаченных услуг.

Перечислим юридические риски:

- неразвитая законодательная и подзаконная нормативная база;
- нарушение требований законодательства при переходе к облачным вычислениям;
- возможность появления конфликтов по поводу вопросов об ответственности сторон, о владельце данных, обрабатываемых в облаке, а также по поводу оперативного учета, восстановления после аварий и взломов.

Выделим основные технологические риски, связанные с переходом на облачные вычисления:

- гарантии подлинности сайта (атаки типа «фишинг»), подмена сайта (должен обеспечить провайдер);
- атаки типа «человек посередине»;
- способы определения и гарантии подлинности пользователя при доступе к облаку и сервисам;
- возможность потери пользователями контроля над приложениями и службами;
- действия злоумышленников из числа привилегированных пользователей провайдера;
- неполное удаление данных в облачной инфраструктуре при уходе клиента или согласованном стирании данных;
- отсутствие стандартов для облачных вычислений;
- ошибки изоляции между ресурсами в облачной архитектуре и, как следствие, возможности утечки данных;
- потенциальная опасность нарушения доступности, конфиденциальности и целостности данных при их передаче, хранении и обработке в облаке;
- публичное разглашение данных (доступ неограниченного круга лиц);
- выемка данных или носителей из датацентра провайдера (органы, сотрудники).

Видно, что более половины перечисленных рисков в той или иной степени связаны с вопросами аутентификации и персонификации (персонально назначенные права доступа и независимый аудит действий пользователей [3]).

По такому же принципу можно перечислить риски со стороны провайдера облачных услуг. В частности, как способ устранения наиболее существенных технологических рисков провайдера может рассматриваться решение следующих задач:

- обеспечение базовой защищенной (доверенной) среды на всех уровнях взаимодействия (сервер–сервер, клиент–сервер, клиент–браузер–сервер приложений), в которой, в частности, данные разных клиентов надежно изолированы друг от друга, а клиентам обеспечен прозрачный гарантированно защищенный доступ к их данным и необходимым для обработки этих данных приложениям (сервисам);
- обеспечение контроля действий администраторов и привилегированных пользователей (уровня гарантий защиты от инсайдеров);
- прозрачные и понятные для клиентов принципы системы защиты облачных систем, систем управления, хранения данных и систем контроля за этими процессами.

Одной из непростых задач для провайдера может оказаться обоснование и защита модели угроз, а также выбор средств защиты информации. При этом необходимо учитывать принципы отбора поставщиков облачных сервисов и, в частности, обеспечения доступности.

Особенности аутентификации при доступе к облачным сервисам

Аутентификация для организации облачных вычислений имеет следующие общие особенности:

- для удобства пользователей должны использоваться механизмы однократной удаленной аутентификации при доступе к различным облачным сервисам;

- для обеспечения взаимодействия облачных сервисов с сервисом аутентификации должны использоваться широко распространенные протоколы, стандарты и модели контроля доступа;
- должен использоваться мировой опыт и лучшие практики;
- должна обеспечиваться информационная безопасность сервисов аутентификации.

Основными задачами информационной безопасности для «облачных» вычислений являются:

- обеспечение безопасной удаленной регистрации;
- безопасное ведение учетных записей пользователей;
- обеспечение безопасного делегирования аутентификации и доверия в облачные сервисы;
- управление доверием при взаимодействии облачных сервисов;
- разделение доступа пользователей и контроль доступа в привязке к методу аутентификации пользователя, его роли и требований к уровню доверия в облаке;
- обеспечение контролируемого по времени (по протяженности) доступа с гарантией обрыва сессии по истечении заданного времени доступа.

Участники процессов удаленной аутентификации

Перечислим основных участников аутентификации:

- субъект доступа (называемый также аппликант, претендент, заявитель);
- центр регистрации (ЦР) – его основной задачей является установление и фиксация (закрепление) связи субъекта и его уникального секретного признака – аутентификатора. В качестве такого центра может выступать, например, удаленный ЦР удостоверяющего центра (УЦ), связанный доверительными отношениями с данным УЦ;
- доверяющая сторона – владелец того ресурса, к которому претендует получить доступ субъект доступа. Он проверяет по протоколу аутентификации факт владения субъекта доступа соответствующим аутентификатором – секретом, который выдан субъекту ЦР-ом;
- проверяющая сторона (центр валидации, ЦВ) входит в состав инфраструктуры открытых ключей (ИОК), выполняет проверку наличия фиксированной ЦР-ом связи «субъект доступа – аутентификатор». Например, проверяет, является ли ЭУ действительным (валидным) на момент проверки.

Может иметь место объединение отдельных сущностей в одном лице. Например, ЦР, ЦВ и доверяющая сторона могут быть объединены в единую структуру.

Основные процессы удаленной аутентификации

Напомним, что в основе аутентификации лежат три основных и тесно взаимосвязанных процесса:

1. **Регистрация** – установление (идентификация) личности и регистрация аутентификатора (секрета), а также издание связанного с ним электронного удостоверения (ЭУ) – аналог выдачи паспорта. Также обязательной процедурой является привязка зарегистрированного и изданного для данного субъекта секрета к его личности. По большому счету, главная цель ЭУ – связать секрет (аутентификатор) с личностью и ее предъявленными и проверенными идентификаторами или с новыми идентификаторами, которые выдает ЦР. Данная процедура подразделяется на несколько связанных между собой последовательных процессов, осуществляемых в ЦР [15]. Процедура может производиться с личным присутствием или удаленно. Процедура может проводиться по заданному регламенту или нет.
2. **Протокол аутентификации** – процедура проверки факта владения претендента секретом (аутентификатором). Данная процедура является аналогом предъявления паспорта и сличения фотографии для идентификации личности. Эта процедура осуществляется доверяющей стороной, может быть с разделяемым секретом или нет, устойчивой к атакам по каналу связи или нет. Наиболее сложным вариантом является тот, когда аутентификатор состоит из нескольких компонентов (факторов), и каждый компонент проверяется по своему протоколу. Это так называемая многофакторная аутентификация.
3. **Валидация** (проверка действительности) – процедура проверки подлинности и периода действия ЭУ (аналог проверки действительности паспорта). Осуществляется в центре валидации (ЦВ), может проводиться по заданному регламенту или нет.

В соответствии с методом исследования основных процедур аутентификации, развитым в работе [15], воспользуемся хорошо зарекомендовавшим себя в изучении вопросов безопасности удаленной аутентификации процессным подходом. В работе [15] подробно рассмотрены процесс регистрации и составляющие этот процесс основные процедуры. Результаты этой работы можно полностью распространить и на задачи аутентификации при доступе к облачным вычис-

лениям. Рассмотрим теперь второй основной процесс – протоколы аутентификации.

В процессе собственно аутентификации (протокол аутентификации) участвуют две стороны: претендент и проверяющая сторона. Рассмотрим основные процедуры, критичные с точки зрения безопасности, для обеих сторон, и собственно для процесса обмена претендент–доверяющая сторона. Будем считать реализации алгоритмов, реализованные в протоколах аутентификации, защищенными.

Выделим 4 основные процедуры: хранение секрета (аутентификатора) на стороне заявителя, передачу его доверяющей стороне, хранение учетных записей на сервере доверяющей стороны и проверку предъявленных секретов. Процедуры на сервере проверяющей стороны также будем считать безопасными. На стороне претендента самой критичной процедурой является процесс хранения секрета.

Процедура хранения секрета на стороне субъекта доступа. Простейшим секретом является пароль. Способы его хранения и связанные с этим уязвимости подробно рассмотрены во многих публикациях, например, в [14]. Как показано в этих публикациях, в абсолютном большинстве случаев применение пароля небезопасно, существует множество способов атак для его раскрытия. Одним из относительно безопасных для доставки и хранения пароля является разделение секрета и доставка частей пароля пользователю по различным независимым каналам.

Применение технологии OTP (One Time Password – технологии открытых паролей) более привлекательно, это уже средство усиленной аутентификации [13]. Однако для применения OTP необходимо выстроить инфраструктуру, допускающую применение технологий OTP и построенных на едином формате атрибутов средств предоставления доступа ко всем облачным сервисам [14]. Это дорого и представляется возможным реализовать только в частном или корпоративном облаке.

Третьим известным и самым перспективным механизмом аутентификации является применение в качестве главного аутентификатора ключа электронной подписи (ЭП). В ст. 10 Федерального закона 63-ФЗ сказано, что «ответственность за хранение ключа подписи лежит на его владельце». При массовом использовании ЭП к описанным процедурам будут привлечены разные слои населения, в том числе люди, совершенно далекие от информационных технологий и информационной безопасности. Это – одна сторона медали. Другая сторона – действительно важные ресурсы и самый серьезный подход к формированию (генерации) ключей подписи. В стандарте FIPS [10] и драфте его апргрейда [11], а также в рекомендациях ЕС [12] и проектах европейских требований, разработанных ETSI в 2011 г., для формирования ключевой пары квалифицированной подписи существует требование использования исключительно SecureSignatureCreationDevice (SSCD) устройств. Заметим, что в действующих на сегодня регламентах УЦ зачастую отсутствует элементарное требование активации флага «неизвлекаемость закрытого ключа». Для хранения закрытого (секретного) ключа существует несколько альтернатив:

- запись и последующее хранение в реестре компьютера;
- запись на дискету;
- запись на электронный носитель (USB-ключ, смарт-карту), например, в EEPROM, в лучшем случае – с взведенным флагом «неизвлекаемость контейнера из носителя» при любых манипуляциях (введение PIN-кода пользователя, PIN-кода администратора, ...);
- генерация и гарантируемая неизвлекаемость в SSCD-устройстве.

Для предпоследнего варианта (запись на электронный носитель) необходим, как минимум, сертификат ФСТЭК России на использование носителя для надежного хранения ключевых контейнеров.

Естественно, последний из перечисленных вариантов сразу выглядит наиболее безопасно, особенно если устройство имеет сертификаты не только FIPS, ITSec, но и сертификат ФСБ России.

Процедура предъявления аутентификатора доверяющей стороне. Пароль по современным требованиям, как правило, передается в зашифрованном виде.

OTP передается по сети в открытом виде. Защита кода OTP в данном случае состоит в том, что при формировании кода OTP используется вектор начальной инициализации согласно RFC6560. Вторым фактором защиты считают непродолжительность сеанса OTP и то, что в следующем сеансе используется уже новый код (невозможность повторного использования перехваченного кода OTP). Для усиления функций защиты в корпоративном использовании применяется способ, состоящий в комбинации парольной защиты и OTP. Серверу доверяющей стороны при этом претендент на доступ предъявляет комбинацию из последовательно набранных символов, состоящую из многоразового пароля и кода OTP.

Особенности предоставления доступа к облачным сервисам

Обычный (многоразовый) пароль не имеет ограничения по времени. По этой причине его

можно применять для организации доступа только для частных облаков, где можно не ограничивать срок оказания услуги.

Для публичных облаков, как правило, требуется предоставить доступ не к одному, а к нескольким сервисам, расположенным, как правило, в разных облаках. Например, это могут быть облака, принадлежащие разным ведомствам (ФНС, ПФР, МВД,...). Одноразовый пароль при этом также не годится. Либо он становится многоразовым (нарушение безопасности), либо сервис окажется недоступным для пользователя вследствие его остановки, т.к. для следующей сессии требуется свежий OTP-пароль.

Таким образом, для предоставления доступа к приложениям, размещенным в публичных облаках, единственным способом безопасной аутентификации остается строгая взаимная аутентификация «пользователь–сервер», основанная на применении цифрового сертификата и механизма электронной подписи. При этом, как показано в [3], для граждан и сотрудников коммерческих предприятий для получения ряда услуг могут использоваться усиленные неквалифицированные сертификаты подписи, а для уполномоченных сотрудников государственных органов, подписывающих документы с правовыми последствиями, необходимо применять средства аутентификации, основанные на усиленных квалифицированных сертификатах электронной подписи, закрытые ключи которой должны генерироваться в устройствах класса SSCD.

Итак, для организации аутентификации при доступе к облачным сервисам следуют выводы:

• для задачи «делегирование полномочий» нельзя использовать пароль (нельзя ограничить по времени) и технологию OTP (одноразовый пароль становится многоразовым или получим «отказ в обслуживании» из-за невозможности сгенерировать следующий OTP). При использовании механизма электронной подписи делегирование проводится с применением стандартных функций PKI;

• для вычислений в облаках, требующих разделения доступа, применение секретов классов «пароль» и OTP неприемлемо с точки зрения обеспечения безопасности пользователя;

• для обеспечения аутентификации в облаках необходимо применять только строгую двустороннюю аутентификацию на основе электронной подписи.

Заключение

Для успешного развития проектов, связанных с переходом к облачным вычислениям, необходимо уделять вопросам обеспечения информационной безопасности повышенное внимание. В частности, для общедоступного типа облаков наиболее актуальными становятся вопросы управления доступом пользователей и хранения информации ограниченного доступа, в частности, персональных данных, в зашифрованном или обезличенном виде. Для решения задачи разделения доступа предлагается рекомендовать методы персонификации доступа с применением современных средств двусторонней взаимной строгой аутентификации.

Результаты данной работы могут использоваться как для построения единой государственной системы идентификации и аутентификации, так и для построения отраслевых и корпоративных решений, использующих облачные вычисления.

В развитие данной работы планируется исследование проблем надежности процессов аутентификации, особенно при доступе к облачным сервисам.

Список литературы

1. Федеральный закон «Об электронной подписи» № 63-ФЗ от 7 апреля 2011 г.

2. 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"». URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=122455 (дата обращения: 23.02.2012).

3. Сабанов А.Г. Аутентификация при электронном обмене документами // Доклады Томского государственного университета систем управления и радиоэлектроники. 2011. № 2 (24). С. 263–266.

4. Ministerial Declaration on Authentication for Electronic Commerce 7–9 October 1998. URL: http:// it-law.wikia. com/wiki/Ottawa_Declaration_on_Authentication_for_Electronic_Commerce (дата обращения: 23.02.2012).

5. CWA 14365. Guide of use of Electronic Signature. Jan. 2003. URL: http://www.sigillum.pl/sig-cmsws/page/GetFile.aspx?cfid=187&fn=wses_n0202.pdf (дата обращения: 23.02.2012).

6. OMB Memorandum M-04-04 E-Authentication Guidance for Federal Agencies December 16, 2003. URL: http://csrc.nist.gov/drivers/documents/m04-04.pdf (дата обращения: 23.02.2012).

7. Homeland Security Presidential Directive 12 (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors. August 27, 2004. URL: http://www.whitehouse.gov/sites/default/files/omb/ memoranda/fy2005/m05-24.pdf (дата обращения: 23.02.2012).

8. NISTSpecialPublication 800-63 April 2006. URL: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf (дата обращения: 23.02.2012).

9. OECD Recommendation on Electronic Authentication. June 12, 2007. URL: http://www.oecd.org/ dataoecd/32/45/38921342.pdf (дата обращения: 23.02.2012).

10. 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-201-1-chng1.pdf (дата обращения: 23.02.2012).

11. FIPS PUB 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors. March 2011. URL: http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf (дата обращения: 25.02.2012).

12. ETSI draft SR 000 000 v0.0.2 Rationalized Framework for Electronic Signature Standardization August 2011 & ETSI TS 1, 103173. URL: http://www.epractice.eu/files/Rationalised%20Framework%20for%20Electronic%20Signature%20Standardisation.pdf (дата обращения: 25.02.2012).

13. Сабанов А.Г. Технологии идентификации и аутентификации // ВКССConnect!. М., 2006. № 1. С. 65–79.

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

15. Сабанов А.Г. Основные процессы аутентификации // Проблемы информационной безопасности. Компьютерные системы. СПб. 2012. № 2 (в печати).

SOME FEATURES OF AUTHENTICATION WHEN ACCESSING CLOUD SERVICES

A.G. Sabanov

Some features of authentication when accessing cloud services are considered. The use of password and one-time password protection technologies is shown to be justified for a private cloud, while it does not meet the information security requirements of the current legislation for a public cloud. To provide secure access to cloud services it is recommended to apply strong mutual authentication technologies using the mechanism of a qualified electronic signature.

Keywords: remote authentication, identification, risks, electronic signature, cloud computing, cloud services.