Инженерный вестник Дона, №3 (2017)
ivdon.ru/ru/magazine/archive/n3y2017/4348

Методика выявления сетевых атак класса «человек посередине» на основе анализа транзитного трафика

В.В. Галушка, В.А. Фатхи, Д.В. Фатхи, Е.Н. Чуйкова

Донской государственный технический университет, Ростов-на-Дону

Аннотация: Статья посвящена проблеме защиты данных от перехвата в результате выполнения атак типа «человек посередине». Предлагаемая методика выявления данных атак основывается на анализе заголовков транзитных пакетов, проходящих через шлюз по умолчанию. На основе полученных данных строится таблица соответствия IP и MAC адресов, для которой программными средствами обеспечивается актуальность и достоверность. Адреса пакетов, проходящих через шлюз, сравниваются с записями в данной таблице и, в случае несовпадения и невозможности подтверждения правильности адресов в заголовках канального и сетевого уровней, делается вывод о наличии в сети дополнительного промежуточного узла, появившегося в результате подмены шлюза по умолчанию. В статье приводятся подходы к программной реализации данной методики, описывается алгоритм анализа пакетов.
Ключевые слова: локальная сеть, «человек посередине», DHCP-spoofing, ARP-poisoning, анализ трафика, шлюз, сетевой адрес, пакет, ARP-таблица.

Введение

Современные информационные технологии основываются на всё более широком использовании распределённых систем, в связи с чем происходит как количественный рост объёмов передаваемого по сети трафика, так и качественное изменение его содержания. Информация, передаваемая по сети, всё чаще включает в себя секретные сведения, коммерческую тайну, персональные данные и т.п. Развитие сетевых технологий, их усложнение и постоянное появление новых, создают потенциальные возможности как для появления неизвестных ранее способов сетевых атак, так и для поиска нестандартных путей использования распространённых уязвимостей [1].

В связи с этим, важной проблемой становится защита данных при их передаче по сети, неотъемлемой частью которой является выявление сетевых атак, среди которых наибольшую угрозу представляют атаки, относящиеся к классу man-in-the-middle или «человек посередине» [2]. Их успешная

реализация позволяет злоумышленнику перехватывать сообщения, передаваемые между узлами сети, извлекая из них любую информацию.

Постановка задачи

В большинстве случаев доступ конечных пользователей в сеть интернет осуществляется из внутренней локальной сети организации или провайдера (рис. 1). При этом за предоставление доступа отвечает шлюз — аппаратное устройство, или установленное на компьютер программное обеспечение, выполняющее функции сопоставления адресов внутренней сети адресу во внешней, а также управление пользователями и учёт трафика.

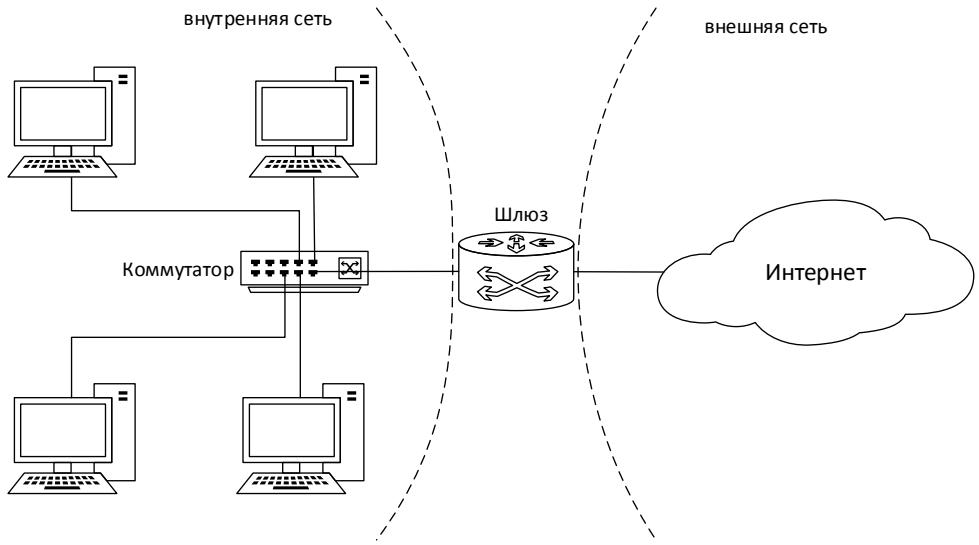


Рис. 1. – Типовая схема соединения локальной сети с интернетом

Чаще всего для выполнения указанной выше атаки используется подмена какого-либо из адресов: IP или MAC. Так например DHCP-spoofing использует поддельные ответы DHCP-сервера для того, чтобы задать узлу сети в качестве адреса шлюза IP-адрес злоумышленника [3], а при атаке типа ARP-poisoning путём рассылки ложных уведомлений протокола ARP подменяется MAC-адрес шлюза [4]. В результате любой из этих атак путь прохождения пакета изменяется и в него добавляется ещё один

промежуточный узел — как правило компьютер злоумышленника, на котором он сможет просматривать содержимое передаваемых в сеть и получаемых из неё сообщений жертвы.

Как следует из рисунка и описаний, приведённых выше, в конфигурации локальной сети шлюз играет одну из важнейших ролей. Через него проходят все пакеты, отправляемые с узлов локальной сети в интернет и получаемые ими обратно, поэтому защиту от сетевых атак целесообразно реализовывать именно на нём, к тому же получить доступ к такому компьютеру для злоумышленника гораздо сложнее, чем к любому другому, а его администрированию уделяется особое внимание.

Существующие методы защиты от атак, основанных на подмене адресов шлюза, достаточно ограничены в применении. Так, например, физические устройства, способные предотвратить такие атаки относятся к верхнему ценовому сегменту, требуют тщательной настройки и затрудняют переконфигурирование сети.

Использование шифрования также связано со значительными сложностями. Для использования шифрующего прокси-сервера необходим отдельный высокопроизводительный компьютер, способный в режиме реального времени выполнять шифрование/дешифрование всех проходящих через него пакетов, а также его правильная конфигурация и грамотное администрирование [5]. Более того, при использовании прокси-сервера необходимо на каждом клиентском компьютере задавать настройки подключения к нему, а некоторые программы вообще не способны работать через прокси-сервер.

Проблемы, возникающие при использовании для шифрования протокола HTTPS, заключаются в том, что в вопросах безопасности приходится полагаться на разработчиков и администраторов сайта, так как только от них зависит, какой именно протокол будет использоваться при

передаче данных. К тому же, данный способ шифрования применяется только к HTTP-траффику, то есть он позволяет защитить только логины/пароли вводимые на web-страницах, оставляя уязвимыми, например, почтовые сообщения, telnet-команды и прочие данные, передаваемые не по протоколу HTTPS.

Таким образом, актуальной является задача разработки метода обнаружения атак, основанных на подмене адресов, путём анализа транзитных пакетов на компьютере, выполняющем функции интернет-шлюза.

Методика защиты

Система защиты, работающая на интернет-шлюзе, может выявлять сетевые атаки только путём анализа заголовков проходящих через него пакетов. В случае атак типа «человек посередине» путь пакета модифицируется, то есть к нему добавляется промежуточный узел, что отражается на содержимом полей заголовков канального и сетевого уровня [5, 6]. Заголовок сетевого уровня содержит IP-адреса узла источника и назначения, заголовок канального уровня — MAC-адреса источника и назначения.

На рисунке 2 показана схема сети, уже рассмотренная ранее, и на ней обозначены IP и MAC адреса компьютеров. В процессе её функционирования шлюз формирует ARP-таблицу — таблицу соответствия IP и MAC адресов.

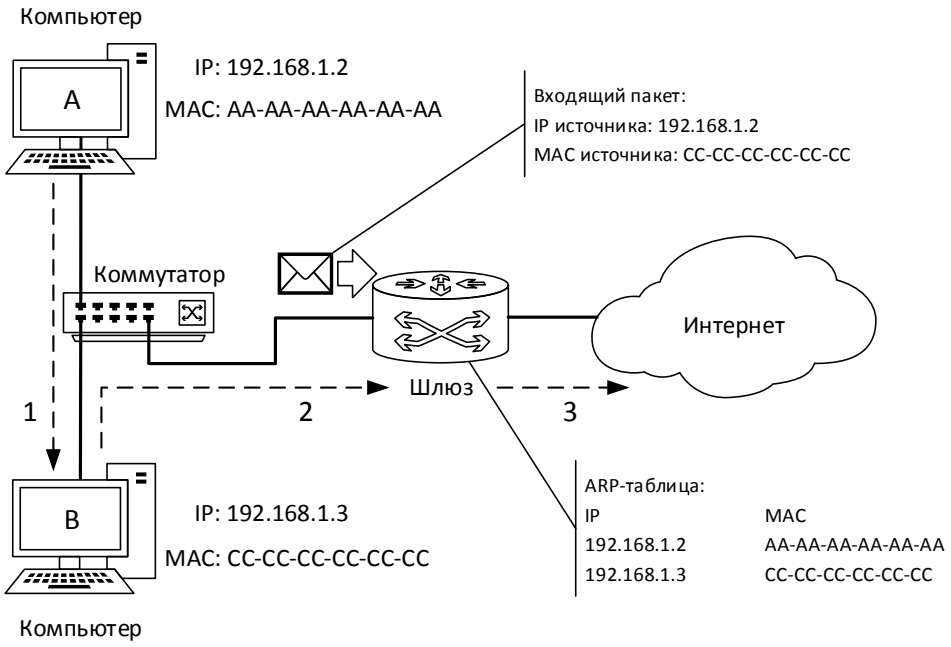


Рис. 2. – Схема функционирования сети после подмены шлюза

После успешной подмены адреса шлюза по умолчанию для компьютера B, пакеты от компьютера A будут направляться в интернет по маршруту, обозначенному пунктирными стрелками. При этом IP-адрес источника будет всегда оставаться одинаковым — это адрес компьютера, пославшего пакет, то есть компьютера A — 192.168.1.2, однако протоколы нижних уровней, осуществляя физическую передачу пакета, будут записывать в поле MAC-адреса источника адрес компьютера, через который этот пакет прошёл последним, а это всегда будет MAC-адрес злоумышленника. В результате моделирования, проведённого в Cisco Packet Tracer было установлено, что для показанного на рисунке 2 примера, пакет, приходящий на шлюз будет иметь следующие записи (см. рис. 3 а):

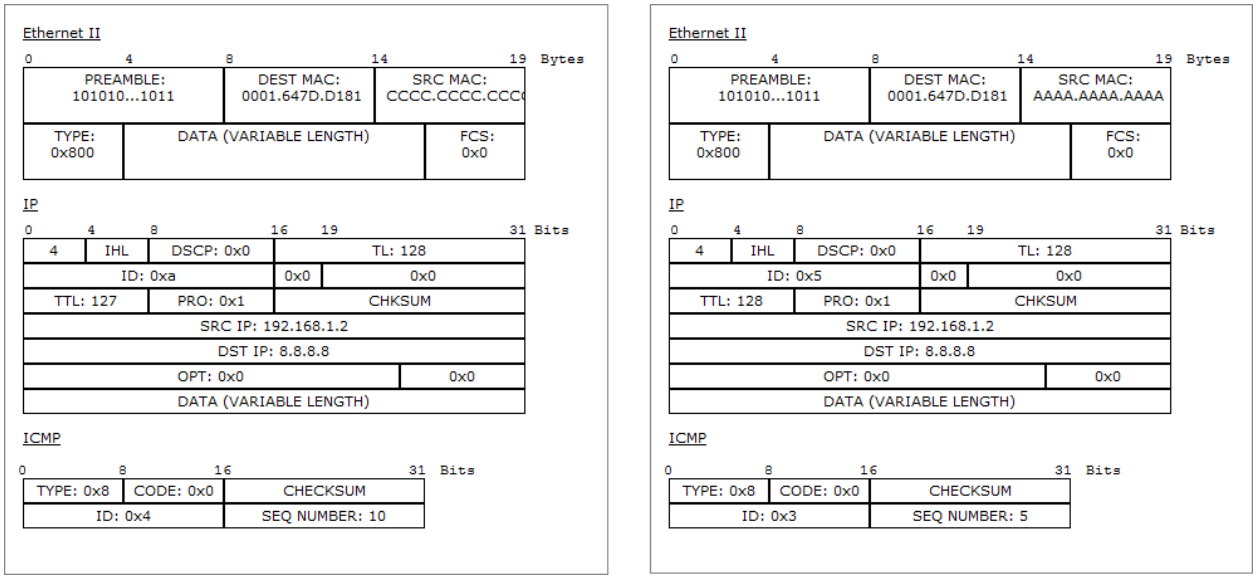
1) IP-адрес источника: 192.168.1.2;
2) MAC-адрес источника: CC-CC-CC-CC-CC-CC.

Данные записи не соответствуют содержимому ARP-таблицы шлюза и должны как минимум вызвать подозрение.

В отличие от пакета, следующего по изменённому маршруту, в пакете, пришедшем напрямую от компьютера, IP и MAC адреса источника всегда совпадают с какой-либо записью в ARP-таблице (см. рис. 3 б).

Используя описанные свойства пакетов, полученных от разных источников, можно реализовать программную защиту от такого рода атак. Она будет включать в себя 3 этапа:

1. захват проходящего через шлюз пакета;
2. анализ его заголовков сетевого и канального уровней;
3. принятие решения о дальнейших действиях с пакетом.



а) при подмене адреса шлюза б) при нормальном функционировании

Рис. 3. – Содержимое заголовков пакета

Особенности программной реализации методики защиты

Для осуществления первого этапа необходимо использовать одну из библиотек захвата траффика. Наиболее известной из них является библиотека Pcap (Packet capture), которая позволяет создавать программы анализа данных, поступающих на сетевую карту компьютера. Она предназначена для использования совместно с языками C/C++, а для работы

с библиотекой на других языках, таких как Java, .NET, используют оболочки. В частности, для языка C# используется SharpPcap.

Наиболее важным является второй этап. На нём необходимо извлечь из пакета сначала заголовок канального уровня, на котором используется протокол Ethernet, затем заголовок сетевого уровня из протокола IP (см. рис. 4). На основании полученных данных должна быть построена собственная таблица соответствия адресов [7]. И хотя формально она схожа с ARP-таблицей, но таковой не является, так как использует принципиально другой способ формирования, а именно, записи попадают в неё в результате анализа реальных пакетов данных, проходящих через компьютер, и для каждой записи используется активная система подтверждения, которая рассылает запросы и проверяет ответы в случае обнаружения каких-либо изменений [8].

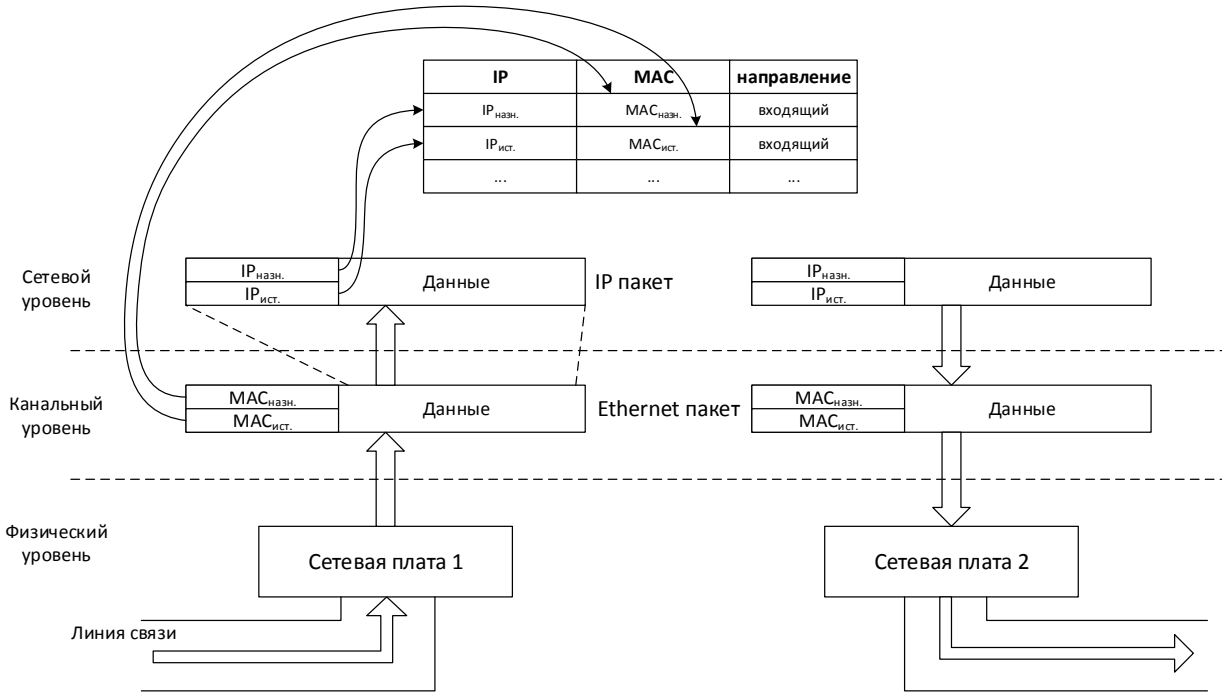


Рис. 4. – Схема формирования таблицы соответствия IP- и MAC-адресов

В процессе функционирования состояния программного объекта, представляющего пакет, могут меняться в зависимости от наступления определённых событий. Для отображения состояний системы или объекта, а

также их взаимосвязи служит диаграмма состояний UML (рис. 5). Из неё видно, что пакет, пришедший в приложение для анализа изначально имеет статус «новый», затем происходит проверка таблиц соответствия IP и MAC адресов. Если IP и MAC адреса в заголовках пакета соответствуют записям, имеющимся в таблице, то такой пакет считается правильным и на этом работа алгоритма анализа заканчивается.

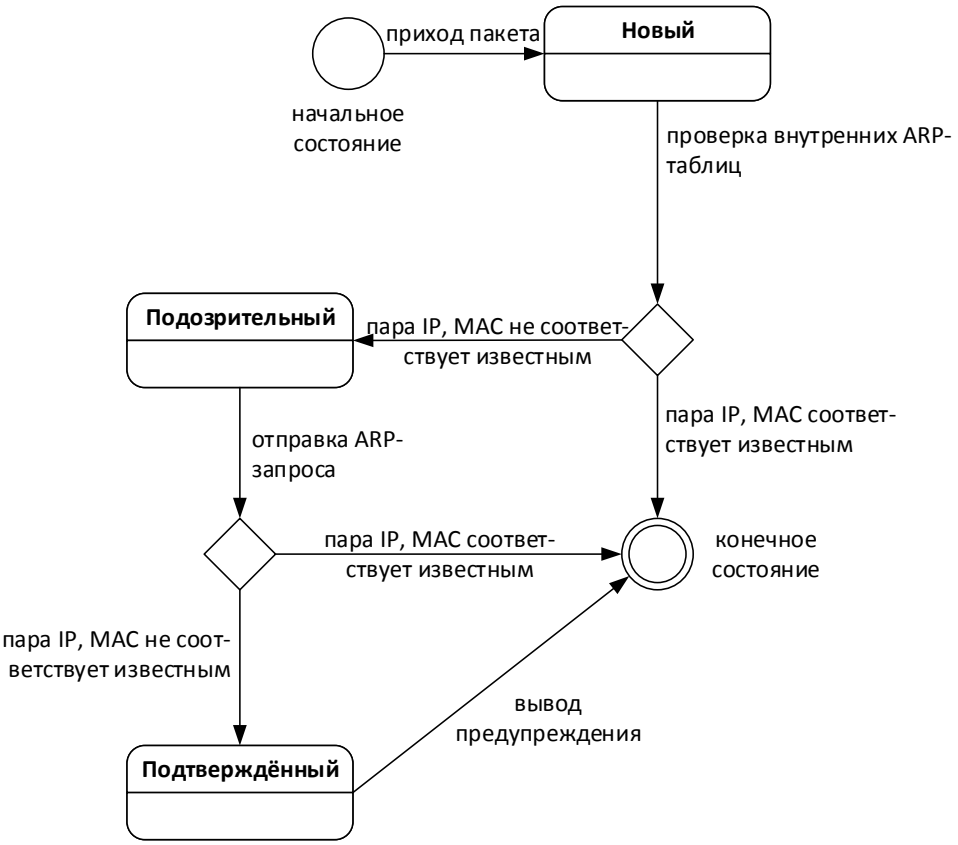


Рис. 5. – UML-диаграмма состояний пакета в процессе анализа

Если же IP и MAC адреса в заголовках пакета не соответствуют записям во внутренней таблице приложения, то пакету присваивается статус «подозрительный». Дело в том, что несоответствия могут возникнуть не только в результате сетевой атаки, но и в результате нормальных процессов функционирования сети, например, смены динамического IP-адреса узла по истечении срока аренды (MAC-адрес при этом остаётся неизменным) [9]. Для того, чтобы убедиться, что расхождения информации в пакете и в программе

вызваны действиями, не связанными с атакой, посылается ARP-запрос. Его цель — уточнить (или обновить) соответствие IP- и MAC-адресов, при этом подмена сразу двух этих адресов атакующей стороной невозможна, так как компьютер, реально имеющий, например, запрашиваемый IP-адрес всё равно пришлёт ответ, который получит программа, пусть и наряду с подменённым ответом. Сам факт прихода двух ответов с одинаковыми IP-адресами, но разными MAC-адресами свидетельствует о неправильном функционировании сети и скорее всего вызван именно атакой с целью подмены адреса [10].

По итогам запроса и результатам ответа на него, пакет переходит либо в состояние подтверждённого наличия промежуточного узла, либо алгоритм анализа завершается. При переходе в состояние «подтверждён» администратору выдаётся сообщение о том, что пакет прошёл через промежуточный узел, что означает, что все данные из него могли быть перехвачены злоумышленником.

Выводы

Представленный метод защиты от атак типа «человек посередине» позволяет обнаруживать пакеты, прошедшие через компьютер посредника в результате изменения адреса шлюза по умолчанию. В отличие от других способов он может быть использован на существующем компьютере, выполняющем функции интернет-шлюза, и не требует увеличения его производительности или установки дополнительного оборудования.

Единственным его недостатком является то, что для обнаружения атаки необходимо, чтобы хотя бы один пакет прошёл через компьютер злоумышленника, однако данный недостаток не является существенным благодаря большому количеству служебного трафика (DNS-, ARP-, ICMP-запросы), который всегда передаётся перед пользовательскими данными.

Литература

1. Владимирова Т.В. Сетевые коммуникации как источник информационных угроз // Социологические исследования. 2011. №5. С. 123-129.

2. Pandey, A. and J.R. Saini, 2012. A Simplified Defense Mechanism Against Man-In-TheMiddle Attacks. International Journal of Engineering Innovation & Research, 5(1): pp.385-389.

3. Галушка В.В., Баранцева В.А. Алгоритм обнаружения сетевых атак на основе подмены ответов DHCP-сервера // Инновационные технологии научного развития: сборник статей международной научно-практической конференции. Казань: АЭТЕРНА, 2017. С. 16-19.

4. Kumar, S. and Sh. Tapaswi, 2012. A centralized detection and prevention technique against ARP poisoning. Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), The Society of Digital Information and Wireless Communications (SDIWC), pp. 367-374.

5. Jerschow, Y.I., Ch. Lochert, B. Scheuermann and M. Mauve, 2008. CLL: A Cryptographic Link Layer for Local Area Networks. Security and Cryptography for Networks: 6th International Conference, Springer, pp. 21-38.

6. Ажмухамедов И.М., Марьенков А.Н. Поиск и оценка аномалий сетевого трафика на основе циклического анализа // Инженерный вестник Дона, 2012, №2. URL: ivdon.ru/ru/magazine/archive/n2y2012/742/.

7. Козьмовский Д.В., Куватов В.И., Примакин А.И. Методы анализа трафика и определения сетевой деятельности в вычислительных сетях в интересах контроля пользователей // Вестник Санкт-Петербургского университета МВД России. 2014. №1. С. 112-115.

8. Галушка В.В., Верхорубова Е.Д. Методы и средства выявления сетевых атак на основе анализа транзитных пакетов // Труды Северо-Кавказского

филиала Московского технического университета связи и информатики. 2016. №9. С. 298-303.

9. Бабенко Г.В., Белов Г.В. Анализ трафика TCP/IP на основе методики допустимого порога и отклонения // Инженерный вестник Дона, 2011, №2. URL: ivdon.ru/ru/magazine/archive/n2y2011/446/.

10. Скуратов А.К., Безрукавный Д.С. Администрирование телекоммуникационной сети на основе статистического анализа трафика // Вестник Тамбовского государственного технического университета. 2004. №4. С. 919-923.

References

1. Vladimirova T.V. Sotsiologicheskie issledovaniya. 2011. №5. pp. 123-129.

2. Pandey, A. and J.R. Saini, 2012. International Journal of Engineering Innovation & Research, 5(1): pp.385-389.

3. Galushka V.V., Barantseva V.A. Innovatsionnye tekhnologii nauchnogo razvitiya: sbornik statey mezhdunarodnoy nauchno-prakticheskoy konferentsii. Kazan', 2017. pp. 16-19.

4. Kumar, S. and Sh. Tapaswi, 2012. Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), The Society of Digital Information and Wireless Communications (SDIWC), pp. 367-374.

5. Jerschow, Y.I., Ch. Lochert, B. Scheuermann and M. Mauve, 2008. Security and Cryptography for Networks: 6th International Conference, Springer, pp. 21-38.

6. Azhmukhamedov I.M., Mar'enkov A.N. Inženernyj vestnik Dona (Rus), 2012, №2. URL: ivdon.ru/ru/magazine/archive/n2y2012/742/.

7. Koz'movskiy D.V., Kuvatov V.I., Primakin A.I. Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. 2014. №1. pp. 112-115.

8. Galushka V.V., Verkhorubova E.D. Trudy Severo-Kavkazskogo filiala Moskovskogo tekhnicheskogo universiteta svyazi i informatiki. 2016. №9. pp. 298-303.

9. Babenko G.V., Belov G.V. Inženernyj vestnik Dona (Rus), 2011, №2. URL: ivdon.ru/ru/magazine/archive/n2y2011/446/.

10. Skuratov A.K., Bezrukavnyy D.S. Vestnik Tambovskogo gosudarstvennogo tekhnicheskogo universiteta. 2004. №4. pp. 919-923.