ТЕХНОЛОГИЯ СОКРЫТИЯ КОНЕЧНОГО АДРЕСА DOMAIN FRONTING

Тюрин К.А.[1], Черкесова Л.В.[2], Сафарьян О.А.[3]

Сеть Интернет в современном представлении является очень большой и сложной системой, состоящей из множества промежуточных узлов, которые могут контролироваться различными людьми, организациями или государственными структурами. Этот факт предъявляет особенные требования к передаче данных, содержание которых может быть конфиденциальным. Существует большое число различных технологий, позволяющих скрывать содержимое передаваемых данных при помощи средств криптографии. Тем не менее, часто возникает задача сокрытия не только передаваемых данных, но и самого факта их передачи. Для достижения этой цели необходимо сокрыть факт обращения к ресурсу, на который (или с которого) будет производиться передача данных. В настоящее время для этого применяются технологии ретрансляции трафика в реальном времени, иначе называемые проксированием. Однако, использование узлов ретрансляции может не решать проблему полностью, к тому же требует сложных технических и административных мер по поддержке необходимой инфраструктуры ретрансляции. В статье предложено практическое применение метода построения туннеля ретрансляции, позволяющего скрывать факт обращения к удаленному ресурсу за обращением к публичным ресурсам. Этот метод заключается в особенности некоторых серверов перенаправлять принятые запросы по адресу, переданному через заголовки пакета запроса. Так как заголовки пакета могут быть зашифрованы целевой домен может быть скрыт за публичным. Несмотря на то, что обратиться таким образом к произвольному домену не представляется возможным, это позволяет разместить сервер ретрансляции в зоне, доверенной для публичного сервера. Такой сервер ретрансляции, в свою очередь, может осуществлять запросы к произвольным адресам. Экспериментальные исследования показали эффективность использования этого метода и возможность его применения для практических задач.

***Ключевые слова**: анонимизация, деанонимизация, прокси–сервер, система TOR, скрытая передача информации, глубокий анализ пакетов, системы обнаружения вторжений, системы предотвращения вторжений, сеть доставки содержимого, канал утечки информации, обход блокировок Интернет–ресурсов, meek, заголовки HTTP, TLS, HTTPS.*

DOI: 10.21681/2311-3456-2017-3-43-48

Введение. С ростом и развитием интернет–технологий возникли требования по их регулированию. Сеть Интернет представляет собой развитую инфраструктуру и становится важным контроль доступа пользователей к различным ресурсам. В частности, появляются задачи ограничения доступа или установления факта обращения пользователей к конкретным ресурсам. Такие мероприятия производятся в различных масштабах, начиная от небольших корпоративных сетей и заканчивая государственным уровнем. Необходимость контроля объясняется требованиями к безопасности.

Так, для корпоративных сетей важным является устранение возможности утечки конфиденциальной информации, что выделяет две важные подзадачи: предотвращение вторжения злоумышленника и вредоносного ПО во внутреннюю сеть и предотвращение отправки чувствительной информации сотрудниками.

Для государственных нужд контроль передачи информации необходим с целью обнаружения преступных действий. Как правило, контроль осуществляется путем анализа передаваемого трафика.

В качестве другой меры обеспечения безопасности на различных уровнях применяются методы блокировки доступа к ресурсам [1]. Их можно разделить на две категории: «белые» и «черные» списки.

Наличие «черных» списков подразумевает запрет доступа пользователей на определенные ресурсы, в то время как доступ к ресурсам, отсутствующим в этом списке, не подвергается ограничению. Политика «белых» списков является более строгой за счет того, что доступ к произвольному

1 Тюрин Кай Андреевич, научный сотрудник, Федеральное государственное автономное научное учреждение «Научно-исследовательский институт «Специализированные вычислительные устройства защиты и автоматика» (ФГАНУ НИИ «Спецвузавтоматика»), Ростов–на– Дону, Россия. E-mail: kayvflu@gmail.com

2 Черкесова Лариса Владимировна, профессор, доктор физико–математических наук, Донской государственный технический университет, Ростов–на–Дону, Россия. E-mail: chia2002@inbox.ru

3 Сафарьян Ольга Александровна, доцент, кандидат технических наук, Донской государственный технический университет, Ростов–на–Дону, Россия. E-mail: safari_2006@mail.ru

ресурсу по умолчанию запрещен, за исключением ресурсов, находящихся в списке. Таким образом, можно выделить следующие возможные варианты стороннего наблюдателя:

- локальный администратор сети;
- IDS (англ. Intrusion Detection System — системы обнаружения вторжений) — программное обеспечение, предназначенное для анализа сетевых соединений и передаваемых через них данных с целью обнаружения попыток проникновения злоумышленником [2];
- IPS (англ. Intrusion Prevention System — системы предотвращения вторжений) — программное обеспечение, обладающее функционалом IDS, которое, кроме возможности обнаружения вторжений, предоставляет также возможность автоматизированного противодействия с целью защиты внутренней сети [3];
- DLP (англ. Data Leak Prevention — предотвращение утечек информации) — системы анализа передаваемых пользователем во внешнюю сеть данных, совершающие их анализ на предмет чувствительной информации [4];
- системы обнаружения аномалий — программное обеспечение, предназначенное для анализа действий пользователя и обнаружения отклонений в его поведении [5];
- СОРМ (Системы оперативно-розыскных мероприятий) — аппаратно-программные комплексы, предназначенные для анализа передаваемых пользователями сети данных [6];
- другие системы и субъекты сети, имеющие доступ к передаваемым данным.

При разработке методов построения скрытых каналов передачи необходимо учитывать, что все вышеперечисленные варианты стороннего наблюдателя могут использовать технологии DPI (англ. Deep Packet Inspection – глубокий анализ пакета), которые позволяют анализировать не только заголовки, но и содержимое передаваемых пакетов [7].

Несмотря на то, что контроль передаваемой информации производится с целью обеспечения безопасности, существуют ситуации, в которых необходимо сохранить конфиденциальность передаваемых данных и скрыть факт их передачи. В качестве противодействия методам ограничения или контроля доступа к ресурсу используется технология ретрансляции сетевого трафика через промежуточные узлы сети.

Однако технологии ретрансляции сетевого трафика в большинстве случаев не обладают способами сокрытия факта их использования от стороннего наблюдателя. Так, обращение к некоторому прокси –серверу может расцениваться как аномальное поведение для пользователя (особенно если при этом необходимо пользоваться нетипичным для данного пользователя протоколом). Регулярность обращения так же может представлять собой подозрительное поведение.

В данной статье рассматривается именно задача сокрытия подключения к первому узлу цепочки ретрансляции (или единственному).

Перед тем, как рассматривать методы сокрытия использования средств ретрансляции, необходимо рассмотреть основные стратегии их использования.

Основные методы использования технологий ретрансляции. К системам ретрансляции могут применяться различные требования в зависимости от поставленных задач. Рассмотрим подробнее проксирование трафика на примере трех основных векторов его применения: анонимизация, обход блокировок ресурсов и сокрытие обращения.

Применение технологии ретрансляции трафика в рамках задач анонимизации основывается на том факте, что свойства профиля пользователя, информация о котором известна ресурсу назначения, будут отличаться от свойств клиента (например, ресурс будет обладать информацией об IP-адресе последнего узла цепочки ретрансляции, а не о настоящем адресе пользователя).

Обход блокировки ресурса подразумевает, что для пользователей из определенного государства (или пользователей определенной сети) может быть запрещен доступ к некоторому ресурсу. Тем не менее, они могут иметь свободный доступ к использованию некоторого узла ретрансляции, который, в свою очередь, может иметь доступ к ресурсу. В таком случае компьютер пользователя и узел ретрансляции находятся в различных сегментах сети.

В рамках задачи сокрытия посещения ресурса становится необходимо «замаскировать» использование одного ресурса под использование другого. При этом может быть несущественным, что будет знать о пользователе сам ресурс. Также не является значимым наличие или запрет непосредственного доступа к ресурсу из локальной сети пользователя.

Несмотря на то, что сокрытие факта посещения часто является одним из этапов анонимизации, в данной работе эти задачи рассматриваются отдельно.

Domain Fronting. Рассматриваемая в статье технология основывается на особенности протокола HTTPS. Пакеты данного протокола содержат два набора заголовков. Часть заголовков, относящихся к протоколу TLS [8], находятся в открытой части сообщения, в то время как другая часть, относящаяся к протоколу HTTP, находится в зашифрованной части пакета. В обоих множествах заголовков существует поле, содержащее доменное имя ресурса назначения, значения которого могут отличаться в пределах одного пакета. Стороннему наблюдателю доступно только открытое множество заголовков. Таким образом, возможно скрывать реальный адрес обращения в шифрованную область HTTPS-пакета, в то время как открытая часть содержит адрес другого сервера, обращение к которому не запрещено.

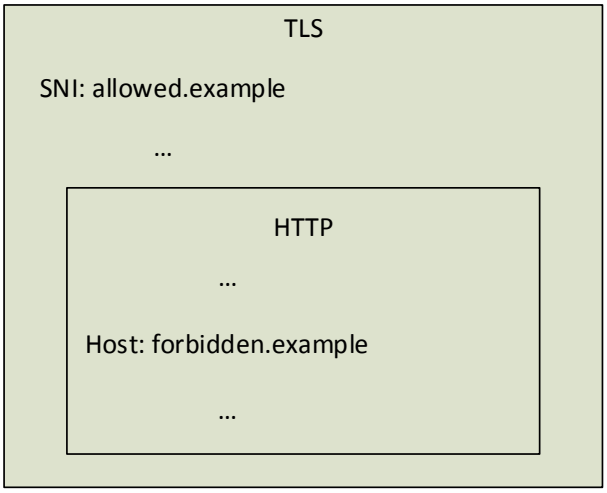

Рис. 1. *Схематичное изображение HTTPS пакета*

На рисунке 1 изображено схематичное изображения HTTPS пакета, где протокол TLS инкапсулирует HTTP. Протокол TLS содержит заголовок SNI (Server Name Indication) — указание имени сервера. Этот заголовок используется для аутентификации и содержит адрес сервера, к которому напрямую подключается клиент. Так как значение заголовка SNI совпадает с реальным адресом сервера, оно не представляет никакого интереса для стороннего наблюдателя. В свою очередь, зашифрованный HTTP пакет не доступен для наблюдателя и может содержать в качестве значения заголовка Host доменное имя (или адрес) ресурса, к которому клиент действительно хочет произвести запрос. При получении такого пакета ресурс, обладающий необходимым функционалом, может ретранслировать запрос на нужный сервер.

Для использования исследуемого метода на практике возникает необходимость в наличии разрешенного домена, позволяющего получить доступ к узлу ретрансляции. В качестве таких серверов могут применяться ресурсы, использующие технологию CDN (Content Delivery Network — Сеть доставки данных), в основе которой лежит идея распределения серверов отправки данных для сглаживания географических и региональных особенностей обращения клиентов к ресурсам [9]. Так, обращение к одному и тому же ресурсу из различных мест может повлечь за собой получение ответа с ближайших серверов (за счет технологии anycast), несмотря на то, что со стороны клиента соединение выглядит так же, как и при соединении с единственным сервером (за счет технологии проксирования). Таким образом, благодаря Domain Fronting можно обращаться к общеизвестному домену, отправляя через него запросы к узлу ретрансляции, который, в свою очередь, может осуществлять соединение с запрещенными ресурсами.

В качестве примеров использования CDN можно представить облачных провайдеров, например, Google, Amazon или Azure. Они могут предоставлять доступ к серверам приложений, размещенных в их инфраструктуре.

Существующие реализации. Описываемая в данной статье технология используется в пакете расширения возможностей системы анонимизации Tor [10]. Этот пакет называется meek и состоит из нескольких частей:

- meek–client реализует возможность соединения с сетью Tor с использованием Domain Fronting на стороне клиента;
- meek–browser–client предназначен для решения проблемы возможности обнаружения

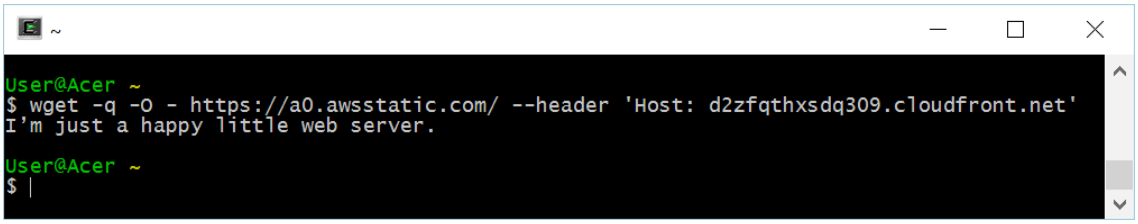

Рис.2. *Пример обращения к ресурсу*

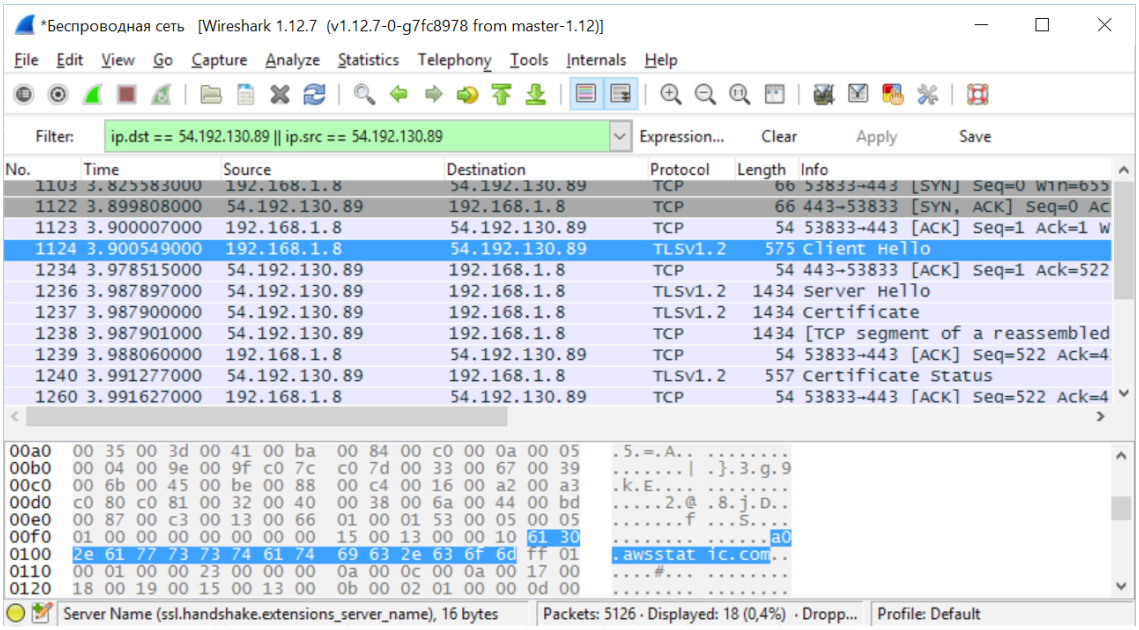

Рис.3. *Доменное имя в клиентском пакете*

использования технологии Domain Fronting на основе анализа TLS-отпечатков;

- meek server устанавливается на сервер в инфраструктуре CDN и служит для проксирования соединения ко входным узлам сети Tor.

На момент написания статьи пакет meek поддерживает использование следующих CDN:

Google App Engine (meek–google);

Amazon CloudFront (meek–amazon);

Microsoft Azure (meek–azure).

Экспериментальное исследование.

Для проверки использования данного метода было произведено обращение к серверу meek, находящемуся в CDN Amazon CloudFront (рис.2).

Весь трафик, передаваемый в процессе данного соединения, был записан при помощи ПО Wireshark 1.12.7. Анализ пакетов показал, что они не содержат информации о ресурсе, с которого были непосредственно получены данные.

При этом пакеты, передаваемые в начале сессии, содержат доменное имя сервера CDN (рис. 3, 4).

Выводы. Рассмотренная в данной статье технология Domain Fronting может быть использована для сокрытия факта обращения к определенному ресурсу или для обхода блокировок, использующих анализ содержимого передаваемых пакетов. Данный метод может быть полезен для задач:

1. Анонимизации. Сокрытие факта использования средств ретрансляции и маскирование сессии усложняет задачу сопоставления пользователя и ресурса.

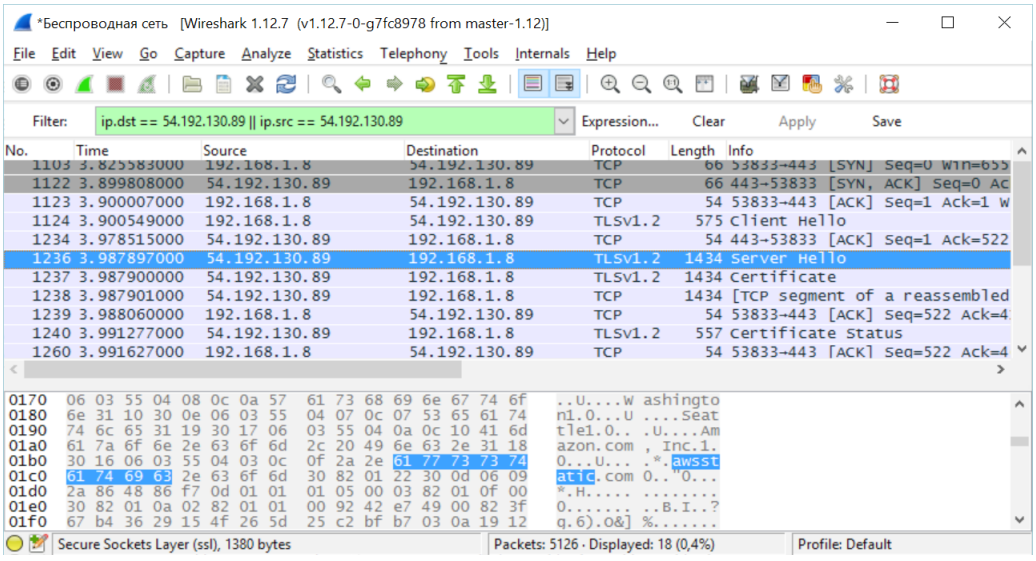

Рис.4. *Доменное имя в серверном пакете*

2. Обхода блокировок. Изменение назначения запроса на удаленном сервере и шифрование содержимого не позволяет провайдеру запретить доступ к ресурсу, так как с его стороны соединение будет выглядеть легитимным.

3. Сокрытие факта посещения. Подключение через прокси такого типа не вызывает подозрений у администратора сети или средств контроля. Таким образом, Domain Fronting может применяться для построения скрытых (или маскированных) каналов передачи информации.

На текущий момент времени не существует устойчивых способов противодействия использованию данного метода.

Рецензент: *Габриэльян Дмитрий Давыдович, профессор, доктор технических наук, заместитель начальника по науке научно–производственного комплекса ФГУП «Ростовский НИИ Радиосвязи», г. Ростов-на-Дону, Россия. E–mail: d.gabrieljan2011@yandex.ru*

Литература:

1. Костырная О.Г., Максимов П.В. Ограничение доступа к сети Интернет: правовые аспекты и техническая реализация. Екатеринбург. Международный научно-исследовательский журнал. 2014. № 8-1 (27). С. 60 – 61.
2. Слугин И.А. Регуляция сетевого пространства в России: текущая ситуация и возможные перспективы. // Бизнес. Общество. Власть. М.: Национальный исследовательский университет «Высшая школа экономики». 2012. №12. С. 95-105.
3. Силантьева К.Ю. Системы обнаружения вторжений (IDS): Сборник статей международной научно–практической конференции, Уфа, 2015. С. 78 – 80.
4. Дугин Андрей Проектирование инфраструктуры IDS/IPS. архитектура сетевых систем // Системный администратор. М.: Синдикат 13. 2012. № 1 – 2 (110 – 111). С. 64–66.
5. Фаткиева Р. Р. Разработка метрик для обнаружения атак на основе анализа сетевого трафика. // Вестник Бурятского государственного университета. Математика, информатика. – 2013. – Вып. 9. – С. 81–86.
6. Слугин И.А. Регуляция сетевого пространства в России: текущая ситуация и возможные перспективы // Бизнес. Общество. Власть. М.: Национальный исследовательский университет «Высшая школа экономики». 2012. № 12. С. 95 – 105.
7. Чемодуров А.С., Карпутина А. Ю. Обзор средств фильтрации трафика в корпоративной сети // Научно–методический электронный журнал Концепт. Киров: Межрегиональный центр инновационных технологий в образовании. 2015. № 2. С. 71 – 75.
8. Рахманова З.Ч. Применение SSL/TLS–протокола и других способов защиты данных в WEB-приложениях: сб. научн. тр. Информационные технологии в экономике и управлении. Махачкала: Дагестанский государственный технический университет. 2015. С. 51 – 57.
9. Южанинов Р.И., Кокоулин А.Н., Даденков С.А. Сравнительный анализ методов моделирования сети доставки контента (CDN) // Наука и бизнес: пути развития. Тамбов: Фонд развития науки и культуры. 2016. №3. С. 42 – 44.
10. Кузичкина О.А. Сеть TOR как способ подключения к «глубокому» интернету // Интеллектуальный потенциал XXI века: ступени познания. Новосибирск: Общество с ограниченной ответственностью «Центр развития научного сотрудничества». 2014. № 25. С. 129–131.

THE TECHNOLOGY OF HIDING THE DESTINATION ADDRESS DOMAIN FRONTING

K. Tyurin[4], L. Cherckesova[5], O. Safaryan[6]

Modern Internet network is big and complex system that consists of many intermediate nodes. These nodes may be under the control of different people, organizations or governments. Because of this, the data transfer is very important to be confidential. There are exist many technologies that provide to encrypt data with cryptography methods. But some cases require hiding not only data but the fact of transferring. To do this it is necessary to disguise the requesting resource. For this purpose are used technologies of real–time traffic relaying. These technologies are called proxying. But using of proxy servers may not completely solve the problem and require technical and administrative measures to maintain the relaying infrastructure. In this paper, we present the application of creating a relaying tunnel that masks request to the forbidden re–

4 Kay Tyurin, researcher, «Federal State Autonomous Scientific Establishment «Scientific Research Institute «Specialized Security Computing Devices and Automation» (FSASE «Spetsvuzavtomatika»), Rostov–on–Don, Russia. E-mail: kayvflu@gmail.com

5 Larissa Cherckesova, Dr. Sc., Prof., Don State Technical University, Rostov–on–Don, Russia. E-mail: chia2002@inbox.ru

6 Olga Safaryan, Ph.D., Associate Professor, Don State Technical University, Rostov–on–Don, Russia. E-mail: safari_2006@mail.ru

sources with the public resources. This method is based on the fact that some servers could redirect some requests to the address from request header. It cause opportunity to hide required domain behind the public one. One cannot make request to arbitrary address this way, but it possible to place some retranslation server in some public server trust zone. This proxy–server should allow to connect to any Internet address. Experimental research showed that this method can be used for any practical needs.

***Keywords**: anonymization, deanonymization, proxy –server, TOR system, hidden data transfer, deep packet inspection, intrusion prevention system, intrusion detection system, content delivery network, data leak channel, bypassing the Internet resources block, meek, HTTP headers, TLS, HTTPS.*

References

1. Kostyrnaya O.G., Maksimov P.V. Ogranichenie dostupa k seti Internet: pravovye aspekty i tekhnicheskaya realizaciya. Ekaterinburg. Mezhdunarodnyj nauchno – issledovatel'skij zhurnal. 2014. № 8–1 (27). Pp. 60–61.
2. Slugin I.A. Regulyaciya setevogo prostranstva v Rossii: tekushchaya situaciya i vozmozhnye perspektivy. // Biznes. Obshchestvo. Vlast'. Moscow.: Nacional'nyj issledovatel'skij universitet «Vysshaya shkola ehkonomiki». 2012. №12. Pp. 95 – 105.
3. Silant'eva K.YU. Cistemy obnaruzheniya vtorzhenij (IDS): Sbornik statej mezhdunarodnoj nauchno-prakticheskoj konferencii, Ufa, 2015. Pp. 78 – 80.
4. Dugin Andrej Proektirovanie infrastruktury IDS / IPS. arhitektura setevyh system // Sistemnyj administrator. M.: Sindikat 13. 2012. № 1–2 (110–111). Pp. 64 – 66.
5. Fatkieva R.R. Razrabotka metrik dlya obnaruzheniya atak na osnove analiza setevogo trafika // Vestnik Buryatskogo gosudarstvennogo universiteta. Matematika, informatika, 2013, iss. 9, pp. 81-86.
6. Slugin I.A. Regulyaciya setevogo prostranstva v Rossii: tekushchaya situaciya i vozmozhnye perspektivy // Biznes. Obshchestvo. Vlast'. Moscow: Nacional'nyj issledovatel'skij universitet «Vysshaya shkola ehkonomiki». 2012. № 12. Pp. 95–105.
7. Chemodurov A., Karputina A. Obzor sredstv fil'tracii trafika v korporativnoj seti // nauchno-metodicheskij ehlektronnyj zhurnal Koncept. Kirov: Mezhregional'nyj centr innovacionnyh tekhnologij v obrazovanii. 2015. № 2. Pp. 71–75.
8. Rahmanova Z.CH. Primenenie SSL/TLS-protokola i drugih sposobov zashchity dannyh v WEB-prilozheniyah: sb. nauchn. tr. Informacionnye tekhnologii v ehkonomike i upravlenii. Mahachkala: Dagestanskij gosudarstvennyj tekhnicheskij universitet. 2015. Pp. 51 – 57.
9. Yuzhaninov R.I., Kokoulin A.N., Dadenkov S.A. Sravnitel'nyj analiz metodov modelirovaniya seti dostavki kontenta (CDN) // Nauka i biznes: puti razvitiya. Tambov: Fond razvitiya nauki i kul'tury. 2016. №3. Pp. 42 – 44.
10. Kuzichkina O.A. Set' TOR kak sposob podklyucheniya k «glubokomu» internetu // Intellektual'nyj potencial XXI veka: stupeni poznaniya. Novosibirsk: Obshchestvo s ogranichennoj otvetstvennost'yu «Centr razvitiya nauchnogo sotrudnichestva». 2014. № 25. Pp. 129 – 131.