Copyright © 2015 by Academic Publishing House *Researcher*

Published in the Russian Federation
European Journal of Computer Science
Has been issued since 2015.
ISSN: 2412-2033
Vol. 1, Is. 1, pp. 34-40, 2015

DOI: 10.13187/ejcs.2015.1.34
www.ejournal39.com

UDC 004.41

The Use of Technology for Traffic Anonymization Exposure to Information Resources

[1] Sergei D. Karpov
[2] Igor A. Spivak

[1] Military Academy of the Strategic Missile Forces to them, Russian Federation
Karbysheva street, Balashikha city, 143900
PhD (technical), associate professor
E-mail: kds-zn@mail.ru
[2] NCCD of the Russian Federation, Russian Federation
Znamenka street, 19, Moscow city, 119160
E-mail: kavips24@yandex.ru

Abstract

The article offers a perspective, an effective and relatively simple method based on the joint use of technologies of anonymity TOR and secure information exchange VRN, the use of which will allow the anonymous "surfing" on the Internet and to actively influence the information resursy having access to the global information and telecommunications network the Internet.

Keywords: Internet, information resources, traffic.

Введение

Развитие человечества характеризуется определенными скачкообразными этапами развития, различными по продолжительности и содержанию. Каждый этап такого развития сопровождался появлением новых видов оружия, все более разрушительного: механического, огневого, химического, биологического, ядерного. Современный уровень развития человечества подошел к такой черте, когда использование оружия массового поражения для уничтожения живой силы и объектов становится неприемлемым по многим причинам: нарушение экологии, массовая гибель гражданского населения, разрушение инфраструктуры и т.п. Возникшие между развитыми и развивающимися государствами глубокие противоречия, причиной которых является борьба за обладание сырьевыми, энергетическими, людскими ресурсами, запасами питьевой воды, продуктов питания, можно разрешить, как считают руководители развитых стран, путем применения информационного оружия. Воздействие данного оружия на человека, общество и государство, технические системы управления любыми процессами во многих случаях незаметно, а последствия сравнимы с применением оружия массового поражения.

Результаты

В настоящее время большинство развитых стран мира обладает теми или иными образцами информационного оружия, и находятся в состоянии информационного соперничества или информационного противостояния.

Сферой информационного противостояния является телевидение, радио, пресса, а самые напряженные сражения идут в Интернет-пространстве: в информационных системах государственных и крупных коммерческих структур, имеющих выход в сеть Интернет, Интернет-сайтах, зарегистрированных как средства массовой информации, в социальных сетях, информационных блогах, новостных лентах и т.п.

Вышеуказанные обстоятельства обусловили возникновение потребности в разработке новых способов и специализированных программно-технических средств воздействия на информационные ресурсы, имеющие выход в глобальную информационно-телекоммуникационную сеть Интернет.

Способ воздействия на информационные ресурсы, имеющие выход в сеть Интернет

Способ воздействия на информационные ресурсы, имеющие выход в сеть Интернет может быть основан на совместном использовании технологии анонимности TOR и технологии защищенного обмена информацией VPN.

Технология TOR (от англ. *The Onion Router* – луковый маршрутизатор) представляет собой свободное программное обеспечение для анонимизации трафика (удаления или сокрытия данных в сети с целью предотвращения идентификации источника трафика и места назначения).

Открытый исходный код – один из самых главных факторов, позволяющих своевременно выявить всевозможные дефекты программного обеспечения и невозможность тайного встраивания в него «черных ходов» специальных служб.

Технология TOR – это совокупность взаимодействия многих серверов сети, каждый из которых предоставляет часть ресурсов своего Интернет-подключения для нужд сети. Данный принцип работы близок к принципу работы пиринговых сетей. Любой пользователь может быть сервером, отдавая часть ресурсов для развития анонимной сети, и, тем самым, улучшая свою собственную анонимность. TOR случайно выбирает несколько серверов из всех доступных (список которых он периодически скачивает с центрального сервера) и строит «тоннель», проходящий через эти промежуточные точки. Трафик пропускается через этот тоннель, у него есть вход – приложение TOR на машине и выход – последний из случайно выбранных для этого тоннеля серверов сети TOR. Передаваемый пакет данных последовательно зашифровывается открытыми ключами серверов, входящих в цепочку, начиная с её конца. При этом компьютер непосредственно отсылает данные на первый сервер в этой цепи, который снимает с данных свой слой шифра и передаёт их далее, а с реальной точкой назначения, непосредственно общается сервер, служащий точкой выхода из тоннеля.

Применение технологии TOR позволяет защитить пользователя от слежки и возможных негативных последствий посещения любого информационного ресурса в сети Интернет. Применяя TOR, на сервере информационного ресурса невозможно выяснить IP-адрес и местонахождение пользователя. Серверы-посредники получают только ограниченные необходимые сведения. Например, первый сервер сети TOR, выбранный для тоннеля, с которым идет взаимодействие напрямую, не может точно определить, предназначены ли данные для потребителя или компьютер всего лишь является посредником для кого-то другого. Сокрытие информации так, чтобы каждый элемент цепи имел доступ только к той части, которая предназначена ему, реализуется с помощью проработанного и надежного метода шифрования - криптографии с открытыми ключами. Даже если сервер сети TOR находится под контролем противника, тот не может получить доступ к части информации, предназначенной для следующих серверов тоннеля (рис. 1).

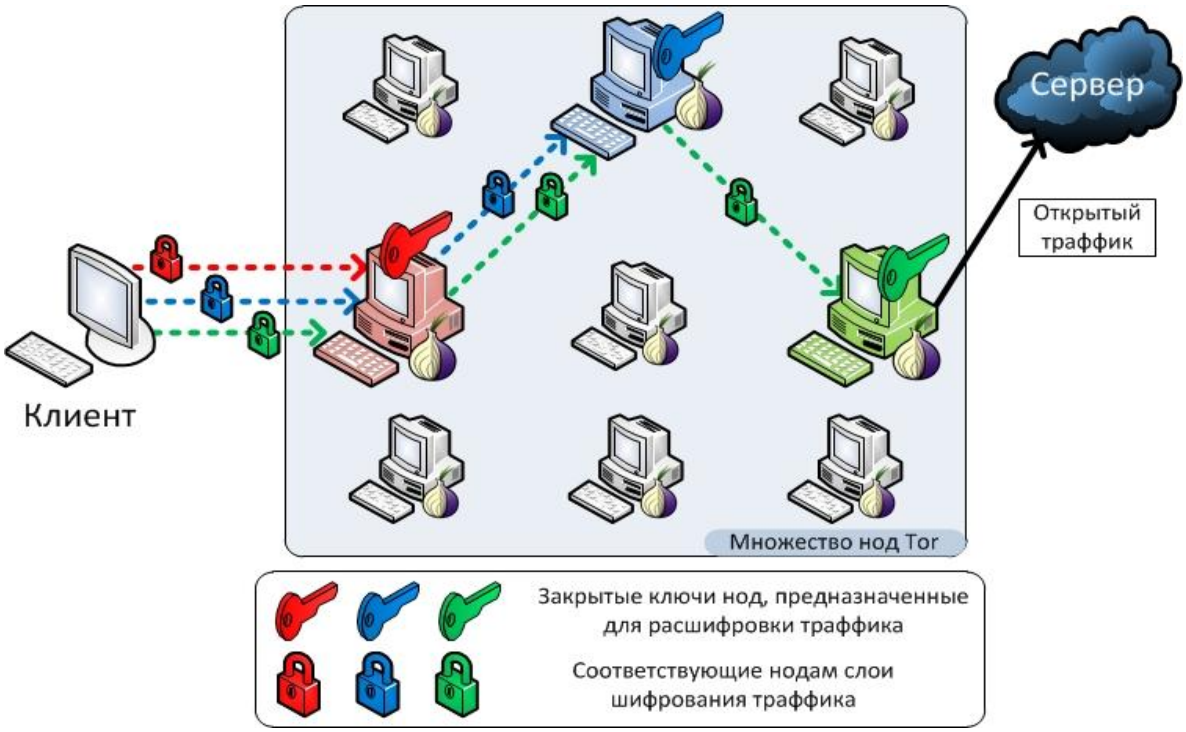

Рис. 1. Схема использования технологии TOR для анонимизации трафика

Таким образом, технология TOR решает свою главную задачу: обеспечивает высокий уровень анонимности пользователя при передаче http-траффика и известной модели угроз, при условии соблюдения всех обязательных правил.

Технология VPN (от англ. *Virtual Private Network* – виртуальная частная сеть) – это технология которая создает логическую сеть поверх другой сети. Несмотря на то, что коммуникации осуществляются по публичным сетям с использованием небезопасных протоколов, за счёт шифрования создаются закрытые, от посторонних, каналы обмена информацией. VPN позволяет объединить, например, несколько пользователей в единую сеть с использованием для связи между ними высокозащищенных каналов.

По своей сути VPN обладает многими свойствами выделенной линии, однако развертывается она в пределах общедоступной сети, например, сети Интернет. С помощью тоннелирования пакеты данных транслируются через общедоступную сеть как по обычному двухточечному соединению. Между каждой парой «отправитель – получатель данных» устанавливается своеобразный тоннель – безопасное логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого (рис. 2).

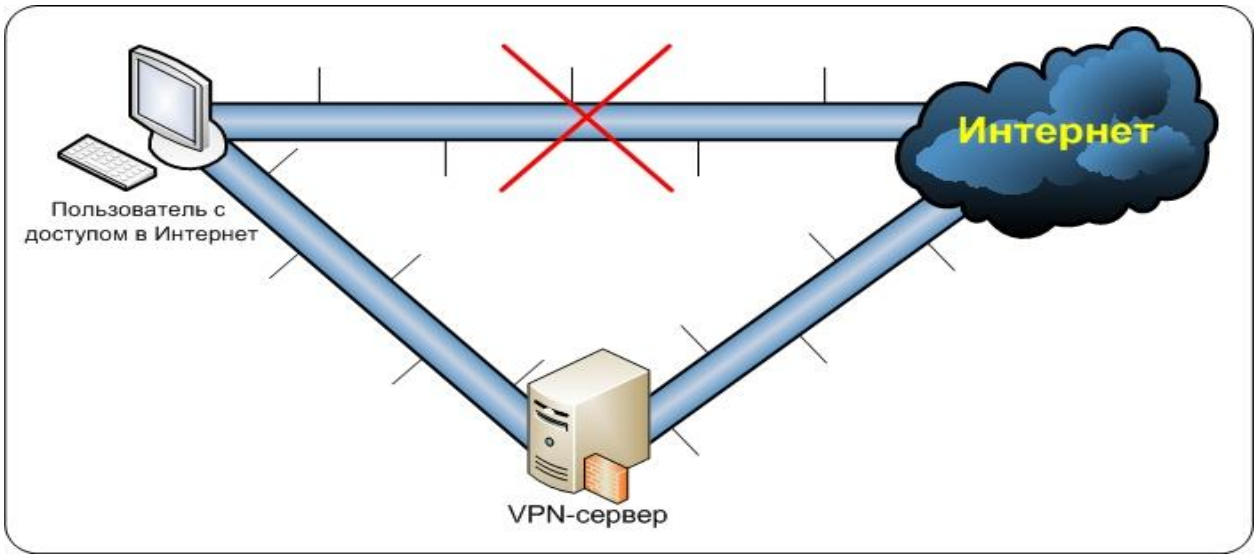

Рис. 2. Использование VPN-сервера для организации защищенного канала выхода в сеть Интернет

Принцип работы VPN не противоречит основным сетевым технологиям и протоколам. Например, при установлении соединения удаленного доступа клиент посылает серверу поток пакетов стандартного протокола PPP. В случае организации виртуальных выделенных линий между локальными сетями их маршрутизаторы также обмениваются пакетами PPP. Тем не менее, принципиальным моментом является пересылка пакетов через безопасный тоннель, организованный в пределах общедоступной сети.

Совместное использование различных информационных технологий является одним из известных подходов к построению и совершенствованию информационных систем [1-5]. С целью разработки способа воздействия на информационные ресурсы, имеющие выход в глобальную информационно-телекоммуникационную сеть Интернет, предлагается объединить рассмотренные информационные технологии TOR и VPN. Рассмотрим более подробно предлагаемую схему реализации способа (рис. 3).

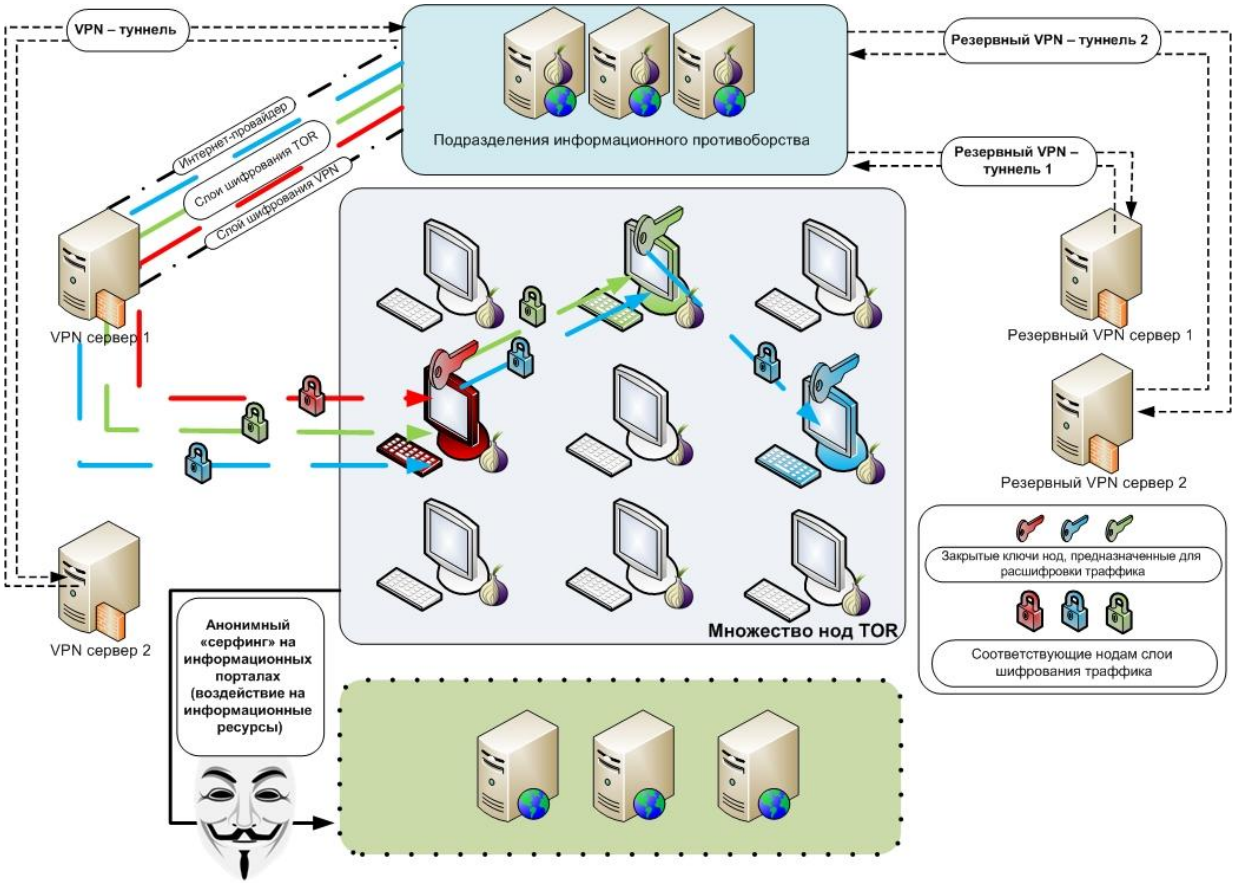

Рис. 3. Схема реализации способа воздействия на информационные ресурсы, имеющие выход в сеть Интернет

В предлагаемой схеме реализации способа воздействия на информационные ресурсы VPN-сервер является постоянным входным узлом подразделения информационного противоборства. Шифрованный трафик отправляется в сеть TOR исключительно с VPN-сервера.

На практике схема может быть реализована следующим образом: сначала производится подключение к VPN-серверу, далее запускается TOR-браузер, который автоматически настраивает нужную маршрутизацию через VPN-тоннель.

Совместное использование технологий TOR и VPN позволяет компенсировать их недостатки, скрыть факт использования технологии TOR и защитить выходной трафик от Интернет-провайдера, веб-сервера, а также других пользователей сети, включая вероятных противников. Учитывая необходимость доверять VPN-серверу, а в данном случае без применения специальных средств это невозможно – применяется технология анонимности TOR. Поэтому в случае взлома VPN-сервера и получения персональных данных, пользователь останется анонимным в сети и неизвестным для злоумышленника. А в случае теоретической компрометации TOR, защиту обеспечит рубеж VPN. Важно также отметить, что любой выходной узел легко выделит клиента в общем потоке, так как большинство пользователей идут на разные ресурсы, а при использовании подобной схемы клиент идёт всегда на один и тот же VPN-сервер, поэтому предлагается использовать ряд резервных VPN-серверов с целью «запутывания» маршрута исходящих пакетов.

Заключение

Таким образом, предлагается перспективный, эффективный и достаточно простой способ, основанный на совместном использовании технологий анонимности TOR и защищенного обмена информацией VPN, применение которого позволит осуществлять анонимный «серфинг» в сети Интернет и активно воздействовать на информационные

ресурсы, имеющие выход в глобальную информационно-телекоммуникационную сеть Интернет.

Примечания:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов. 4-е изд., испр. и доп. СПб.: ПИТЕР, 2010. 900 с.

2. Викиучебник //: Защита конфиденциальных данных и анонимность в интернете [Электронный ресурс, 2015 г.]. URL: https://ru.wikibooks.org/ wiki/ Защита_конфиденциальных_данных_и_анонимность_в_интернете (дата обращения 01.02.2015 г.).

3. TOR Bug Tracker & Wiki //: Installing and Configuring TOR [Электронный ресурс, 2015 г.]. URL: https://trac.TORproject.org/projects/TOR (дата обращения 20.01.2015 г.).

4. Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A. About one approach to a question of classification of intellectual systems of information security // Modeling of Artificial Intelligence. 2014. № 1 (1). p. 29-44.

5. Simonyan A.R., Simonyan R.A., Ulitina E.I. Waiting time in the elementary multichannel queue system with different intensity service of calls and with expectation // European researcher. Series A. 2011. № 5-1 (7). p. 533-536.

6. Карпов Д.С., Роганов А.А., Федорищев О.Н., Борисов Р.С. Системы передачи информации. - учебное пособие по специальности 230201 "Информационные системы и технологии". М.: ФГБОУВПО РГУТиС, 2013. 136 с.

7. Карпов Д.С. Повышение эффективности планирования навигационных определений объектов ракетной техники в ходе летного эксперимента // Военная мысль. 2013. № 2. С. 24-30.

References:

1. Olifer V.G., Olifer N.A. Komp'yuternye seti. Printsipy, tekhnologii, protokoly. Uchebnik dlya vuzov. 4-e izd., ispr. i dop. SPb.: PITER, 2010. 900 c.

2. Bikiuchebnik //: Zashchita konfidentsial'nykh dannykh i anonimnost' v internete [Elektronnyi resurs, 2015 g.]. URL: https://ru.wikibooks.org/ wiki/ Zashchita_ konfidentsial'nykh_dannykh_i_anonimnost'_v_internete (data obrashcheniya 01.02.2015 g.).

3. TOR Bug Tracker & Wiki //: Installing and Configuring TOR [Elektronnyi resurs, 2015 g.]. URL: https://trac.TORproject.org/projects/TOR (data obrashcheniya 20.01.2015 g.).

4. Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A. About one approach to a question of classification of intellectual systems of information security // Modeling of Artificial Intelligence. 2014. № 1 (1). p. 29-44.

5. Simonyan A.R., Simonyan R.A., Ulitina E.I. Waiting time in the elementary multichannel queue system with different intensity service of calls and with expectation // European researcher. Series A. 2011. № 5-1 (7). p. 533-536.

6. Karpov D.S., Roganov A.A., Fedorishchev O.N., Borisov R.S. Sistemy peredachi informatsii. - uchebnoe posobie po spetsial'nosti 230201 "Informatsionnye sistemy i tekhnologii". M.: FGBOUVPO RGUTiS, 2013. 136 s.

7. Karpov D.S. Povyshenie effektivnosti planirovaniya navigatsionnykh opredelenii ob"ektov raketnoi tekhniki v khode letnogo eksperimenta // Voennaya mysl'. 2013. № 2. S. 24-30.

УДК 004.41

Использование технологий анонимизации трафика для воздействия на информационные ресурсы

[1] Дмитрий Сергеевич Карпов
[2] Андрей Игоревич Спивак

[1] Военная академия РВСН им. Петра Великого, Российская Федерация
ул. Карбышева, 8, г. Балашиха, 143900
Кандидат технических наук, доцент
E-mail: kds-zn@mail.ru
[2] НЦУО РФ, Российская Федерация
ул. Знаменка, д. 19, г.Москва, 119160
старший преподаватель
E-mail: kavips24@yandex.ru

Аннотация. В статье предлагается перспективный, эффективный и достаточно простой способ, основанный на совместном использовании технологий анонимности TOR и защищенного обмена информацией VPN, применение которого позволит осуществлять анонимный «серфинг» в сети Интернет и активно воздействовать на информационные ресурсы, имеющие выход в глобальную информационно-телекоммуникационную сеть Интернет.

Ключевые слова. Интернет, информационные ресурсы, трафик.