5. Mery zashchity informatsii v gosudarstvennykh informatsionnykh sistemakh [Measures for protection of information in government information systems]. *Metodicheskiy dokument FSTEK Rossii: utv. FSTEK Rossii 11.03.2014* [Methodological document the FSTEC of Russia: appr. The FSTEC of Russia 11.03.2014]. Moscow, 2014, pp. 176.
6. Rossiyskaya Federatsiya. Prikazy. Ob utverzhdenii trebovaniy po zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh [of The Russian Federation. The orders. Approval requirements for protection of information, not state secrets contained in the state information systems] *[prikaz FSTEK Rossii №17: izdan FSTEK Rossii 11.03.2013]* [the order of the FSTEC of Russia No. 17: published by the Russian FSTEC 11.03.2013]. 1st ed. Moscow, 2013, pp. 37.
7. Rossiyskaya Federatsiya. Prikazy. Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh [of The Russian Federation. The orders. On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in information systems of personal data] *[prikaz FSTEK Rossii №21: izdan FSTEK Rossii 18.03.2013]* [the order of the FSTEC of Russia No. 21: published by the Russian FSTEC 18.03.2013]. 1st ed. Moscow, 2013, pp. 20.
8. *Boytsov I.V.* Kak zashchitit' virtual'nuyu infrastrukturu po trebovaniyam FSTEK [How to protect virtual infrastructure requirements FSTEC], *Informatsionnaya bezopasnost'* [Information Security], 2014, No. 1, pp. 30-32.
9. *Lapshin S.V., Konyavskaya S.V.* Zashchita sistem virtualizatsii [Protection systems virtualization], Informatsionnaya bezopasnost' [Information Security], 2010, No. 6, pp. 34-35.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Курносов Кирилл Викторович – НГУЭУ; e-mail: kursorkvk@mail.ru; 630099, г. Новосибирск, ул. Каменская, 52/1; тел.: 89137532181; кафедра информационной безопасности; студент.

Селифанов Валентин Валерьевич – e-mail: sfo1@mail.ru; тел.: 83832640484; кафедра информационной безопасности; старший преподаватель; начальник 6 отдела Управления ФСТЭК России по Сибирскому федеральному округу.

Kurnosov Kirill Viktorovich – Novosibirsk State University of Economics and Management; e-mail: kursorkvk@mail.ru; 52/1, Kamenskaya street, Novosibirsk, 630099, Russia; phone: +79137532181; the department of information security; student.

Selifanov Valentin Valer'evich – e-mail: sfo1@mail.ru; phone: +73832640484; the department of information security; senior lecturer; head of the 6th Department FSTEC of Russia in SFD.

УДК 004.057.4

А.М. Максимов, Е.Н. Тищенко, О.В. Серпенинов

РАССМОТРЕНИЕ HTTP-ЗАГОЛОВКА СТАНДАРТА ДЕ-ФАКТО X-FORWARDED-FOR КАК ЭЛЕМЕНТА, СПОСОБСТВУЮЩЕГО ОСУЩЕСТВЛЕНИЮ НСД К ВЕБ-РЕСУРСАМ

Рассмотрен один из аспектов функционирования современных компьютерных сетей – заголовки протоколов. Проведен краткий анализ документов, в которых представлены стандарты, регулирующие функционирование рассматриваемого протокола HTTP в сети Интернет. В частности, сделан анализ нестандартного заголовка для протокола HTTP – X-Forwarded-For. Данный заголовок является стандартом де-факто, что отражено и в документах, описывающих и регламентирующих его использование. Произведён краткий обзор распространённости платформ, которые поддерживают использование означенного заголовка. В результате анализа с точки зрения безопасности установлено наличие рис-

ка использования заголовка X-Forwarded-For. Риск представляет собой возможность осуществления несанкционированного доступа (НСД) с повышенными привилегиями к запрашиваемому ресурсу. Помимо этого рассмотрена ситуация, когда данная возможность осуществления НСД с использованием указанного заголовка может быть реализована (в том числе ситуации, когда происходит взаимодействие компонентов различных уровней (веб-сервер и веб-приложение). Ситуация включает в себя рассмотрение случаев с использованием стандартных средств (таких, как прокси, балансиры нагрузки) при доступе к сети Интернет. По результатам исследования сформулированы некоторые положения, позволяющие уменьшить вероятность реализации обнаруженной угрозы.

Ввеб-сервер; X-Forwarded-For; HTTP-заголовок; REMOTE_ADDR.

A.M. Maximov, O.V. Serpeninov, E.N. Tischenko

REVIEW OF DE FACTO STANDARD X-FORWARDED-FOR HTTP-HEADER AS ELEMENT CONDUCTIVE TO UNAUTHORIZED ACCESS TO WEB RESOURCES

The article contains review one of functioning aspects of modern networks – headers. Review includes short analysis of documents, which describe standards and functioning of HTTP-headers. In particular, X-Forwarded-For HTTP-header was considered. Also there was reviewed importance of the proper use of headers due to wide presence of platforms with X-Forwarded-For HTTP-header support. As a remark there was a brief overview of market part of most popular web-servers. The presence of risk in case of the X-Forwarded-For de facto standard header use was determined. Threat realization allows getting unauthorized access with elevated privileges to the target system. Beside this, case when X-forwarded-For header represents the unauthorized entry point, was also considered. Reviewed cases also include situation analysis when standard resource (like proxy, load balancers) are used and situation of several independent parts (like web application and web server) complex functioning. In conclusion, some affirmations, based on obtained result, were formulated to reduce chances of system penetration.

Web-server; X-Forwarded-For; HTTP-header; REMOTE_ADDR.

Используемые в настоящее время протоколы передачи данных регламентированы различными документами. Большинство таких документов имеют название RFC (англ. *request* for Comments – тема для обсуждения) и номер и публикуются организацией IEFT (англ. Internet Engineering Task Force – Инженерный совет Интернета). При этом данные документы могут разрабатываться под эгидой научных, общественных и интернет-организаций. Помимо смысловой нагрузки аббревиатуры, RFC рассматривается именно как стандарт для сети Интернет и охватывает подавляющее число параметров, так или иначе связанных с её функционированием. Однако не исключено существование некоторых свойств, не описанных в RFC. Более того, такие свойства действительно существуют. Одним из таких стандартов де-факто является проект стандарта, описывающий поле заголовка X-Forwarded-For (XFF) протокола HTTP [1].

Данный заголовок поддерживается большинством распространённых продуктов и устройств, реализующих функции прокси-серверов [2, 3], кэширования, балансировки нагрузки [4, 5], веб-серверов и т.д. Среди перечисленного особенно примечателен класс веб-серверов, поскольку он представлен небольшим перечнем наименований, и при этом программные продукты, входящие в данный класс программного обеспечения, поддерживают стандарт X-Forwarded-For (здесь и далее под веб-сервером будет пониматься программная платформа, обеспечивающая функционирование веб-ресурса, или веб-приложения; под веб-приложением (или веб-ресурсом) подразумевается некий код, выполнение которого даёт пользователю конечный результат (т.е. веб-сайт, портал, отдельная веб-страница и т.д.)).

Поддержка присутствует в таких продуктах, как Apache, Microsoft IIS, Nginx. Ежемесячные исследования, проводимые порталом Netcraft.com, по состоянию на 6 июня 2014 года показали следующую статистику: среди 968 882 453 исследованных сайтов, 36,50 % используют веб-сервер Apache, 36,35 % – веб-сервер Microsoft IIS, 13,81 % – веб-сервер Nginx. Таким образом, на долю трёх перечисленных платформ приходится 86,66 % исследованных сайтов [6].

Заголовок X-Forwarded-For используется для идентификации оригинального IP-адреса клиента, который подключается к веб-серверу посредством прокси-сервера или через балансир нагрузки. В ряде случаев для корректной работы веб-приложения или портала бывает необходимо однозначно определить источник клиентского подключения. Однако в точке назначения в качестве исходного адреса подключения будет виден адрес последнего прокси-сервера или балансира нагрузки, через которое подключение прошло. Этот факт может препятствовать нормальному функционированию ресурса для определённых пользователей, если окажется, что все они используют одну точку подключения в виде прокси-сервера или балансира нагрузки. Фактически такая ситуация наблюдается и при использовании технологии NAT (трансляция адресов), и соответственно возникает точно такая же проблема (обсуждение которой проходит в рамках документа RFC6269) [7]. Наглядно взаимодействие всех описанных компонентов показано на рис. 1.

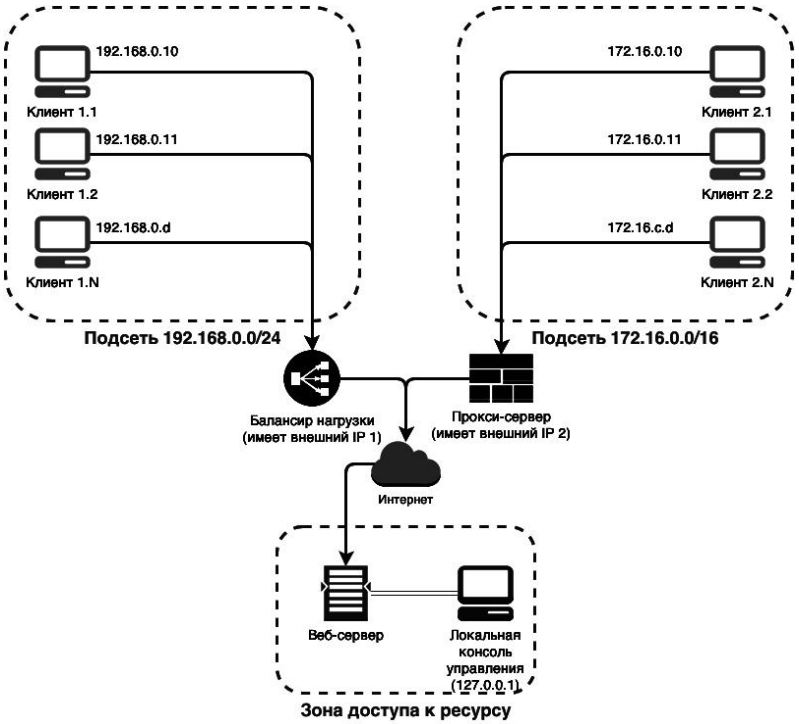

Рис. 1. Взаимодействие клиентов с конечным ресурсом с использованием прокси-сервера, балансира нагрузки

Если предположить, что в описанной схеме не используются заголовки типа X-Forwarded-For, то для веб-сервера все пришедшие подключения из сети Интернет будут представлены исключительно внешними IP-адресами. Фактически возникает ситуация, когда весь набор, состоящий из N клиентов частной подсети

(здесь и далее для удобства описания используется формат бесклассовой адресации сети) 192.168.0.0/24 и подключающийся посредством балансира нагрузки, будет выглядеть для веб-сервера как один и тот же клиент с внешним IP-адресом 1. Аналогичная ситуация возникает и в случае использования прокси-сервера. В приведённом примере подключения со всех N клиентов подсети 172.16.0.0/16 будут видны для веб-сервера как множественные подключения одного и того же клиента с внешним IP-адресом 2.

При использовании заголовков типа X-Forwarded-For, веб-сервер имеет возможность определять не только внешний IP-адрес, но и частный адрес клиента. Комбинация этих значений позволяет однозначно определить, кто из клиентов внутри частной подсети осуществляет доступ к веб-серверу. Данное утверждение справедливо, поскольку внешние IP-адреса уникальны и их существует достаточно ограниченное число.

Несмотря на то, что частные адреса не уникальны в принципе, они не повторяются в рамках одной подсети, находящейся за устройством с внешним IP-адресом. Именно по этой причине комбинация «уникальный внешний IP – частный IP» является неповторяющейся. Утверждение перестаёт быть справедливым в случае использования нескольких последовательно подключённых устройств типа балансира нагрузки или прокси-сервера. В таком случае конечный результат зависит от конфигурации промежуточных узлов.

Практической пользой применения заголовка является ситуация блокирования атак типа DoS. Без использования XFF-заголовка для предотвращения неоправданной нагрузки на веб-сервер возникает необходимость блокировать весь внешний IP-адрес (или диапазон адресов). В таком случае при наличии множества клиентов N частной сети за внешним IP-адресом под блокировку попадёт как злоумышленник, так и остальные пользователи, которые к атаке не имеют никакого отношения. В случае использования XFF-заголовка становится возможным блокировать исключительно злоумышленника, при этом сохраняя доступность ресурса для других пользователей.

Реально существующим примером описанной ситуации является функционирование интернет-провайдеров, поскольку некоторые из них используют схемы NAT и частных подсетей, не выдавая внешнего IP-адреса каждому своему пользователю.

Ещё одним фактом, способствующим широкому использованию данных HTTP-заголовка X-Forwarded-For, является сбор статистики по веб-ресурсу его владельцами. Благодаря сочетанию «уникальный внешний IP – частный IP» можно идентифицировать, сколько уникальных клиентов из выбранной частной подсети посещает ресурс. Данная статистика в дальнейшем может использоваться для различных целей (например, прогнозирование изменений нагрузки на веб-ресурс (которая не всегда явно зависит от аппаратного обеспечения [11]), анализ статистики для формирования более эффективных механизмов поиска и вывода информации конечным пользователям, формирования рекламных компаний и т.д.).

Но, помимо множества положительных сторон, использование заголовка X-Forwarded-For несёт в себе одну особенность, которая является таковой лишь на первый взгляд. Информацию об исходном адресе подключения используют как способ повысить защищённость веб-ресурса путём ограничения доступа к определённому функционалу ресурса со всех IP-адресов, кроме заранее определённых. Более того, зачастую предлагается при развёртывании ресурса запретить какой-либо доступ не только с внешних IP-адресов, но и с частных, которые входят в одну подсеть вместе с веб-ресурсом, оставляя при этом возможность только лишь локального управления (т.е. с адреса 127.0.0.1 (он же localhost)). Такие рекомендации можно встретить, например, при установке и настройке БД MySQL, где имеется соответствующий пункт меню с пояснением.

Как уже было указано ранее, наиболее распространённые веб-серверы поддерживают обработку заголовка XFF и в дальнейшем передают полученные данные непосредственно ресурсу, развёрнутому на базе этого веб-сервера. Полученный из заголовка X-Forwarded-For адрес присваивается как значение переменной REMOTE_ADDR, откуда затем и передаётся веб-ресурсу. Данная переменная также поддерживается подавляющим количеством веб-серверов (например, в Apache посредством модуля mod_rpaf, или в Microsoft IIS средствами из комплекта поставки). Таким образом, есть достаточно унифицированные стандартные возможности обработки нестандартных (но используемых) заголовков, что позволяет создателям веб-приложений избегать дублирования функционала.

Однако даже при должной конфигурации веб-приложения и базы данных к нему с сильными ограничениями на доступ к административной части (т.е. уже упомянутый доступ только с локальной консоли администрирования с адреса 127.0.0.1) остаётся вероятность раскрытия административной части веб-ресурса сторонним лицам, не уполномоченным на это. В случае недостаточного внимания к процессу конфигурации веб-сервера в части использования нестандартных заголовков становится возможным получить несанкционированный доступ путём проведения некоторых предварительных подготовительных действий.

Самым простым и наглядным вариантом является развёртывание прокси-сервера атакующим. В таком случае производится конфигурация прокси-сервера таким образом, чтобы атакующий в качестве клиентской платформы для подключения использовал клиентскую платформу с адресом 127.0.0.1, т.е. фактически осуществлял доступ с самого прокси, где в конфигурации приложения для работы с веб-ресурсом в качестве точки выхода указан прокси-сервер, расположенный на локальной машине. Таким образом, в заголовок XFF будет включён адрес 127.0.0.1. При развёртывании же этого заголовка на стороне веб-сервера без должной конфигурации в переменную REMOTE_ADDR будет внесён адрес 127.0.0.1, который и будет передан уже самому веб-ресурсу. При этом для веб-ресурса будет присутствовать видимость того, что клиент подключается с локальной системы, т.е. начинают действовать разрешения, предоставляющие более широкие полномочия в системе, в том числе и доступ к локальной консоли администрирования. В упрощённом виде данная схема представлена на рис. 2, где сперва происходит внос значения 127.0.0.1 в HTTP-заголовок X-Forwarded-For в системе злоумышленника, его передача и дальнейшее развёртывание на стороне веб-сервера и передача веб-ресурсу.

Данная ситуация, например, воспроизводима с одним из популярных средств администрирования phpMyAdmin для СУБД MySQL. Несмотря на то, что изначально при конфигурировании MySQL был запрещён доступ к БД и к средству администрирования БД со всех адресов, кроме 127.0.0.1, при доступе по схеме, представленной на рис. 2, административная панель становится доступна. Более того, становится возможным и процесс авторизации, что, в свою очередь, открывает доступ к непосредственно БД. При этом выявить источник проблемы может быть затруднительно, поскольку на уровне веб-сервера в журналы доступа в качестве клиента будет записан адрес, который фигурирует как значение переменной REMOTE_ADDR, т.е. 127.0.0.1.

Таким образом, проблема вполне может возникнуть из-за разности в конфигурации между приложением и сервером.

В качестве решения проблемы можно использовать подход, когда правила доступа к административным частям веб-ресурса регулируются не исключительно по адресам подключающихся клиентов, но с использованием данного функционала вкупе с другими возможностями (например, как это реализовано в инструменте phpMyAdmin, где по умолчанию предлагается авторизация через ввод пары «логин-пароль»).

Другим решением, которое поможет сократить вероятность коллизий, когда адрес из чужой частной подсети воспринимается как адрес из своей частной подсети, может быть переход на IPv6. В силу особенностей IPv6 (ограниченность адресного пространства IPv4 по сравнению с IPv6) пропадает практическая необходимость таких механизмов, как NAT. Однако это снижает возможности лишь случайных ситуаций получения доступа к ресурсам не уполномоченными на это лицами. При этом не исключается возможность целенаправленного воздействия злоумышленником, поскольку в стандарте IPv6 по-прежнему присутствуют такие понятия, как (рис. 2).

- Loopback – представлен в IPv4 как 127.0.0.1/8, т.е. localhost. В IPv6-адресации данный адрес представлен в виде: 1/128;
- Unique Local Unicast – стандарт RFC [8], пришедший на смену стандарту site-local, [9] который, в свою очередь, являлся аналогом частных сетей 10.0.0.0/8, 172.16.0.0/16 и 192.168.0.0./24.

Рис. 2. Доступ злоумышленника к веб-ресурсу через передачу значения 127.0.0.1 в заголовке XFF

Ещё одним средством снижения шансов осуществления НСД посредством эксплуатации особенностей обработки веб-сервером заголовка X-Forwarded-For может быть использование нестандартных или изменяемых значений путей к административным элементам веб-ресурсов [10]. Однако такой подход также не способен полностью оградить от проблем, поскольку лишь маскирует точки доступа с привилегированными правами.

Таким образом, в качестве общих рекомендаций к решению проблемы можно предложить следующее:

- не строить систему безопасности на основе одного элемента (в рассматриваемом случае с доступом к phpMyAdmin это была проверка только по IP, к тому же ещё и при помощи нестандартного, но распространенного заголовка X-Forwarded-For). При необходимости использования рассмотренного заголовка XFF в целях безопасности следует совмещать несколько средств безопасности, например с использованием пары «логин-пароль»;
- не доверять непроверенным данным, приходящим в приложение из других систем (в рассматриваемом случае передавалось значение переменной REMOTE_ADDR к веб-ресурсу от веб-сервера).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Стандарт «Forwarded HTTP Extension». [Электронный ресурс]: The Internet Engineering Task Force (IETF). URL: http://tools.ietf.org/html/rfc7239.
2. Документация прокси-сервера Squidю [Электронный ресурс]: Configuring Squid. URL: http://wiki.squid-cache.org/squidFaq/ConfiguringSquid.
3. Документация прокси-сервера Apache Module mod_proxyю [Электронный ресурс]: Apache Module mod_proxy. URL: http://httpd.apache.org/docs/trunk/mod/mod_proxy.html.
4. Документация администратора балансира нагрузки Barracudaю [Электронный ресурс]: Barracuda Load Balancer – Administrator Guide – Release 4.2. URL: https://techlib.barracuda.com/LOAD.
5. Конфигурация Cisco ACE с NAT и вставка заголовка клиентского IPю [Электронный ресурс]: Configure ACE with Source NAT and Client IP Header Insert. URL: http://www.cisco.com/c/en/us/support/docs/interfaces-modules/ace-application-control-engine-module/107399-ace-sourcenat-config.html.
6. Исследование веб-серверов «June 2014 Web Server Survey»ю [Электронный ресурс]: The Internet Engineering Task Force (IETF). URL: http://news.netcraft.com/archives/2014/06/06/june-2014-web-server-survey.html.
7. Стандарт «Issues with IP Address Sharing»ю [Электронный ресурс]: The Internet Engineering Task Force (IETF). URL: http://tools.ietf.org/html/rfc6269.
8. Стандарт «Unique Local IPv6 Unicast Addresses»ю [Электронный ресурс]: The Internet Engineering Task Force (IETF). URL: http://tools.ietf.org/html/rfc4193.
9. Стандарт «Deprecating Site Local Addresses»ю [Электронный ресурс]: The Internet Engineering Task Force (IETF). URL: http://tools.ietf.org/html/rfc3879.
10. *Максимов А.М.* Анализ особенностей осуществления атак на веб-сервер посредством генерации ошибочных запросов // Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 143-148.
11. *Максимов А.М., Тищенко Е.Н.* Особенности использования носителей информации в защищённых информационных системах // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 238-244.

REFERENCES

1. Standart «Forwarded HTTP Extension»: The Internet Engineering Task Force (IETF). Available at: http://tools.ietf.org/html/rfc7239.
2. Dokumentatsiya proksi-servera Squid [Documentation of the proxy server Squid]: Configuring Squid. Available at: http://wiki.squid-cache.org/squidFaq/ConfiguringSquid.

3. Dokumentatsiya proksi-servera Apache Module mod_proxy [Documentation of the proxy server Apache Module mod_proxy]: Apache Module mod_proxy. Available at: http://httpd.apache.org/docs/trunk/mod/mod_proxy.html.
4. Dokumentatsiya administratora balansira nagruzki Barracuda [Documentation administrator load balancer Barracuda]: Barracuda Load Balancer – Administrator Guide – Release 4.2. Available at: https://techlib.barracuda.com/LOAD.
5. Konfiguratsiya Cisco ACE s NAT i vstavka zagolovka klientskogo IP [The Cisco ACE configuration with NAT and insert the client IP header]: Configure ACE with Source NAT and Client IP Header Insert. Available at: http://www.cisco.com/c/en/us/support/docs/interfaces-modules/ace-application-control-engine-module/107399-ace-sourcenat-config.html.
6. Issledovanie veb-serverov «June 2014 Web Server Survey» [Study web servers, "June 2014 Web Server Survey": The Internet Engineering Task Force (IETF). Available at: http://news.netcraft.com/archives/2014/ 06/06/june-2014-web-server-survey.html.
7. Standart «Issues with IP Address Sharing»: The Internet Engineering Task Force (IETF). Available at: http://tools.ietf.org/html/rfc6269.
8. Standart «Unique Local IPv6 Unicast Addresses»: The Internet Engineering Task Force (IETF). Available at: http://tools.ietf.org/html/rfc4193.
9. Standart «Deprecating Site Local Addresses» [Электронный ресурс]: The Internet Engineering Task Force (IETF). Available at: http://tools.ietf.org/html/rfc3879.
10. *Maksimov A.M.* Analiz osobennostey osushchestvleniya atak na veb-server posredstvom generatsii oshibochnykh zaprosov [Analysis of attacks on the web server by generating erroneous requests], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2013, No. 12 (149), pp. 143-148.
11. *Maksimov A.M., Tishchenko E.N.* Osobennosti ispol'zovaniya nositeley informatsii v zashchishchennykh informatsionnykh sistemakh [Features of the use of media in secure information systems], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2011, No. 12 (125), pp. 238-244.

Статью рекомендовал к опубликованию д.т.н., профессор Г.Е. Веселов.

Максимов Алексей Михайлович – Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Ростовский государственный экономический университет (РИНХ)»; e-mail: ironmanpc@rambler.ru; 344002, г. Ростов-на-Дону, ул. Б. Садовая, 69, к. 211, 306а; тел.: 89286014570; аспирант.

Тищенко Евгений Николаевич – e-mail: celt@inbox.ru; тел.: 89281440403; кафедра информационных технологий и защиты информации; зав. кафедрой; д.э.н.; доцент.

Серпенинов Олег Витальевич – e-mail: serpeninov53@mail.ru; тел.: 89185064000; кафедра информационных технологий и защиты информации; к.т.н.; доцент.

Maximov Alexey Mikhailovich – Rostov State University of Economics (RSUE); e-mail: ironmanpc@rambler.ru; 69, B. Sadovaya street, room 306a, 211, Rostov-on-Don, 344002, Russia; phone: +79286014570; postgraduate student.

Tischenko Evgeniy Nickolaevich – e-mail: celt@inbox.ru; phone: +79281440403; the department of information technologies and information security; head of department; dr. of ec. sc.; associate professor.

Serpeninov Oleg Vitalyevich – e-mail: serpeninov53@mail.ru; phone: +79185064000; the department of information technologies and information security; cand. of eng. sc.; associate professor.