THE MODELLING OF THE EXCITATION CONDITIONS OF THE RANDOM APERTURE ANTENNA

Garnova N.V., Kostin V.N.

The paper presents the results of an experimental and computer modeling of the levels of electromagnetic fields intensity (EMFI) generated by a physical simulation of a random aperture antenna (RAA). It is proved that the term «phase error» can be used in study of EPMI of real RAA by statistical simulation method described in the article.

Keywords: *the levels of electromagnetic fields intensity, random aperture antenna, physical simulation of RAA, amplitude and phase errors, the statistical simulation method.*

Маслов Олег Николаевич, д.т.н., профессор, заведующий Кафедрой экономических и информационных систем Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел. 8-846-228-00-36; 8-902-371-06-24. E-mail: maslov@psati.ru

Раков Александр Сергеевич, к.т.н., доцент Кафедры мультисервисных сетей и информационной безопасности (МСИБ) ПГУТИ. Тел. 8-927-651-41-96. E-mail: racov-as@psuti.ru

Силкин Алексей Андреевич, ассистент Кафедры МСИБ ПГУТИ. Тел. 8-909-344-70-39.

УДК 004.56

АЛГОРИТМ ЗАЩИЩЕННОЙ АУТЕНТИФИКАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Кузнецов М.В., Чигирь Р.В.

В статье рассмотрены аспекты информационной безопасности при использовании технологий облачных вычислений, выявлены уязвимости клиентского соединения и предложен новый алгоритм защищенной аутентификации.

Ключевые слова: облачные вычисления, уязвимость клиента, взаимная проверка подлинности, защищенная аутентификация, «Kerberos», VPN.

Современный телекоммуникационный рынок претерпевает в последнее время принципиальное изменение в понимании о продукте, предоставляемом конечному пользователю. Время, когда телекоммуникационные компании предоставляли только услуги пользования линейными сооружениями связи, постепенно подходит к концу. Подобный подход уже не способен обеспечить прежний уровень доходности, что был, например, десять лет назад. Поэтому компании идут на расширение оказываемых услуг. Такими услугами могут стать различные сервисы, оказываемые по принципу облачных технологий. Данное направление в области построения и пользования сетевых структур является новым, эффективным и весьма перспективным, так как позволяет обеспечить максимальную производительную мощность при минимальном капиталовложении в саму организацию сети. Данная структура становится столь привлекательной еще и потому, что позволяет легко и динамично масштабировать необходимые ресурсы под нужды конкретных пользователей и автоматизировать все протекающие ИТ-процессы, выбирая готовые пакеты облачных платформ.

Однако из-за того, что данный подход является новым, и еще не изучены все возможные проблемы и уязвимости, возникает вопрос о безопасности использования подобных систем. Тем более что сервисы, использующие подобный подход к организации своей структуры, уже начинают сталкиваться с тем, что прежние меры и способы перестают быть столь же эффективными что и прежде. Самыми известными случаями за последнее время стали атаки на сервисы Amazon и eBay, а также на сервис закладок Magnolia. Опыт данных компаний показал, насколько могут быть уязвимы облачные сервисы при использовании мер безопасности предыдущего поколения, не учитывающих всех особенностей построения облачной инфраструктуры. Также стало ясно, что если не обеспечить должный уровень безопасности, то можно понести не только финансовые убытки, но и потерять большую часть своей клиентской базы, как в случае с Magnolia.

Одними из отличительных свойств облачных вычислений является доступность их ресурсов из любой точки мира, с любого терминала пользователя, имеющего выход к сети Internet, а также отсутствие географической привязки вычислительной инфраструктуры самого облака. Именно реализация этих функций и мешает использо-

ванию традиционных подходов в обеспечении безопасности, так как ни клиент, ни оператор услуг не могут знать наверняка, где именно находится тот или иной ресурс, в каком месте будет произведен вход в систему. Возникает проблема защищенности от сетевых атак. В связи с этим ведущие компании-разработчики программного обеспечения направляют свои усилия на создание средств защиты сред облачных вычислений. Национальные и международные организации, лидирующие в области разработки стандартов, ведут серьезную работу.

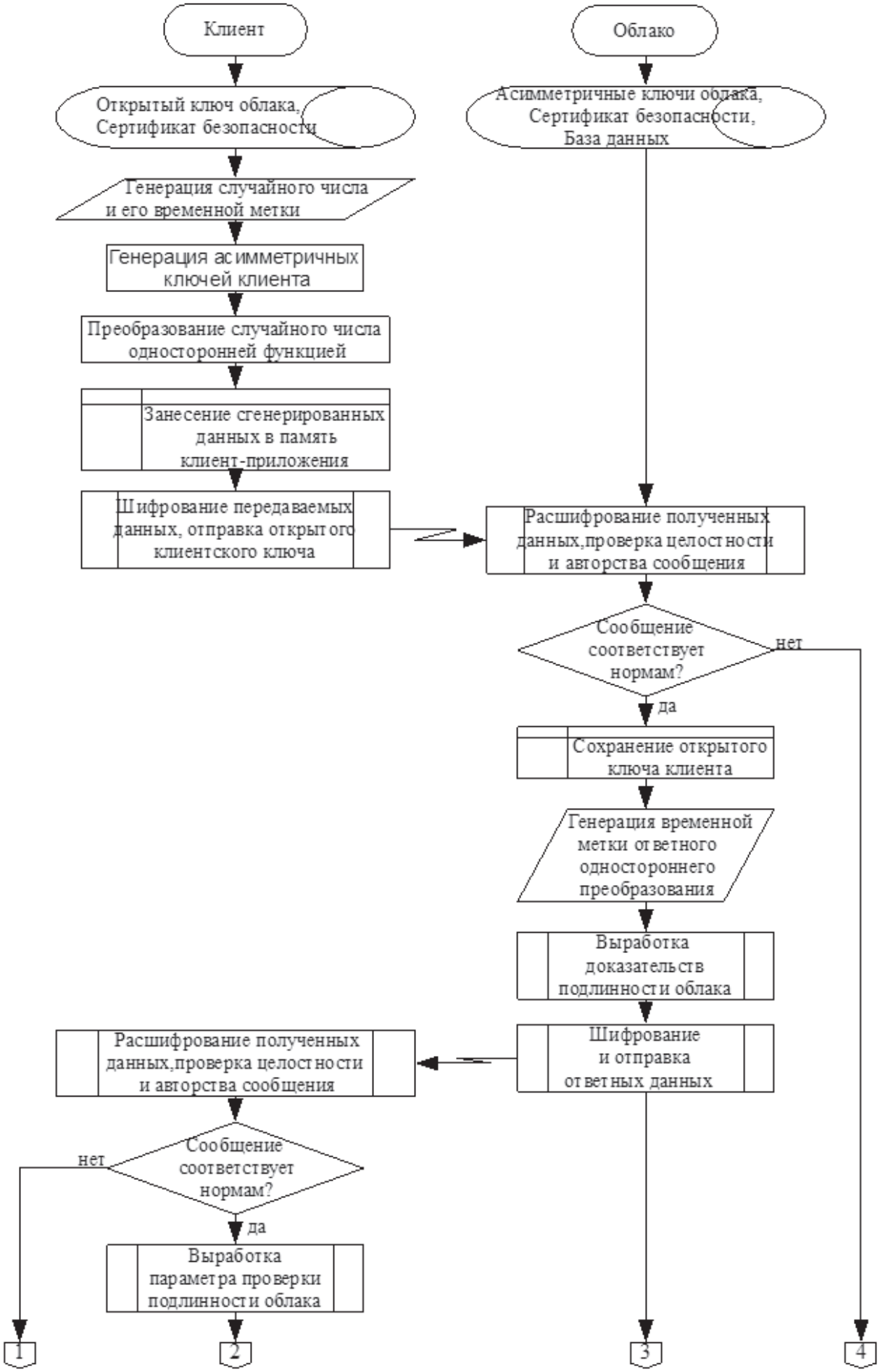
Одной из важнейших проблем, решаемых при построении новых систем безопасности облачных вычислений, является уязвимость клиента при подключении и работе в облаке, а также самой облачной инфраструктуры при предоставлении выделенных услуг каждому отдельному пользователю. Возникают трудности с неоднозначностью определения сторон, в связи с чем становится реальной угроза подмены одной из сторон, участвующей в процедуре идентификации пользователя, а также обостряется проблема распределения ключей безопасности в подобных системах. В связи с этим поднимается вопрос пересмотра традиционных подходов к системе идентификации пользователей, так как они уже не способны обеспечить прежний уровень безопасности из-за особенностей облачных структур.

За предыдущий период развития инфокоммуникационных систем в сфере безопасности сложились определенные критерии оценок эффективности работы системы, подходы к организации структуры сети, правила ее пользования. Также появились передовые производители, на которых стали ориентироваться остальные производства и решения которых вызывают большой интерес, а значит и спрос, у потребителей. Возникли некоторые предпочтения в типологии построения сетей и их безопасности.

Наиболее широкое распространение получила технология проверки «Церберос», где осуществляется трехсторонняя проверка подлинности под управлением, так называемого, арбитра. Данная структура за время пользования зарекомендовала себя как очень надежная, весьма быстродейственная и эффективная, но в современных условиях «повышенной облачности» она не способна работать на прежнем уровне, так как возникает проблема неопределенности положения того или иного ресурса. К тому же все яснее проявляется проблема зависимости эффективности системы от безопасности и определенности доступа к решающей стороне (арбитру). Это выражается в том, что, учитывая особенности построения облачных структур, невозможно наверняка определить, к тому ли мы серверу аутентификации обращаемся. Возникает явная уязвимость подмены проверяющей стороны на стороннюю, управляемую злоумышленником. К тому же в ходе эксплуатации данной системы была выявлена проблема неустойчивости к атакам с воспроизведением пакетов. Собственно, чем и воспользовались злоумышленники в 2008 г. при атаке на сайты Amazon и eBay.

Решения на российском рынке облачных технологий также заставляют задуматься об эффективности их работы. Так как рассылка ключей безопасности через средства связи предыдущего поколения (почту, узлы междугородной связи) не соответствует ни должной скорости распространения информации, ни уровню обеспечения безопасности, так как ее соблюдение напрямую зависит от порядочности конкретных людей, занимающихся доставкой. Затем, существует уязвимость утраты ключа шифрования на физическом уровне (неаккуратное хранение присланного листа с напечатанным кодом доступа). Притом безопасность сеанса напрямую зависит от безопасности shttp-сессии, так как ключ безопасности вводится напрямую в веб-форму приложения, соответственно, появляется возможность проведения атаки на сторону пользователя с предварительным накоплением информации через сниффинг (ключ безопасности не остается постоянным на все время пользования). Также явным слабым местом является уязвимость атаки «человек посередине». Известны множество случаев подобных атак, в итоге, защищенность от них определяется заинтересованностью в их совершении со стороны злоумышленника, другими словами – вопрос времени.

К тому же оба этих подхода имеют значительный минус: для их функционирования необходимо обеспечить хранение массива ключей безопасности, как ресурсов доступа, так и каждого конкретного клиента. Соответственно, утрата конфиденциальности этого массива данных влечет за собой снижение эффективности обеспечения безопасности идентификации практически до нуля. Так, например, в 2009 г. сервис для хранения закладок Magnolia потерял все свои данные, в результате чего часть клиентов покинула сервис. К тому же необходимо учитывать, что подобные массивы занимают ресурсы облачных вычислений и при значительном расширении клиентской базы могут привести к увеличению


Клиент
Облако
Открытый ключ облака, Сертификат безопасности
Асимметричные ключи облака, Сертификат безопасности, База данных
Генерация случайного числа и его временной метки
Генерация асимметричных ключей клиента
Преобразование случайного числа односторонней функцией
Занесение сгенерированных данных в память клиент-приложения
Шифрование передаваемых данных, отправка открытого клиентского ключа
Расшифрование полученных данных,проверка целостности и авторства сообщения
Сообщение соответствует нормам?
нет
да
Сохранение открытого ключа клиента
Генерация временной метки ответного одностороннего преобразования
Выработка доказательств подлинности облака
Шифрование и отправка ответных данных
Расшифрование полученных данных,проверка целостности и авторства сообщения
Сообщение соответствует нормам?
нет
да
Выработка параметра проверки подлинности облака
1
2
3
4

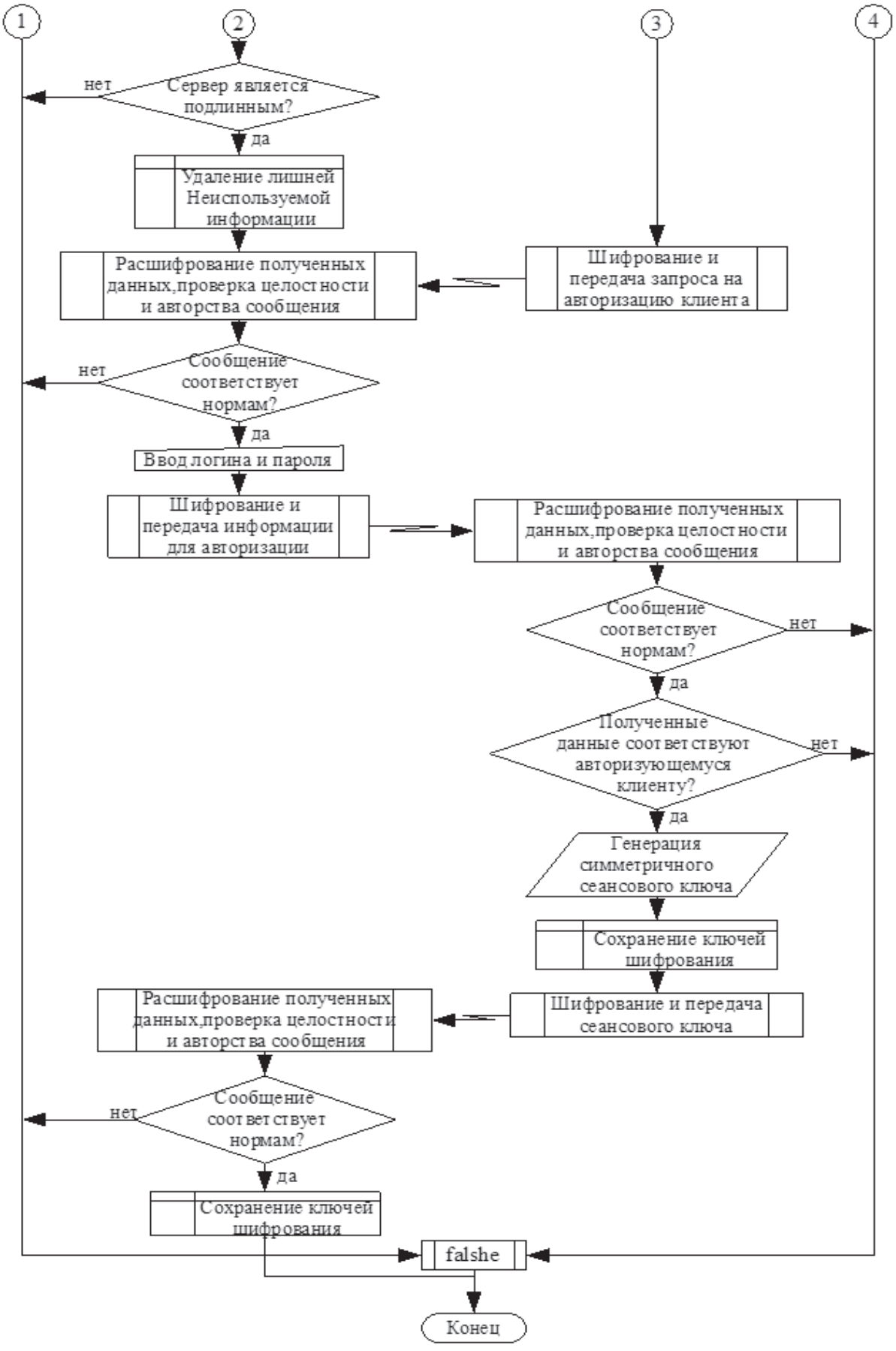


Рис. 1. Схема алгоритма защищенной аутентификации

времени на поиски и обработку данных массивов. Причем при учете российского опыта, когда один ключ прикрепляется на всегда за одним человеком, по сути, становясь своеобразным электронным паспортом, появляется проблема контроля и утилизации ключей клиента и, как следствие, ограниченности числа пользователей.

В связи с этим возникает потребность в разработке принципиально нового подхода к процедуре распознавания сторон, который должен обеспечить независимость каждой из них общения, гарантированность безопасности обмена данными, а также эффективность использования задействованных ресурсов. Также данная система должна учитывать и особенности новой облачной структуры: доступность контента с любого устройства, независимость от географической локации пользователя и ресурса, обеспечения равного качества обслуживания вне зависимости от метода входа в систему.

Данные задачи способен решать разрабатываемый метод аутентификации, использующий технологии VPN в канале между облачными вычислениями и конечным пользователем, с взаимной проверкой подлинности.

Данная модель проведения процедур базируется на принципе взаимонезависимости участвующих в процессе аутентификации сторон. Алгоритм взаимной проверки подлинности позволяет бороться с возможной неопределенностью участников сеанса связи в сети облачных вычислений. Это обеспечивается тем, что техническая база каждой стороны позволяет полноценно как проверить подлинность противоположной стороны, так и привести все необходимые доказательства своей легальности, что отсутствовало в предыдущих стандартах проведения подобных процедур.

Рассмотрим подробнее предлагаемый подход проведения операций идентификации сторон.

На начальном этапе клиент-приложение вырабатывает запрос на получение прав доступа к ресурсам облака. Для этого вырабатывается случайное число «R» по определенному алгоритму, прописанному в сертификате «X». Используя полученное число и текущее время, в системе вырабатываются асимметричные клиентские ключи шифрования, а также проводятся процедуры модификации случайного числа с использованием односторонних функций, указанных также в сертификате приложения для проведения процедуры проверки аутентичности сервера. Получив данные значения, клиент отправляет запрос на сервер, используя открытые ключи шифрования, прописанные в сертификате, с расстановкой временных меток, необходимых для предотвращения атак с задержкой сообщения при его ретрансляции. Сервер анализирует полученный запрос и высылает подтверждение своей подлинности, пересылая преобразованную по определенному алгоритму метку подлинности. Затем сервер запрашивает данные на подтверждения подлинности клиента. И клиент по организованному асимметричному каналу связи передает все необходимые данные для успешного завершения процедуры. После чего на сервере вырабатывается сеансовый ключ и высылается по тому же закрытому каналу. Причем асимметричные ключи могут использоваться для нанесения электронной цифровой подписи на пересылаемые сообщения. Если подобной необходимости нет, то данные ключи удаляются.

Благодаря защищенной аутентификации появляется возможность гибкого использования платформ выхода к облачным вычислениям, обеспечивается эффективность достоверного использования ресурсного пространства облачной структуры, а также вывод обеспечения безопасности обмена данных на более высокий уровень.

Обе стороны сеанса взаимодействия в облачной технологии являются независимыми и самодостаточными, способными как провести полноценную процедуру идентификации, так и предоставить всю необходимую информацию для подтверждения своей подлинности. Это позволяет снизить риски, связанные с подменой сторон, участвующих в определении идентичности.

К тому же асимметричность канала в процессе аутентификации и распределения сеансовых ключей ведет к увеличению уровня безопасности как самих процессов, так и сеанса связи в целом. Смена ключей шифрования с каждым новым сеансом также способствует уменьшению самих угроз перехвата ключа и снижает потери при его перехвате, так как он является действительным только до конца текущего сеанса.

Возможное увеличение времени процедур аутентификации и распределения ключей по сравнению с симметричными протоколами компенсируется тем, что предлагается автоматизация распространения и обновления ключей. Экономия требуемого объема памяти в облаке обеспечивается за счет создания одноразовых ключей шифрования, а не хранения громоздких баз ключей безопасности. А если учитывать, что последние тенденции в сетях передачи данных говорят о том, что пропускная способность каналов будет стремительно расти, данная проблема может стать неактуальной.

Предложенный алгоритм не имеет идеологической привязки к какому-либо алгоритму шифрования, поэтому он способен работать на любой платформе. Учитывая современный интерес российских компаний к системам, использующим российские протоколы шифрования, данное решение может обеспечить реальную техническую базу для внедрения и использования на отечественном рынке своих систем безопасности. К тому же простота алгоритма должна сказаться на удобстве его обслуживания и контроля в лучшую сторону.

Главными достоинствами данного алгоритма являются:

- универсальность использования стандартов шифрования;
- независимость идентифицирующихся сторон сеанса связи в облаке;
- динамичность изменения одноразовых ключей безопасности;
- безопасность распределения ключей;
- экономия ресурсов облака для хранения обслуживающей информации.

Литература

1. Емельянова Ю.Г., Фраленко В.П. Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления // Программные системы: теория и приложения. №8, 2011. – С. 17-31.
2. Кондрашин М. Безопасность облачных вычислений // Storage News. №1 (41), 2010. www.storagenews.ru
3. Патент PCT/US2007/088475 от 20.12.2007 Microsoft Corporation.
4. De Lutiis P., Di Caprio G., Moiso C. PCT Patent 2005/107204, 04.05.2005.
5. Кузнецов М.В., Ротенштейн И.В., Чигирь Р.В. Информационная безопасность в облачных вычислениях // Материалы XIII МНТК «Проблемы техники и технологии телекоммуникаций». Изд. УГАТУ. Уфа, 2012. – С. 244-246.

THE ALGORITHM SECURE AUTHENTICATION WHEN USING CLOUD COMPUTING

Kuznetzov M.V., Chigir R.V.

In the article the aspects of information security in the use of technologies of cloud computing, revealed the vulnerability of the client connection and proposed a new algorithm for secure authentication.

Keywords: *cloud computing, the vulnerability of the client, mutual authentication, secure authentication, «Kerberos», VPN.*

Кузнецов Михаил Владимирович, к.т.н., доцент Кафедры систем связи Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел. 8-927-6527894. E-mail: mv.kuz-netsov@yandex.ru

Чигирь Роман Викторович, студент 5 курса ПГУТИ. Тел. 8-927-603-20-38. E-mail: rwch63@mail.ru

УПРАВЛЕНИЕ И ПОДГОТОВКА КАДРОВ ДЛЯ ОТРАСЛИ ИНФОКОММУНИКАЦИЙ

УДК 316.334

ВЗАИМОДЕЙСТВИЕ ВУЗОВ САМАРСКОЙ ОБЛАСТИ С КОМПАНИЯМИ, РЕАЛИЗУЮЩИМИ ПРОГРАММЫ ИННОВАЦИОННОГО РАЗВИТИЯ, НА ПРИМЕРЕ ПГУТИ И ОАО «РОСТЕЛЕКОМ»

Заманова О.В., Каменев В.А., Каменев Е.А., Табаков К.В.

Рассматриваются вопросы формирования и реализации программ инновационного развития, осуществляющих компаниями с государственным участием. Приводятся показатели реализации данной программы на примере ОАО «Ростелеком» и Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ).

Ключевые слова: программа инновационного развития, НИОКР, целевая подготовка

Введение

Формирование и реализация программ инновационного развития (далее – ПИР) осу-