УДК 004.77
ББК 32.973.202
Д 58

Довгаль В.А.
Кандидат технических наук, доцент кафедры автоматизированных систем обработки информации и управления инженерно-физического факультета Адыгейского государственного университета, Майкоп, тел. (8772) 59-39-11, e-mail: urmia@mail.ru

Особенности реализации безопасного подключения к «облачным» сервисам

(Рецензирована)

Аннотация. *Рассматриваются безопасные методы подключения к «облачным» сервисам как отдельных пользователей, так и отдельных компаний. Проведен анализ услуг типа «инфраструктура как сервис» (IaaS), предоставляемых хостинг-провайдерами, а также решений для подключения отдельных клиентов и компаний. Предлагается комплекс мероприятий, применяемый для обеспечения проблемы безопасности подключения, предотвращения угроз безопасности в «облаках» и обеспечения необходимого уровня безопасности информации.*

Ключевые слова: *«облачные» технологии, услуг типа «инфраструктура как сервис» (IaaS), методы подключения к «облачным» сервисам с предотвращением угроз информации.*

Dovgal V.A.
Candidate of Technical Sciences, Associate Professor of Department of Automated Systems of Processing Information and Control of Engineering-Physics Faculty, Adyghe State University, Maikop, ph. (8772) 59-39-11, e-mail: urmia@mail.ru

Features of realization of safe connection to «cloudy» services

Abstract. *The paper discusses the safe methods of connection to «cloudy» services of both certain users and separate companies. The analysis of granting services of the type of «infrastructure as service» (IaaS) presented by hosting providers and decisions for connection of certain clients and companies is carried out. The complex of actions applied to provide safety of connection, prevention of threats to security in «clouds» and ensuring necessary level of safety of information is offered.*

Keywords: *«cloudy» technologies, services of the type of «infrastructure as service» (IaaS), methods of connection to «cloudy» services with prevention of threats to information.*

Тренд последнего времени в области хранения данных предприятием – перенос собственной ИТ-инфраструктуры на сторону хостинг-провайдера, предоставляющего услуги «облачных» сервисов. Первоочередное требование заказчика состоит не только в гарантированной возможности доступа к ресурсам и приложениям в любой момент времени, но и в безопасном использовании собственной информации. Порождаемый пользователями «облачного» подхода спрос заставляет хостеров задуматься о предоставлении услуги типа «инфраструктура как сервис» (Infrastructureas a Service, IaaS), которая активно внедряется в мире [1]. IaaS, как новая технология и модель обслуживания, способна изменить деятельность компаний и стать важнейшим стимулом инноваций и сокращения текущих расходов. В соответствии с ней серверы и другие ресурсы предоставляются по мере необходимости через «облако», обеспечивая самообслуживание и доступ к ИТ-ресурсам по запросу. В результате создание необходимых инструментов разработчиками может занимать очень короткий промежуток времени (минуты или часы).

Модель IaaS отличается от традиционного порядка применения информационных технологий, открывая перед компаниями новые возможности использования сервисов. Компании любого масштаба могут получить доступ к самым современным центрам обработки данных (ЦОД), защищенным серверам и высокопроизводительным системам хранения. При этом компания может не тратить средства на создание инфраструктуры.

Основные преимущества модели IaaS:

1. Унифицированная система управления. IaaS предоставляет единый интерфейс управления вместо множества систем, требующих мониторинга и контроля. В результате увеличиваются эффективность и надежность частных и общественных «облачных» сред;

2. Сервисы по запросу. Модель IaaS позволяет компаниям изменять набор используемых сервисов в зависимости от уровня эффективности их деятельности в то или иное время (при значительном росте бизнеса могут возрастать потребности в сервисах);

3. Взаимная совместимость. Поддержка моделью IaaS любого количества платформ (виртуальных, физических или «облачных»), в отличие от традиционных ИТ-поставщиков, обычно использующих ряд патентованных систем. При смене провайдера в этом случае трудностей, как правило, не возникает.

Использование IaaS ослабляет зависимость от конкретного производителя и уменьшает связанные с этим сложности. Кроме того, у предприятий отпадает необходимость создавать у себя новую инфраструктуру, обеспечивать ее защиту и налаживать управление, направляя все ресурсы на развитие инноваций.

Как правило, к «облачному» сервису подключаются как отдельные пользователи, так и отдельные компании, уже располагающие собственной локальной инфраструктурой. Поэтому имеет смысл рассмотреть задачу подключения с двух сторон, уделяя внимание возможным способам, вариантам и инструментам. Отдельный акцент необходимо сделать на обеспечение проблемы безопасности подключения.

Подключение конечных пользователей к «облачным» сервисам

В качестве конечных пользователей можно рассматривать не только индивидуальных клиентов, но и отдельные мелкие и даже средние компании, которые не имеют своей локальной ИТ-инфраструктуры. Они предпочитают разворачивать все необходимые для бизнеса решения и сервисы в «облаке» IaaS-провайдера. Такой подход экономически оправдан, выгоден и удобен, хотя и требует выбора соответствующего метода подключения.

Как правило, для подключения к «облачным» сервисам конечными пользователями применяются комбинации различных решений. Наиболее распространенными являются [2]:

- RDP-клиент;
- RemoteApp;
- Веб-доступ;
- RemoteAccess VPN;
- VPN site-to-site;
- DirectAccess;
- VDI.

Выбор того или иного инструмента удаленного подключения зависит непосредственно от практических потребностей конкретного клиента, сотрудника или отдела. Веб-интерфейс будет удобен таким специалистам, как бухгалтеры, аналитики, маркетологи. Разработчикам или тестировщикам приложений, ERP-консультантам вполне подойдет вариант RDP-подключения или что-то другое. Выбор зависит от направления деятельности пользователей или мелкой компании.

1). Подключение посредством удаленного рабочего стола (RDP-клиент) – наиболее распространенный, удобный, универсальный и часто используемый инструмент, предоставляющий возможность удаленного доступа к рабочему месту, в том числе развернутому и в «облаке».

Его основой является Remote Desktop Protocol (RDP) – проприетарный протокол прикладного уровня, обеспечивающий удаленную работу пользователя с компьютером,

на котором выполняется сервис терминального доступа. RDP-клиенты разработаны для всех часто используемых в бизнесе операционных систем (ОС).

Данное решение позволяет дополнительно конфигурировать параметры клиента удаленного рабочего стола. Пользователь может сохранить идентификационные данные, чтобы при подключении не вводить их каждый раз заново. Хотя политики безопасности, применяемые на предприятиях, этого делать не рекомендуют. Кроме того, можно настроить параметры экрана, раскладки клавиатуры, звуков проигрывания и прочее.

Со стороны сервис-провайдера выдвигается требование наличия выделенного сервера терминалов (Terminal Server). Подключение конечного пользователя осуществляется запуском программы клиента RDP в одной из используемых операционных систем, с помощью которой пользователь подключается к серверу терминалов и видит рабочий стол удаленной системы. В рамках установленного соединения пользователь может запускать развернутые на сервере терминалов приложения.

Настройки, выбираемые по умолчанию при подключении по RDP, при реализации удаленного доступа используют слабое шифрование, делая возможным перехват и расшифровку трафика. Повысить безопасность и оптимизировать RDP позволит только применение дополнительных технологий [3]. Как пример – технология Remote Desktop Gateway (шлюз удаленных рабочих столов), позволяющая удаленным авторизованным пользователям подключаться как к ресурсам физической сети предприятия, так и к сети в «облаке» IaaS-провайдера. Она использует RDP-протокол поверх протокола HTTPS, гарантируя при этом безопасное соединение с обеспечением надежного метода шифрования между удаленными пользователями Интернета и ресурсами в «облаке», необходимыми для работы пользовательских приложений.

2). Инструмент RemoteApp (удаленные приложения служб терминалов) является разновидностью рассмотренного выше RDP-клиента. Но в отличие от него, RemoteApp позволяет организовать удаленный доступ к установленным приложениям на сервере в «облаке».

RDP-клиента дает возможность использовать приложения, эмулируя их локальную установку – пользователь видит рабочий стол, программы, ярлыки, панель управления и прочее (иллюзия работы с экземпляром операционной системы). RemoteApp предоставляет пользователю доступ только к запущенному удаленному приложению в рамках своего физического устройства.

Например, клиент запускает ярлык редактора Microsoft Word, расположенный на рабочем столе своего локального компьютера, после чего инициируется процесс проверки подлинности (хотя редактор не установлен на локальной станции пользователя). Успешная аутентификация (авторизация) позволяет запустить приложение, которое «публикуется» на удаленном сервере. В свою очередь RemoteApp осуществляет подключение к удаленному серверу. Таким образом, формируется RDP-сессия, после чего стартует и запускается само приложение без возможности отображения удаленного рабочего стола. Этот процесс для пользователя создает эффект локальной установки приложения.

Применение RemoteApp актуально в случаях, когда:

- необходимо ограничить доступ к конкретным приложениям;
- совмещена работа пользователя на локальной машине с использованием какого-то приложения, вынесенного в «облако»;
- приложение должно быть доступно в специфических условиях и при низкой скорости Интернета.

Со стороны сервис-провайдера выдвигается требование наличия сконфигурированного RD Session Host Server с размещенным на нем списком соответствующих про-

грамм (Remote App Programslist). Именно из этого списка выполняется подключение конечного пользователя запуском сконфигурированного rdp-файла для инициирования подключения к приложению по RDP. Как вариант возможен запуск ярлыка приложения с рабочего стола или меню Пуск для инициирования подключения к приложению по RDP (из списка Remote App Programslist).

Со стороны пользователя запускаемые удаленные приложения служб терминалов выглядят так, как если бы они исполнялись непосредственно в системе пользователя. При этом приложения интегрируются в рабочий стол системы пользователя с масштабированием окна и собственным значком приложения в панели задач.

3). Веб-доступ к службам терминалов позволяет организовать доступ к определенным приложениям и рабочим столам в «облаке» (как в ранее рассмотренных вариантах) с помощью браузера, который установлен на подавляющем большинстве вычислительных устройств. Для пользователя такой вариант выглядит следующим образом: он запускает браузер, вводит необходимый адрес, проходит проверку подлинности, а далее работает с «опубликованным» приложением (приложениями) или удаленным рабочим столом (столами), получая доступ к приложениям или удаленному рабочему столу средствами web. При этом ярлыки приложений размещаются на предварительно настроенной веб-странице.

Со стороны сервис-провайдера выдвигается требование наличия выделенного сервера терминалов (Terminal Server). Как пример, операционная система Windows Server 2008/2012 + служба TS WebAccess. Подключение конечного пользователя осуществляется по URL для доступа к ресурсу посредством веб-браузера.

Еще одним из возможных вариантов подключения к «облачным» сервисам является Virtual Private Network (VPN) – виртуальная частная сеть, позволяющая обеспечить одно или несколько надежных сетевых соединений поверх сети Интернет, используя при этом различные средства криптографии.

Существует два типа VPN-туннелей: Remote Access VPN и Site-to-site VPN, на которых основаны следующие два решения.

4). Remote Access VPN – удобный, безопасный и достаточно часто используемый инструмент подключения к ресурсам «облака», создающий надежный и защищенный туннель между приложением на компьютере клиента и каким-либо устройством (например, VPN-концентратором, маршрутизатором, Cisco ASA и т.п.), расположенном в облаке хостинг-провайдера.

Со стороны сервис-провайдера выдвигается требование наличия сконфигурированного VPN-устройства (сервера). Со стороны клиента для подключения требуется:

- наличие интернет-подключения;
- запуск ярлыка для подключения к VPN-серверу, после установки которого реализуется доступ к ресурсам компании.

Со стороны пользователя работа решения выглядит следующим образом: на стороне клиента устанавливается исходящее VPN-подключение, которое пользователь использует по необходимости. Для реализации доступа к удаленному ресурсу пользователь запускает ярлык VPN, вводит свою идентификационную информацию и при успешной проверке подлинности получает доступ к необходимым ресурсам. Иными словами, компьютер пользователя за счет выданных при VPN-подключении параметров IP-конфигурации попадает в сеть виртуального удаленного офиса в «облаке» и может использовать ресурсы так, как если бы он находился непосредственно в офисе компании.

5). Site-to-site VPN – решение, устанавливающее туннель между двумя устройства (например, VPN Server 1 и VPN Server 2, изображенными на рисунке 1). В этом случае пользователи находятся за устройствами, в локальных сетях, и на их компьютерах не требуется установка какого-либо специального программного обеспечения.

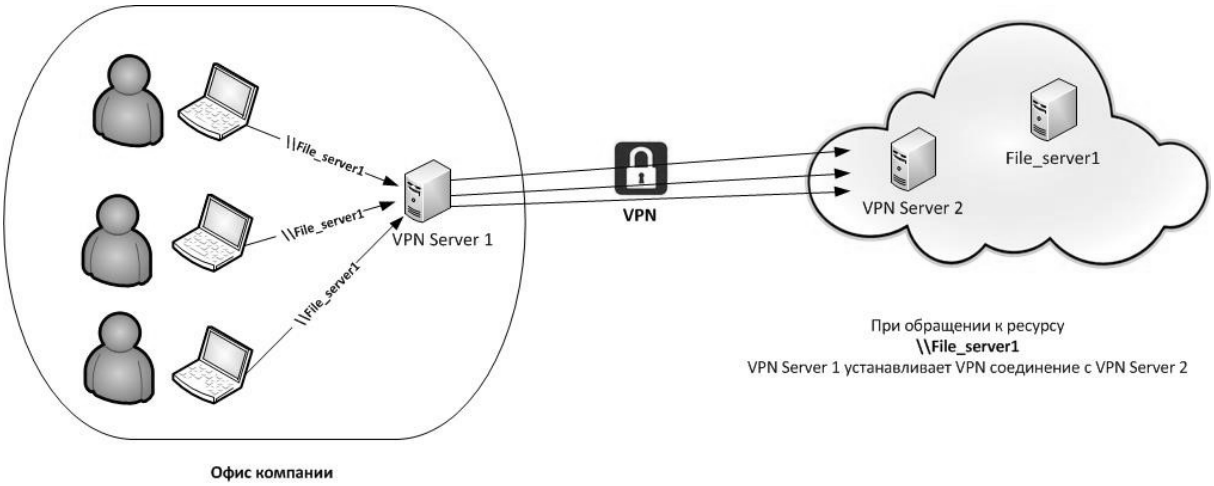

Рис. 1. Пример реализации Site-to-Site VPN-соединения

Подключение Site-to-Site VPN на уровне VPN-сервера в «облаке» и VPN-сервера в офисе компании рекомендуется использовать в компании, имеющей значительное число сотрудников, которым необходим доступ к ресурсам файлового сервера. Для этого в офисе компании необходимо дополнительно развернуть VPN-сервер, а выглядеть процесс доступа к ресурсам файлового сервера будет так, как показано на рисунке 1.

В таком сценарии пользователь обращается к ресурсу в «облаке» напрямую. В нашем примере к ресурсу \\ File_server1 в подсети «облака» при таком обращении VPN Server 1 устанавливает VPN-соединение с сервером VPN Server 2 в «облаке», после чего пользователь видит содержимое запрашиваемого ресурса. На стороне клиента при этом отпадает необходимость создания исходящего VPN-подключения. Такая конфигурация носит название Site-to-Site VPN.

Со стороны сервис-провайдера выдвигается требование наличия двух сконфигурированных VPN-серверов (например, VPN-сервер в компании и VPN-сервер в «облаке»). При подключении конечного пользователя нет необходимости создавать и запускать ярлык VPN-подключения – обращение к ресурсам филиала, головного офиса, «облака» осуществляется напрямую. При обращении к ресурсам VPN-подключение организуется автоматически на уровне серверов и является прозрачным для конечного пользователя.

6). DirectAccess – новая технология, позволяющая реализовать возможность удаленного доступа к ресурсам и корпоративной сети и к ресурсам Интернета сразу же после подключения компьютера пользователя к сети Интернет. То есть пользовательский компьютер, сконфигурированный в качестве клиента DirectAccess, автоматически устанавливает туннель до сервера DirectAccess и через него получает доступ ко всей корпоративной сети. При этом от пользователя не требуется никаких дополнительных действий.

Технология DirectAccess устанавливает туннель между клиентом и сервером автоматически и прозрачно для пользователя. Не требует запуска каких-либо VPN-соединений, ввода учетных данных. Если связь с Интернетом на какое-то время теряется (туннель в это время разрывается), а затем восстанавливается, то опять же автоматически, без участия пользователя восстанавливается и туннель в корпоративную сеть.

Со стороны сервис-провайдера выдвигаются следующие требования:

- наличие одного или более серверов DirectAccess в составе домена;
- наличие центра сертификации (PKI);
- Windows-инфраструктура.

Для подключения конечного пользователя, кроме отсутствия необходимости в создании и запуске ярлыка подключения, также выдвигается ряд требований:

• список клиентских операционных систем, к которым возможно подключение, к сожалению, ограничен;

• компьютер клиента должен входить в состав домена;

• физическое местоположение клиента не имеет значения.

7). VDI (Virtual Desktop Infrastructure, виртуализация рабочих столов) – виртуальная инфраструктура рабочих столов, позволяющая централизовать рабочие станции пользователей на серверах виртуализации, создав при этом единую точку управления, развертывания и обслуживания. Данная технология реализована на многих «облачных» площадках корпоративных IaaS-провайдеров, что обусловлено требованием высокой мобильности бизнеса, а значит постоянной доступности приложений для сотрудников.

Со стороны клиента для обеспечения доступа к своему виртуальному рабочему месту необходимо только наличие интернет-соединения и настольного ПК (как вариант – ноутбука, мобильного телефона или планшета).

На практике виртуализация рабочих столов сводится к выделению сервера в «облаке» IaaS-провайдера, на который устанавливается гипервизор. На нем, в свою очередь, разворачиваются отдельные виртуальные машины с установленными на них клиентскими операционными системами. На конечном устройстве пользователя запускается программа-клиент и происходит подключение к инфраструктуре.

Такая схема подключения очень похожа на RDP-подключение. Однако RDP-подключение к терминальному серверу является отдельной сессией на общем сервере Windows. VDI представляет собой отдельный изолированный контейнер с клиентской ОС. Таким образом, можно выделить два ключевых отличия: серверная ОС против клиентской и отдельная сессия, разделяющая ресурсы одной ОС, против изолированной виртуальной машины.

При работе в терминальном режиме изоляция происходит на уровне сессии, и если приложение вызывает сбой на уровне самой ОС, то вместе с пользователем, запустившим такое приложение, перезагрузятся и остальные пользователи, работающие на этом же сервере. А при использовании виртуализации рабочих столов перезагружена будет только одна виртуальная машина.

Со стороны сервис-провайдера выдвигается требование наличия развернутой инфраструктуры виртуальных рабочих столов VDI. Как пример, это решения от VMware, Citrix, Microsoft. Пользователь получает свой собственный виртуальный ПК, к которому можно подключаться с помощью тонкого клиента, настольного ПК, ноутбука, планшета или смартфона.

Предложенные варианты подключения к «облачному» сервису отдельных пользователей позволят обеспечить эффективное использование хранимой в «облаке» информации с обеспечением высокого уровня безопасности.

Подключение локальной инфраструктуры компании к IaaS-инфраструктуре в «облаке»

Кроме рассмотренных выше вариантов подключения конечных пользователей к «облачным» сервисам, возникают и задачи подключения уже существующей локальной инфраструктуры компании к IaaS-инфраструктуре «облака». В этом случае также существует выбор из нескольких технологий.

Предположим, существует некая компания, располагающая набором собственных серверов, которых недостаточно для запуска нового проекта, требующего достаточно больших вычислительных мощностей и ресурсов. Для покупки нового оборудования компании недостает финансовых средств, и тогда выходом из сложившейся ситуации можно считать подключение локальной инфраструктуры компании к «облачной» инфраструктуре. Затратив незначительное количество финансовых ресурсов, компания получает единое сетевое пространство, удовлетворяющее требованиям реализуемого проекта.

Эффективными решениями для данного примера представляются следующие варианты:

- аренда выделенного канала и подключение к ЦОД для доступа к «облаку»;
- проброс своего кабеля до ЦОД;
- использование точек обмена трафиком.

Рассмотрим каждый из вариантов более подробно.

1). Аренда выделенного канала и подключение к ЦОД для доступа к «облаку»2 подразумевает прямое соединение внутренней сети заказчика с сетью в «облаке» IaaS-провайдера (см. рис. 2). Ввиду совместного использования собственных устройств компании и IaaS-провайдера часто его называют гибридным «облаком».

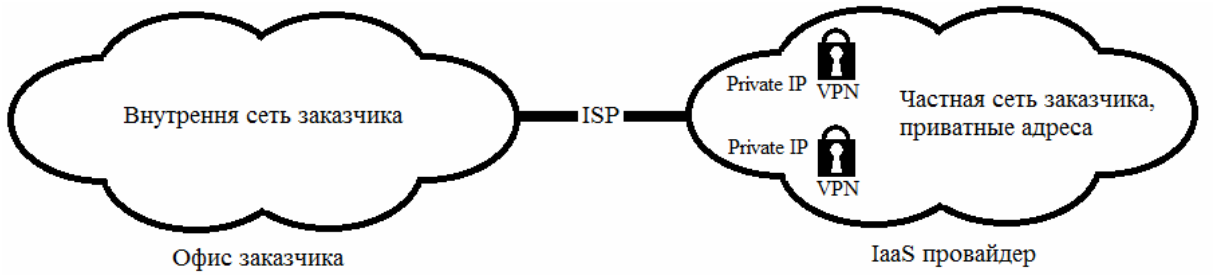

Рис. 2. Пример сценария с выделенным ISP-каналом для доступа к ЦОД в «облаке»

Для реализации такого решения обычно используются каналы связи «точка – точка», физически реализующиеся в виде нескольких выделенных каналов провайдера (а лучше нескольких независимых провайдеров), работающих в режиме автоматического переключения в случае падения одного из них.

Как правило, канал связи предоставляется на основе собственной оптоволоконной сети провайдера с возможностью подписания соглашения об уровне обслуживания, регламентирующего гарантии соблюдения технических характеристик канала. Достоинство такого метода: относительная дешевизна по сравнению с использованием заказчиком собственного кабеля. При этом провайдер, как правило, дает гарантию высокой плотности покрытия, а также безопасности и надежности арендуемых каналов, включая возможность резерва емкости при росте канала.

2). Прокладка своего кабеля до ЦОД подразумевает соединение внутренней сети заказчика и ЦОД назначения собственным кабелем. Такой вариант обычно выбирают компании, которые предъявляют повышенные требования к безопасности и эксплуатационным показателям канала связи.

3). Использование точек обмена трафиком – это способ подключения, при котором кабель прокладывается не до ЦОД «облачного» провайдера напрямую, а до коммутационного оборудования, размещенного IaaS-провайдером на площадках, где располагаются точки обмена трафиком.

Точка обмена трафиком – это место прямого обмена трафиком между интернет-операторами без использования сети сторонних провайдеров. Все ее участники имеют возможность построить соединения друг с другом, задействовав при этом лишь один порт. Благодаря прямым пирингам через точку обмена можно в разы уменьшить загрузку внешних каналов и сократить время передачи данных между участниками.

Большинство корпоративных IaaS-провайдеров размещают собственное сетевое оборудование на этих площадках, что значительно упрощает процесс подключения клиентов к «облачным» ресурсам дата-центров таких поставщиков.

Достоинством такого решения является простота и низкая стоимость прокладки кабеля клиентом. Недостатки – ограниченое количество крупных и известных площадок, где размещаются точки обмена трафиком. Особенно в регионах России.

Таким образом, применение предложенных вариантов и способов подключения к корпоративному «облаку» как со стороны конечного пользователя, так и со стороны организации в целом повышает эффективность использования потока данных, передаваемых между заказчиком и провайдером «облачных» сервисов, и снижает вероятность нарушения конфиденциальности, целостности и доступности данных. Важным является наличие нескольких вариантов, позволяющее конкретному клиенту подобрать наиболее подходящий метод и способ подключения.

Примечания:

1. Что такое IaaS = Что такое_IaaS. URL: http://www.tadviser.ru/index.php
2. Юдина Е. Подключение к корпоративному облаку. URL: http://iaas-blog.it-grad.ru/podklyuchenie-k-korporativnomu-oblaku
3. Довгаль В.А. Методы повышения безопасности в сфере «облачных» технологий // Вестник Адыгейского государственного университета. Сер. Естественно-математические и технические науки. 2014. Вып. 4 (147). С. 170-174. URL: http://vestnik.adygnet.ru

References:

1. What is IaaS = What is_IaaS. URL: http://www.tadviser.ru/index.php
2. Yudina E. Connection to a corporate cloud. URL: http://iaas-blog.it-grad.ru/podklyuchenie-k-korporativnomu-oblaku
3. Dovgal V.A. Methods of safety increase in the sphere of «cloud» technologies // The Bulletin of the Adyghe State University. Ser. Natural-Mathematical and Technical Sciences. 2014. Iss. 4 (147). P. 170-174. URL: http://vestnik.adygnet.ru