УДК 004.056.5

А.С. Шабуров[1], Е.Е. Журилова[1], В.С. Лужнов[2]

[1]Пермский национальный исследовательский политехнический университет, Пермь, Россия
[2]Южно-Уральский государственный университет (Национальный исследовательский университет), г. Челябинск, Россия

ТЕХНИЧЕСКИЕ АСПЕКТЫ ВНЕДРЕНИЯ DLP-СИСТЕМЫ НА ОСНОВЕ FALCONGAZE SECURE TOWER

Проанализирована актуальная проблема защиты от утечки информации ограниченного доступа в корпоративных системах, что требует внедрения новых программно-технических решений. Приведены необходимые статистические данные. Определено понятие DLP-системы как основного инструмента противодействия утечкам информации. Проанализированы основные и дополнительные функциональные возможности подобных систем, разнообразие которых позволяет обеспечить наиболее высокий уровень защиты информации от утечек. Определена сложная задача защиты от утечек конфиденциальной информации в крупных учреждениях и организациях, в том числе и в образовательных учреждениях. Обеспечение защиты информации в условиях реализации задач ПНИПУ как высшего учебного заведения предполагается с использованием DLP-системы на основе программного решения Falcongaze Secure Tower. Проанализированы основные функциональные возможности Falcongaze Secure Tower, порядок и варианты установки и настройки программного обеспечения. Раскрыты основные особенности и преимущества вариантов настройки системы. Приведена иллюстрация консоли администратора, содержащая: монитор состояния, интерфейс для настройки индексирования, интерфейс для настройки обработки цифровых отпечатков, интерфейс настройки пользователей и агентов, интерфейс, позволяющий управлять обработкой почтовых отправлений и распознаванием изображений, а также лицензионную информацию. Раскрыты способы установки агентов на рабочие станции: вручную, с помощью групповых политик либо с использованием возможностей консоли администратора, а также способы осуществления морфологического анализа обрабатываемой информации. Приведена структурно-функциональная схема работы системы Falcongaze Secure Tower и описан основной алгоритм ее работы. Приведены необходимые результаты оценки эффективности работы системы, полученные на основе экспериментальных данных.

Ключевые слова: защита информации от утечки, DLP-система, требования по защите информации, мониторинг, порт зеркалирования, консоль администратора, консоль пользователя, анализ информации, база данных, морфологический анализ, алгоритм стэмминга, эффективность защиты информации.

A.S. Shaburov[1], E.E. Zhurilova[1], V.S. Luzhnov[2]

[1]Perm National Research Polytechnic University, Perm, Russian Federation
[2]South Ural State University (National Research University),
Chelyabinsk, Russian Federation

TECHNICAL ASPECTS OF IMPLEMENTATION OF DLP-SYSTEMS, BASED ON FALCONGAZE SECURE TOWER

It was analyzes the actual problem of preventing the leakage of restricted access information in corporate systems, which requires implementation of new software-technical decisions. Prevent the necessary statistical data. The concept of DLP-system, as the main instrument to counter information leaks, was formed. It was analyzed the basic and advanced functional capabilities of such systems, which variety allows to provide the highest level of protection from information leakage. The difficult task of protection confidential information against leaks in large establishments and organizations, including the educational institutions was determined. Providing of information security in conditions of implementation the tasks of PSTU, as high level educational institution is expected with the using DLP-system, based on software solutions Falcongaze Secure Tower. It was analyzed the main functions of Falcongaze Secure Tower, order and options of installation and configuring the software. It outlines the main features and benefits of system setup options. It was illustrated the admin console, which involves: a status monitor, interface to configure indexing, interface to configure process digital prints, interface to configure users and agents, the interface, which allows you to control the processing of mail and the image recognition, and also license information. It was reveal the methods of installing agents of workstations: manually, using the group policies and using the capabilities of admin console, and also reveal the methods of morphological analysis of the processed information. It was shown the structural- functional scheme of working system Falcongaze Secure Tower, and described the basic algorithm of its work. It was prevented the necessary results of evaluation the effectiveness of the system, based on experimental data.

Keywords: protection of information leakage, DLP-system, requirements for the protection of information, surveillance, mirroring port, admin console, clients console, information analyzing, database, morphological analysis, stemming algorithm, effectiveness of information security.

В настоящее время достаточно актуальной является проблема обеспечения информационной безопасности корпоративных систем, для которых одной из основных задач при создании систем защиты является блокирование каналов утечки информации.

Согласно статистике 2014 г. (рис. 1) большинство утечек происходит через интернет-сервисы [1].

Традиционно к основным средствам предотвращения утечки информации из-за использования интернет-сервисов относятся DLP (Data Loss Prevention)-системы. Существует множество таких систем от различных производителей и с разнообразными функциональными возможностями, однако основным предназначением подобных систем является анализ потоков данных, пересекающих периметр защищаемой информационной системы. В качестве дополнительных возможностей могут быть такие, как периодические снимки рабочего

стола, прослушивание микрофонов, составление отчетных графиков, составление статистики авторизации пользователей для предотвращения входа в систему злоумышленника путем кражи учетной записи. Разнообразные дополнительные функциональные возможности позволяют обеспечить наиболее высокий уровень защиты информации от утечек.

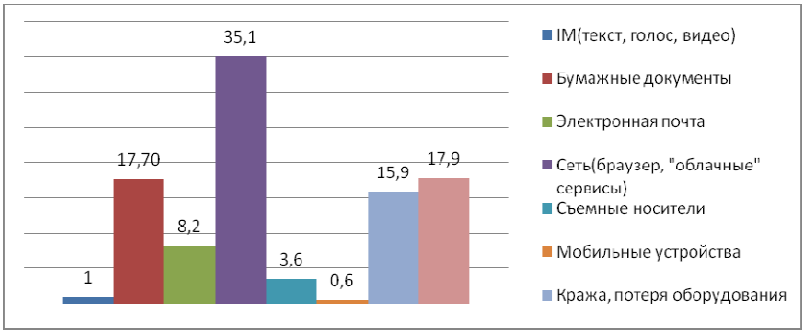

Рис. 1. Статистика утечек конфиденциальной информации через различные источники

Еще одним немаловажным достоинством подобных систем является возможность усиленного контроля нелояльных сотрудников. Например, сотрудники, попадающие под сокращение, могут распространить конкурентам активы компании [2].

Особенно сложной представляется задача защиты от утечек конфиденциальной информации в крупных учреждениях и организациях, как правило, имеющих значительное количество разнообразных информационных ресурсов, в том числе и ресурсов ограниченного доступа. Примером подобных организаций могут считаться образовательные учреждения высшего профессионального образования. Пермский национальный исследовательский политехнический университет представляет собой организацию, состоящую из большого количества разнообразных структурных подразделений, использующих в повседневной деятельности значительные объемы постоянно циркулирующей информации. Данные информационные потоки могут содержать значительное количество информации ограниченного распространения, включая персональные данные студентов и работников ПНИПУ, результаты научных исследований, отчетную документацию.

Обеспечить защиту информации в условиях реализации задач высшего учебного заведения на необходимом уровне безопасности информационных процессов предполагается с использованием DLP-системы на

основе программного решения Falcongaze Secure Tower.

Система Falcongaze Secure Tower, как правило, включает несколько компонентов, находящихся на одном сервере или размещенных на нескольких серверных станциях. При этом локализация небольшого количества администрируемых рабочих станций рационально предполагает ограничиться одним сервером. Благодаря наличию технологии виртуализации такое решение является возможным и позволит более полноценно использовать ресурсы сервера [3].

Установка и настройка программного обеспечения имеют стандартный вид и интуитивно понятный интерфейс. Перед установкой прежде всего необходимо определиться со способом перехвата данных с контролируемых рабочих станций. Secure Tower предоставляет на выбор два способа: перехват с помощью агентов, устанавливаемых на рабочие станции, либо централизованно через порт зеркалирования сетевого коммутатора [4].

Преимуществом первого варианта является возможность перехвата как нешифрованного, так и шифрованного трафика, при этом установки сервера перехвата не требуется. Необходимый комплект компонентов для установки в данном случае состоит из сервера обработки данных, сервера контроля агентов, сервера обработки почты, сервера распознавания, сервера лицензирования и центров отчетности и безопасности.

Второй же способ позволяет осуществить перехват только нешифрованного трафика. Также использование второго способа влечет за собой физическое изменение топологии сети, снижающее ее пропускную способность, что является существенным недостатком данного способа. Одной из основных функциональных особенностей данной системы является возможность автоматического составления графиков по различным показателям для их анализа [5]. Например, график использования рабочего времени пользователями позволяет увидеть и проанализировать, какое количество времени тратится ими на обработку данных, на серфинг по интернет-страницам, общение с другими пользователями. Согласно статистическим данным сотрудники могут тратить на посторонние дела в коммерческих организациях и банках до 10 %, в государственных структурах – до 26 %, а в проектных организациях – до 40 % рабочего времени [6].

Для настройки системы, руководства мониторингом, управления системой существуют два интерфейса: консоль администратора и консоль пользователя. Обе консоли могут быть установлены на любую рабочую станцию, и администратор может управлять настройками программы

из любого места как удаленно, так и с конкретной рабочей станции.

Консоль администратора содержит: монитор состояния, интерфейс для настройки индексирования, интерфейс для настройки обработки цифровых отпечатков, интерфейс настройки пользователей и агентов, интерфейс, позволяющий управлять обработкой почтовых отправлений и распознаванием изображений, а также лицензионную информацию [4].

Монитор состояния показывает краткую информацию по всем работающим серверам, например, скорость передачи сетевого трафика и количество активных агентов для сервера контроля агентов (рис. 2).

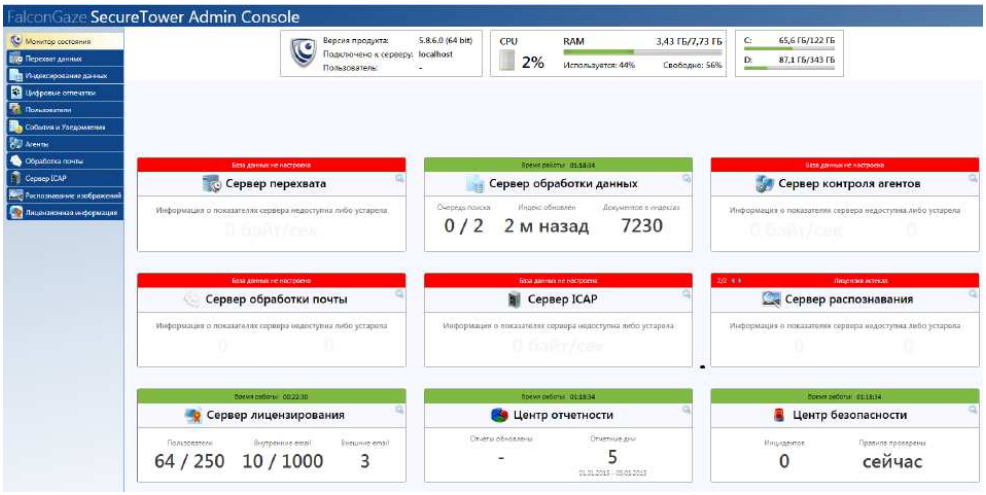

Рис. 2. Консоль администратора – монитор состояния

Настройка индексирования позволяет создать свой индекс поиска либо изменить индекс, настроенный по умолчанию. Если индекс не настроен, то данные индексируются по стандартному индексу. Индексирование данных позволяет распределять и упорядочивать данные, что облегчает их дальнейший поиск по меткам. Если перехваченные данные не проиндексированы или это сделано не корректно, то при поиске информации система не будет выводить адекватные результаты.

Большим преимуществом системы Falcongaze Secure Tower является возможность импорта пользователей из Active Directory, сохраняя имеющуюся уже там структуру. Существуют два режима обращения Falcongaze Secure Tower к AD: ручной и автоматический. В ручном режиме указывается список доменов и пользователи интегрируются только с ним. В автоматическом же режиме Falcongaze сканирует локальную сеть на предмет доступных доменов и импортирует списки

пользователей из найденных доменов. Если интеграция с Active Directory не требуется, список пользователей можно составлять вручную, вводя информацию о них в учетные карточки.

Данная DLP-система имеет три способа установки агентов на рабочие станции: вручную, используя файл с расширением .exe, с помощью групповых политик, используя файл с расширением .msi, либо используя возможности консоли администратора. При установке агентов необходимо настроить хранилище информации, где будет храниться перехваченный трафик. Ручная установка рациональна, если число рабочих станций незначительное, в остальных же случаях лучше использовать групповые политики или консоль администратора.

Консоль пользователя позволяет работать с перехваченным трафиком. К основным ее возможностям относятся: просмотр сетевой активности пользователей, простой и комбинированный поиск информации, мониторинг в реальном времени, построение отчетов, создание правил безопасности и отправка оператору сообщений о нарушениях правил безопасности [7].

Интерфейс поиска информации предоставляет большой выбор параметров для поиска. Поиск может осуществляться по словам, фразам, регулярным выражениям. В зависимости от необходимости можно настроить поиск слов, написанных с использованием транслитерации, либо на основе морфологического анализа [8].

Морфологический анализ представляет собой выделение ключевых слов во входящем потоке текста, что вызывает некоторую сложность, поскольку в русском языке существует большое количество слов исключений, не поддающихся стандартному разбору.

В настоящее время используются три основных способа морфологического анализа:

1. Ручное составление морфологического словаря для конкретного предприятия. Данный способ является трудоемким и неэффективным.

2. Использование алгоритма стэмминга. Данный метод выделения морфологически постоянных частей слов путем удаления известных частей слов, выполняющих заведомо вспомогательную роль, в соответствии с заранее предопределенными правилами.

3. Определение слова по аффиксу и суффиксу. Данный способ, основанный на приведении слова к его первоначальной форме, сегодня является наиболее часто используемым [9].

Кроме того, поиск данных может осуществляться по конкретному пользователю, порту, IP-адресу, дате и времени. В свою очередь, ком-

бинированный поиск позволяет создавать условия поиска информации, объединяя их в логические блоки.

Однако DLP-система, построенная только на анализе информации, не может считаться полноценной и служить надежным средством контроля передачи данных. Необходимо также не забывать о вспомогательных специализированных решениях для логического и физического контроля каналов [10].

В системе Falcongaze Secure Tower существуют как уже настроенные стандартные правила безопасности, так и возможна настройка дополнительных правил безопасности, в зависимости от сферы деятельности организации. Для анализа эффективности работы системы возможны настройка и имитация инцидентов. При этом сообщения об инцидентах в зависимости от настроек могут отправляться по указанному почтовому адресу.

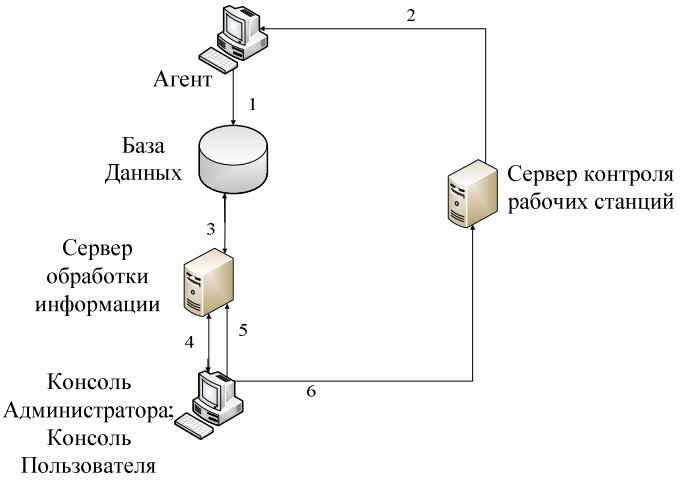

Рис. 3. Структурно-функциональная схема работы системы Falcongaze Secure Tower

Структурно-функциональная схема работы системы представлена на рис. 3 и состоит в следующем. Агенты, установленные на рабочие станции, накапливают данные из приложений, запущенных пользователем, и передают их на хранение в базу данных. Сервер обработки информации выполняет обращения к базе данных, индексирует хранящиеся там данные, выявляет нарушения правил безопасности и осуществляет поиск по индексированным данным.

Клиентская консоль реализует функцию поиска, взаимодействия

оператора с центром обработки информации, а также взаимодействует с центром безопасности. Консоль администратора позволяет осуществлять настройку всех подсистем. Сервер контроля рабочих станций контролирует работу агентов и может осуществлять управление агентами. Цифрой *1* (см. рис. 3) показано движение перехваченных данных от агентов к базе данных. В то же время цифра *2* показывает возможность сервера контроля рабочих станций посылать команды для управления агентами, установленными на рабочих станциях. Цифрой *3* обозначен обмен командами и информацией между базой данных и сервером обработки информации. Сервер обработки информации посылает управляющую команду для индексирования данных. Также через него поступают команды на поиск данных, а база данных отправляет в ответ найденную информацию.

Взаимодействие между клиентской консолью и сервером обработки информации обозначено цифрой *4*. С помощью клиентской консоли оператор отправляет запросы на сервер обработки информации, получая в ответ сообщения о нарушениях, поисковые данные, либо иные требуемые данные. Цифрой *5* обозначены команды управления, посылаемые оператором через консоль администратора для настройки подсистем. Цифра *6* означает посылаемые через консоль администратора команды управления, но уже для сервера контроля агентов.

Оценка эффективности защиты информации с использованием предлагаемого программного решения на базе ПНИПУ и определение степени корректности реагирования системы на нарушения требований безопасности информации были осуществлены экспериментально. Были смоделированы нарушения правил безопасности пользователями с использованием 50 рабочих станций. В результате эксперимента в подразделении ПНИПУ из 37 попыток отправить конфиденциальные данные по открытым каналам связи были выявлены все, а сообщения о нарушениях правил безопасности были отправлены по указанным почтовым адресам.

Таким образом, внедрение системы Falcongaze Secure Tower позволяет решить задачу блокирования распространения конфиденциальной информации через каналы связи в инфраструктуре ПНИПУ. Кроме того, возможности программы позволяют определить структурное подразделение – источник и канал утечки, что, в свою очередь, позволит избежать утечек в дальнейшем. При этом функциональные возможности Falcongaze Secure Tower позволяют обеспечить решение задач защиты информации на достаточно эффективном уровне, что обусловливает применение подобной системы как в подразделениях ПНИПУ, так и в других образовательных учреждениях.

Библиографический список

1. Программный комплекс «Стахановец» как DLP-система: предотвращение утечек конфиденциальной информации [Электронный ресурс]. – URL: https://www.infowatch.ru/report2014 (дата обращения: 07.10.2105).

2. Тимошенко А. DLP как эффективный инструмент работы с нелояльными сотрудниками // Информационная безопасность. – 2015. – № 3. – URL: http://itsec.ru/articles2/dlp/dlp-kak-effektivnyy-instrument-raboty-s-neloyalnymi-sotrudnikami (дата обращения: 30.09.2015).

3. Шабуров А.С., Рашевский Р.Б. Практическое применение VMWARE VSHIELD APP для обеспечения безопасности виртуального веб-сервера // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – Пермь, 2014. – № 11. – С. 94–101.

4. Falcongaze Secure Tower. Руководство системного администратора. – М., 2010.

5. Сайт компании «Фалконгейз». – М., 2010. – URL: http://falcongaze.ru (дата обращения: 10.07.2015).

6. Вахонин С. Эффективность применения контентной фильтрации в DLP-системах // Информационная безопасность. – 2015. – № 3. – URL: http://itsec.ru/articles2/dlp/effektivnost-primeneniya-kontentnoy-filtratsii-v-dlp-sistemah (дата обращения: 30.09.2015).

7. Falcongaze Secure Tower. Руководство пользователя. – М., 2010.

8. Кизянов А.Ф. Разработка и исследование методов и средств полнотекстового индексирования информации с учетом морфологии естественного языка: дис. канд. техн. наук. – Таганрог, 2005.

9. Жаринов Р.Ф. Метод защиты от перлюстрации в DLP-системах // Доклады Томск. гос. ун-та систем управления и радиоэлектроники. – 2012. – № 1–2.

10. Вахонин С. Конфиденциальные данные – под надежный контроль! Использование современной DLP-системы для предотвращения утечек информации // Информационная безопасность. – 2015. – № 3. – URL: http://itsec.ru/articles2/dlp/konfidentsialnye-dannye-pod-nadezhnyy-kontrol-ispolzovanie-sovremennoy-dlp-sistemy-dlya-predotvrascheniya-utechek-informatsii (дата обращения: 30.09.2015).

References

1. Programmnyi kompleks “Stakhanovets” kak DLP-sistema: predotvrashchenie utechek konfidentsial'noi informatsii [The program complex “Stakhanovite” as DLP-system: security leakages prevention], available at: https://www.infowatch.ru/report2014 (accessed 07 October 2015).

2. Tymoshenko A. DLP kak effektivnyi instrument raboty s neloial'nymi sotrudnikami [DLP as an effective tool to deal with disloyal employees]. *Informatsionnaia bezopasnost'*, 2015, no. 3, available at: http://itsec.ru/articles2/dlp/dlp-kak-effektivnyy-instrument-raboty-s-neloyalnymi-sotrudnikami (accessed 30 September 2015).

3. Shaburov A.S., Rashevsky R.B. Prakticheskoe primenenie VMWARE VSHIELD APP dlia obespecheniia bezopasnosti virtual'nogo veb-servera [Actual use of VMWARE VSHIELD APP for reasons of the virtual web server safety]. *Vestnik Permskogo natsional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2014, no. 11, pp. 94-101.

4. Falcongaze Secure Tower. Rukovodstvo sistemnogo administratora [Falcongaze Secure Tower. System Administrator's Guide]. Moscow, 2010.

5. Sait kompanii Falkongeiz [Falcongaze: official web-site]. Moscow, 2010, available at: http://falcongaze.ru (accessed 10 July 2015).

6. Vakhonin S. Effektivnost' primeneniia kontentnoi fil'tratsii v DLP-sistemakh [Content filtering efficiency in the DLP-systems]. *Informatsionnaia bezopasnost'*, 2015, no. 3, available at: http://itsec.ru/articles2/dlp/effektivnost-primeneniya-kontentnoy-filtratsii-v-dlp-sistemah (accessed 30 September 2015).

7. Falcongaze Secure Tower. Rukovodstvo pol'zovatelia [User's manual]. Moscow, 2010.

8. Kizyanov A.F. Razrabotka i issledovanie metodov i sredstv polnotekstovogo indeksirovaniia informatsii s uchetom morfologii estestvennogo iazyka [Development and research of methods and tools for full-text information indexing by reference to the natural language morphology: Ph.D. Thesis]. Ph.D. Thesis. Taganrog, 2005.

9. Zharinov R.F. Metod zashchity ot perliustratsii v DLP-sistemakh [Security method against censorship in DLP-systems]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniia i radioelektroniki*, 2012, no. 1-2.

10. Vakhonin S. Konfidentsial'nye dannye – pod nadezhnyi kontrol'! Ispol'zovanie sovremennoi DLP-sistemy dlia predotvrashcheniia utechek

informatsii [Private data – under standby controll! Modern DLP-system use for information leaks prevention]. *Informatsionnaia bezopasnost'*, 2015, no. 3, available at: http://itsec.ru/articles2/dlp/konfidentsialnye-dannye-pod-nadezhnyy-kontrol-ispolzovanie-sovremennoy-dlp-sistemy-dlya-predotvrascheniya-utechek-informatsii (accessed 30 September 2015).

Сведения об авторах

Шабуров Андрей Сергеевич (Пермь, Россия) – кандидат технических наук, доцент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: shans@at.pstu.ru).

Журилова Елена Евгеньевна (Пермь, Россия) – студентка Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: ele11485995@yandex.ru).

Лужнов Василий Сергеевич (Челябинск, Россия) – ассистент кафедры безопасность информационных систем Южно-Уральского государственного университета (Национального исследовательского университета) (454080, Челябинск, пр. Ленина, 76, e-mail: ua9stz@gmail.com).

About the authors

Shaburov Andrey Sergeevich (Perm, Russian Federation) is a Ph.D. of Technical Sciences at the Department of Automation and Telemechanics, Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: shans@at.pstu.ru).

Zhurilova Elena Evgen'evna (Perm, Russian Federation) is a student at the Department of Automation and Telemechanics, Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: ele11485995@yandex.ru).

Luzhnov Vasiliy Sergeevich (Chelyabinsk, Russian Federation) is an assistant at the Department of Information systems security, South Ural State University (National Research University) (454080, Chelyabinsk, pr. Lenina, 76, e-mail: ua9stz@gmail.com).

Получено 05.10.2015