ИДЕНТИФИКАЦИЯ HTTPS-СОЕДИНЕНИЯ СЕТИ «TOR» ВЕРСИИ TLS V1.3

Лапшичёв В.В.[1], Макаревич О.Б.[2]

Цель работы: *составление набора признаков, позволяющих выявить и идентифицировать установление соединения между клиентом и анонимной сетью «Tor» в условиях применения шифрования потока данных по протоколу TLS v1.3.*

Метод: *применялся программный анализ потока данных, частотные методы, декомпозиция содержимого пакетов данных по признакам их количества, порядка следования, нахождения фреймов в пакете и размерам, сравнительный метод в отношении различных версий протокола шифрования и ресурсов, осуществляющих соединение.*

Полученные результаты: *составлен набор признаков соединения сети «Tor», устанавливаемого с использованием шифрования TLS v1.3, позволяющий выявить и идентифицировать в потоке данных «рукопожатие» между клиентом и сетью «Tor» в целях законного блокирования соединения; проведен сравнительный анализ данных сети «Tor» и соцсети «ВКонтакте» во время установления зашифрованного соединения; изучена и описана структура и отличия «рукопожатия» протоколов TLS версий v1.2 и v1.3; выявлена структура, размеры и порядок расположения фреймов и пакетов данных сети «Tor» и отличного от него соединения, использующих шифрование TLS v1.3.*

Ключевые слова: *сертификат X.509, рукопожатие TLS, законное блокирование доступа, кибербезопасность, деанонимизация.*

DOI:10.21681/2311-3456-2020-06-57-62

1. Введение

Проблематика деанонимизации лиц, совершающих преступления с применением компьютерных технологий, не теряет своей актуальности в связи с высоким ростом развития технологий и их доступности, а также расширением сфер применения ресурсов, обеспечивающих анонимность [1-5]. Одним из основных инструментов, применяемых лицами для совершения противоправных деяний в информационно-коммуникационной сети Интернет, является программный комплекс «Tor» – проект разработанный и развиваемый на средства Министерства обороны и Государственного департамента США.

На сегодняшний день анонимизация пользователей сети «Tor» обеспечивается сетью т.н. узлов «луковой» маршрутизации, а также применением встроенных в браузер Tor программных средств-обфускаторов и использованием с 2018 года протокола шифрования данных TLS версии v1.3.

Проблема идентификации подключения к сети «Tor» состоит в маскировании передаваемых данных под обычное https-соединение, наложение обфусцирующего «цифрового шума», делающего невозможным анализ содержимого, а также в шифровании всех данных с момента начала установления соединения.

Как российскими, так и зарубежными исследователями разработаны различные методы деанонимизации пользователей сети «Tor», основанные на различных видах анализа данных передаваемых между клиентами и анонимной сетью [6-12]. Основные исследования по деанонимизации направлены именно на выявление личности преступника, получение его установочных данных, определение его местонахождения.

В целях обеспечения информационной безопасности и противодействия использованию для совершения преступлений различной направленности анонимайзеров, на взгляд авторов, необходимо применять законное блокирование доступа к сетям и сервисам, позволяющим обеспечивать анонимность использования сети Интернет.

В опубликованных ранее работах [13-16] рассматривались признаки TLS-рукопожатия и самоподписываемых сертификатов X.509 протокола шифрования версии TLS v1.2. В 2018 году сеть «Tor» запустила использование новой версии TLS v1.3, которая с позиций исследования TLS-рукопожатия, ограничила возможности идентификации по признакам, характерным для версии TLS v1.2, а именно по размеру сертификата, передаваемого входным узлом в адрес клиент сети. Данное ограничение связано с шифрованием фреймов пакета, который содержит сертификат.

Содержание данной статьи дополняет проведенные ранее исследования рукопожатия сети «Tor» в части, касающейся новой версии TLS v1.3. Авторы предлагают использовать в качестве набора признаков, идентифицирующих установление соединения сети «Tor», размеры пакетов и фреймов в их составе, порядок фреймов в пакете.

1 Лапшичёв Виталий Витальевич, аспирант, младший научный сотрудник кафедры безопасности информационных технологий Института компьютерных технологий Южного Федерального университета, г. Таганрог, Россия. E-mail: lapshichyov@sfedu.ru

2 Макаревич Олег Борисович, доктор технических наук, профессор, профессор кафедры безопасности информационных технологий Института компьютерных технологий Южного Федерального университета, г. Таганрог, Россия. E-mail: obmakarevich@sfedu.ru

В ходе исследования особенностей установления соединения между клиентом и сервером сети «Tor», в том числе, характеристик самоподписываемых сертификатов X.509, разработан набор признаков для идентификации фазы TLS-рукопожатия.

Выделенный набор признаков начальной фазы подключения к сети «Tor» позволяет использовать его в целях законного блокирования клиента сети для обеспечения безопасности на объектах информационной структуры организаций, предоставляющих услуги доступа к сети Интернет.

2. Анализ TLS-рукопожатия сети «Tor»

Для целей исследования TLS-рукопожатия, осуществляемого сетью «Tor» в ходе соединения входного узла сети и клиентского программного обеспечения, были использованы дампы обмена данных.

Перехват трафика осуществлялся при помощи анализатора сети «Wireshark» в виртуальной среде Oracle VM Virtual Box, запущенной в «Kali Linux», что позволило избежать излишних данных в создаваемых дампах.

Случайным образом на сайте bridges.torproject.org был подобран перечень адресов входных узлов сети «Tor», не использующих обфускацию (маскирование данных «цифровым шумом»), значения которых использовались для настройки маршрутизации браузера «Firefox», входящего в программный комплекс «Tor» (вида IP-адрес:порт): 92.206.11.41:993; 45.155.157.193:9001; 81.202.93.10:9001; 95.217.197.205:11900; 144.76.185.37:9001; 185.220.101.77:5989.

При подключении по каждому адресу велся перехват данных, дамп которых сохранялся в отдельный файл для дальнейшего анализа.

Следует отметить, что в отдельных случаях, по-видимому, из-за отсутствия поддержки входным узлом сети «Tor» версии TLS v1.3, соединение осуществлялось с шифрованием старой версией протокола v1.2.

Используя данные такого соединения, был установлен порядок следования фреймов (кадров) в пакетах TLS-рукопожатия: 1) запрос на подключение клиента client_hello, 2.1) ответ о возможности подключении к серверу server_hello, 2.2) передача сертификата сервера клиенту certificate, 2.3) передача ключей сервера для шифрования server_key_exchange, 2.4) окончание процесса рукопожатия server_hello_done. При этом все указанные данные передаются в незашифрованном виде.

Исследуя TLS-рукопожатие сети «Tor» версии TLS v1.3, можно отметить особенности набора пакетов и фреймов, отличающие его как от предыдущей версии, так и от других ресурсов, использующих такую версию шифрования данных.

В ответ на незашифрованный пакет client_hello сеть «Tor» направляет пакет, в котором только фрейм server_hello передается в незашифрованном виде, но уже последующие фреймы change_cipher_spec и application_data шифруются протоколом версии TLS v1.3.

Поток данных шифруемый TLS v1.3 содержит набор из пяти фреймов: client_hello (запрос на соединения от клиента), server_hello (ответ сервера об установлении соединения), change_cipher_spec (передача набора шифров, используемых для установления шифрованного соединения), application_data (зашифрованные данные) и continuation_data (данные для продолжения соединения). Фреймы application_data составляют около 90% всех передаваемых зашифрованных данных.

В ходе анализа полученных по соединениям данных была выявлена структура пакета server_hello версии TLS v1.3 (табл. 1), в котором фреймы имели определенный, неизменяемый порядок расположения, а также определенный размер. Исключение составил 4-й (с начала пакета) фрейм, размер которого соотносится с размером сертификата сети «Tor» версии TLS v1.2 [13-15], с отличием в 20-30 байт.

Таблица 1

Структура пакета server_hello версии TLS v1.3 сети «Tor» (размер фреймов в байтах)

Server Hello	Change Cipher Spec	Application Data	Application Data	Application Data	Application Data
155	1	23	n	281	69

Данные анализа пакетов шести соединений (рис. 1) дают представление о диапазоне величин фреймов, изменяющихся при каждом новом подключении. В анализе дампов с использованием сниффера (анализатора пакетов) «Wireshark» учитывался размер той части пакета server_hello версии TLS v1.3, который содержал информацию о TLS-фреймах, указанных в таблице (таб. 1). Так, например, весь пакет server_hello версии TLS v1.3 имел размер 1221 байт, а фреймы TLS – 1137 байт. Для целей исследования использовался именно этот фрагмент, так как он содержит 5 фреймов с неизменяемыми величинами и один – с переменной величиной, сходной по размеру с сертификатом шифрования версии TLS v1.2.

Как видно на графике размеров пакетов (рис. 1) в одном случае, при соединении с адресом 144.76.185.37:9001, отсутствовал 4-й фрейм. Это случай установления соединения по версии протокола TLS v1.2. Пакет client_hello передан по версии TLS v1.3, а дальнейшее рукопожатие прошло по предыдущей версии протокола с передачей сертификата в незашифрованном виде размером 593 байта.

3. Верификация данных рукопожатия «Tor»

Для верификации результатов анализа данных предыдущих соединений случайным образом был выбран адрес входного узла сети «Tor» 193.106.166.105, не использующий обфускацию. В ходе подключения по

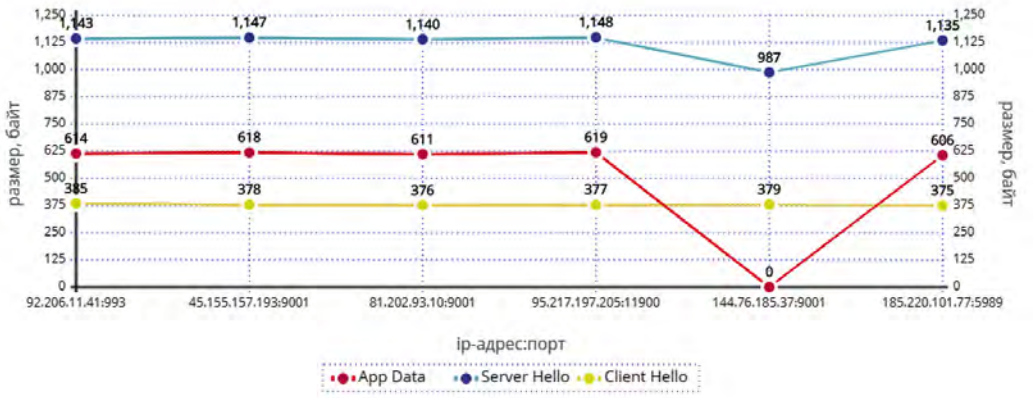

Рис.1. Размеры фреймов client_hello, server_hello и app_data (4й фрейм)

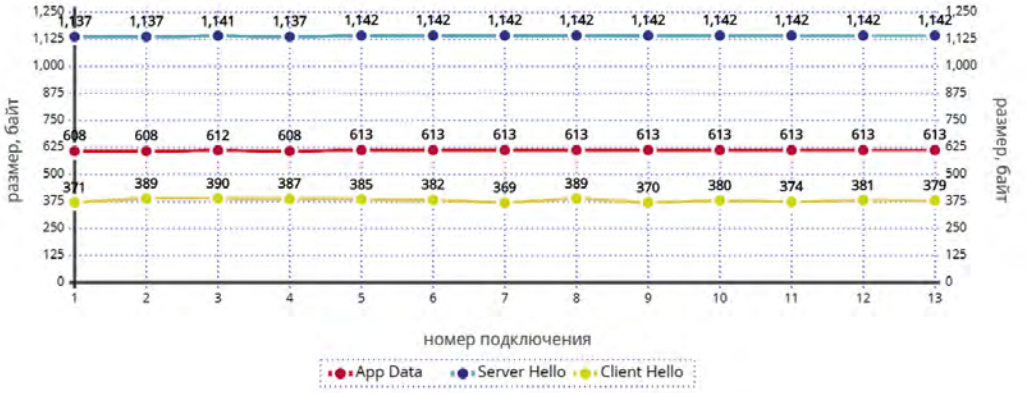

Рис.2. Размеры фреймов рукопожатия с IP-адресом 193.106.166.105

данному адресу производились различные действия с браузером сети «Tor», направленные на переподключение и смену цепочки узлов маршрутизации с использованием встроенных программных опций, что, в свою очередь, выполняло задачу по осуществлению большего количества TLS-рукопожатий, необходимых для дальнейшего перехвата данных и их анализа. На графике (рис. 2) представлены данные 13 TLS-рукопожатий, осуществленных по одному IP-адресу.

Данные первых четырех соединений получены в результате последовательного запуска браузера и завершения его работы. Остальные соединения осуществлялись сменой цепочки маршрутизации.

В первых четырех случаях размеры фреймов client_hello, server_hello и application_data колеблются в определенных пределах. В остальных девяти – размеры фреймов server_hello и application_data неизменны, а колеблется величина client_hello.

Сопоставляя данные двух анализов представляется очевидным, что фрейм client_hello находится в пределах от 369 до 385 байт, server_hello – в части, касающейся TLS фреймов, в пределах от 1135 до 1148 (полностью пакет – от 1221 до 1234 байт). Размер остальных отдельных фреймов соответствовал данным, указанным выше (таб. 1).

Таким образом, для формирования набора признаков следует использовать структуру пакета server_hello, учитывая определенный порядок следования и постоянство размеров пакета, также диапазон размеров 4-го фрейма, совпадающего с размеров сертификата «Tor» предыдущей версии протокола шифрования.

4. Анализ TLS-рукопожатия соцсети «ВКонтакте»

Для исследования свойств TLS-рукопожатия ресурса, использующего протокол шифрования версии TLS v1.3, но не имеющего отношения к сети «Tor», была проведена выборка интернет-сайтов. Анализ подключений указал на факт преобладания использования версии TLS v1.2.

Среди них, тем не менее, сайты facebook.com, twitter.com, instagram.com, vk.com, использовали версию протокола TLS v1.3. В связи с ориентированностью исследований на российский сегмент сети Интернет для анализа TLS-рукопожатий был выбран сайт социальной сети «ВКонтакте».

Реализация TLS-рукопожатия производилась путем ввода в адресную строку адреса соцсети vk.com, после

DOI:10.21681/2311-3456-2020-06-57-62

Таблица 2

Структура пакетов server_hello версии TLS v1.3 соцсети «ВКонтакте» (размер фреймов в байтах)

1-й «полупакет»	**Server Hello**	**Change Cipher Spec**	**Application Data**
	122	1	36
2-й «полупакет»	**Application Data**	**Application Data**	**Application Data**
	3726	96	69

которого осуществлялся переход на страницу ввода аутентификационных данных аккаунта. Вход в аккаунт не осуществлялся.

После шести переходов по адресу соцсети «ВКонтакте» и анализа собранных сниффером «Wireshark» данных выявлено следующее.

Пакет client_hello во всех шести случаях имел размер 585 байт. Пакет server_hello состоял из 6 фреймов, но они были разбиты на два «полупакета» по 3 фрейма каждый. Структура пакета server_hello и размеры фреймов представлены в таблице (таб. 2).

Таким образом, имея сходный с пакетом сети «Tor» порядок и содержание фреймов, пакет server_hello соцсети «ВКонтакте» отличается размерами и структурой, разделением на 2 «полупакета».

5. Выводы

Предложена и опробована методика идентификации https-соединения сети «Tor» версии TLS v1.3, основанная на наборе признаков, полученных в ходе применения программного анализа потока данных анонимной сети, использования частотных методов в отношении размеров файлов и их составных частей, декомпозиции содержимого пакетов данных по признакам их количества, порядка следования, нахождения фреймов в пакете и размерам, а также сравнительного метода в отношении различных версий протокола шифрования и ресурсов, осуществляющих соединение.

По итогам выполнения задач исследования в подготовленный на основе результатов набор указанных признаков вошли:

- размер пакета client_hello (369-385 байт);
- размер пакета server_hello (группа TLS фреймов – 1135-1148 байт, полный размер пакета – 1221-1234 байт);
- порядок следования фреймов пакета server_hello (server_hello-change_cipher_spec-application_data-application_data-application_data-application_data);
- «формула» величин фреймов пакета server_hello (155-1-23-n-281-69 байт) и их расположение в установленном порядке;
- величина 4-го фрейма (n, где 619 байт ≥ n ≥ 606 байт).

Данная работа вместе с работами [13-16] образует методику обнаружения и идентификации использования программного комплекса «Tor» в сетях передачи данных.

Работа выполнена при финансовой поддержке Минобрнауки России (грант ИБ) в рамках научного проекта №23/2020.

Литература

1. Батюкова В.Е. Актуальные проблемы противодействия экстремизму в молодежной среде // Государственная служба и кадры. 2020. №1. С. 67-70. DOI: 10.24411/2312-0444-2020-10013.
2. Бондаренко Ю.А., Кизилов Г.М. Проблемы выявления и использования следов преступлений, оставляемых в сети «Darknet» // Гуманитарные, социально-экономические и общественные науки. 2019. №5. С. 97-101. DOI: 10.23672/SAE.2019.5.31422.
3. Батоев В.Б. Проблемы противодействия экстремистской деятельности, осуществляемой с использованием сети Интернет // Вестник ВИ МВД России. 2016. №2. С. 37-43.
4. Волкова О.В., Высоцкий В.Л., Дроздова Е.А. Актуальные вопросы противодействия наркопреступлениям, совершенным бесконтактным способом // Пробелы в российском законодательстве. 2018. №6. С. 176-178.
5. Усманов Р.А. Характеристика преступной деятельности, осуществляемой в сети Интернет посредством сервисов-анонимайзеров // Юридическая наука и правоохранительная практика. 2018. №4 (46). С. 135-141.
6. Авдошин С.М., Лазаренко А.В. Методы деанонимизации пользователей Tor // Информационные технологии. 2016. Т. 22. № 5. С. 362-372.
7. Басыня Е.А., Хиценко В.Е., Рудковский А.А. Метод идентификации киберпреступников, использующих инструменты сетевого анализа информационных систем с применением технологий анонимизации // Доклады Томского государственного университета систем управления и радиоэлектроники. 2019. Т. 22, № 2. С. 45-51. DOI: 10.21293/1818-0442-2019-22-2-45-51.
8. Avdoshin S.M., Lazarenko A.V. Deep web users deanonimization system // Труды ИСП РАН. 2016. Т. 28, № 3. С. 21-34. DOI: 10.15514/ISPRAS-2016-28(3)-2.

9. Щербинина И.А., Кытманов Н.С., Александров Р.В. Применение технологии DNS-Rebinding для определения реального IP-адреса анонимных веб-пользователей // Вопросы кибербезопасности. 2016. №1 (14). С. 31-35.
10. Martin Steinebach, Marcel Schäfer, Alexander Karakuz, Katharina Brandl, and York Yannikos. 2019. Detection and Analysis of Tor Onion Services. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19). Association for Computing Machinery, New York, NY, USA, art. 66, pp. 1–10. DOI: 10.1145/3339252.3341486.
11. Tao Wang and Ian Goldberg. Improved website fingerprinting on Tor. In Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society (WPES '13). Association for Computing Machinery, New York, NY, USA, 2013, pp. 201–212. DOI: 10.1145/2517840.2517851.
12. Florian Platzer, Marcel Schäfer, and Martin Steinebach. 2020. Critical traffic analysis on the tor network. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20). Association for Computing Machinery, New York, NY, USA, art. 77, pp.1–10. DOI: 10.1145/3407023.3409180.
13. Лапшичёв В.В. Макаревич О.Б. Метод обнаружения и идентификации использования программного комплекса «Tor» // Информатизация и связь. 2020. № 3. С. 17-20. DOI: 10.34219/2078-8320-2020-11-3-17-20.
14. Lapshichyov V.V., Makarevich O.B. TLS Certificate As A Sign Of Establishing A Connection With The Network Tor. The 12th International Conference on Security of Information and Networks (SIN 2019). Proceedings of the 12th International Conference on Security of Information and Networks, 2019, pp. 92-97. DOI: 10.1145/3357613.3357628.
15. Lapshichev V.V. TLS Certificates of The Tor Network And Their Distinctive Features. International Journal of Systems and Software Security and Protection, 2019, vol. 10, № 2, pp. 20-43. DOI: 10.4018/IJSSSP.2019070102.
16. Lapshichyov V., Makarevich O. Technology of Deep Packet Inspection For Recognition And Blocking Traffic Of The Tor Network. Безопасность информации и компьютерных сетей (SIN 2019). Материалы 12-й Международной научной конференции. 2019. С. 24-27.

IDENTIFICATION OF THE "TOR" NETWORK HTTPS-CONNECTION VERSION TLS V1.3

Lapshichyov V.V.[3], Makarevich O.B.[4]

Purpose of the study: *compilation of a set of features that allow to detect and identify the establishment of a connection between the client and the anonymous network Tor in conditions of using encryption of the data stream using the TLS v1.3 protocol.*

Method: *software analysis of the data flow, frequency methods, decomposition of the content of data packets according to their number, sequence, finding frames in a packet and sizes, a comparative method in point of different versions of the encryption protocol and resources making the connection were used.*

Results: *a set of features of the Tor network connection established using TLS v1.3 encryption was compiled, allowing to detect and identify in the data stream a "handshake" between the client and the Tor network in order to legally block the connection; a comparative analysis of the data of the Tor network and the VKontakte social network during the establishment of an encrypted connection was carried out; studied and described the structure and differences of the "handshake" of the TLS protocols v1.2 and v1.3; the structure, size and arrangement of frames and data packets of the Tor network and a connection of other network type, both using TLS v1.3 encryption, has been revealed.*

Keywords: *X.509 certificate, TLS handshake, legal blocking of access, cybersecurity, deanonymization.*

References

1. Batyukova V.E. Aktual'nye problemy protivodeystviya ekstremizmu v molodezhnoy srede // Gosudarstvennaya sluzhba i kadry [State service and personnel], 2020, No 1, pp. 67-70. DOI: 10.24411/2312-0444-2020-10013.
2. Bondarenko Y.A., Kizilov G.M. Problemy vyyavleniya i ispol'zovaniya sledov prestupleniy, ostavlyaemyh v seti «Darknet» // Gumanitarnye, sotsial'no-ekonomicheskie i obshchestvennye nauki [Humanitarian, socio-economic and social sciences], 2019, No 5, pp. 97-101. DOI: 10.23672/SAE.2019.5.31422.

3 Vitaly Lapshichyov, postgraduate student, Department of Information Technology Security of Institute of Computing Technologies and Information Security, South Federal University, Taganrog, Russia. Email: lapshichyov@sfedu.ru

4 Oleg Makarevich, Dr. Sc., Professor of Department of Information Technology Security of Institute of Computing Technologies and Information Security, South Federal University, Taganrog, Russia. Email: obmakarevich@sfedu.ru

3. Batoev V.B. Problemy protivodeystviya ekstremistskoy deyatel'nosti, osushchestvlyaemoy s ispol'zovaniem seti Internet // Vestnik VI MVD Rossii [Gerald of Voronezh Institute of Russian Ministry of Interior], 2016, No 2, pp. 37-43.
4. Volkova O.V., Vysotskiy V.L., Drozdova E.A. Aktual'nye voprosy protivodeystviya narkoprestupleniyam, sovershennym beskontaktnym sposobom // Probely v rossiyskom zakonodatel'stve [Gaps in Russian Legislation], 2018, No 6, pp. 176-178.
5. Usmanov R.A. Harakteristika prestupnoy deyatel'nosti, osushchestvlyaemoy v seti Internet posredstvom servisov-anonimayzerov // Yuridicheskaya nauka i pravoohranitel'naya praktika [Legal Science and Law Enforcement Practice], 2018, No 4 (46), pp. 135-141.
6. Avdoshin S.M., Lazarenko A.V. Metody deanonimizatsii pol'zovateley Tor // Informatsionnye tekhnologii [Information Technology], 2016, b. 22, No 5, pp. 362-372.
7. Basynya E.A., Hitsenko V.E., Rudkovskiy A.A. Metod identifikatsii kiberprestupnikov, ispol'zuyushchih instrumenty setevogo analiza informatsionnyh sistem s primeneniem tekhnologiy anonimizatsii // Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki [Reports of Tomsk State University of Control Systems and Radioelectronics], 2019, vol. 22, No 2, pp. 45-51. DOI: 10.21293/1818-0442-2019-22-2-45-51.
8. Avdoshin S.M., Lazarenko A.V. Deep web users deanonimization system // Trudy ISP RAN, [Proceedings of the Institute for System Programming of the Russian Academy of Sciences], 2016, vol. 28, No 3, pp. 21-34. DOI: 10.15514/ISPRAS-2016-28(3)-2.
9. Shcherbinina I.A., Kytmanov N.S., Aleksandrov R.V. Primenenie tekhnologii DNS-Rebinding dlya opredeleniya real'nogo IP-adresa anonimnyh veb-pol'zovateley // Voprosy kiberbezopasnosti [Cybersecurity Issues], 2016, No 1 (14), pp. 31-35.
10. Martin Steinebach, Marcel Schäfer, Alexander Karakuz, Katharina Brandl, and York Yannikos. 2019. Detection and Analysis of Tor Onion Services. In Proceedings of the 14th International Conference on Availability, Reliability and Security. ARES '19. Association for Computing Machinery, New York, NY, USA, art. 66, pp. 1–10. DOI: 10.1145/3339252.3341486.
11. Tao Wang and Ian Goldberg. Improved website fingerprinting on Tor. In Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society. WPES '13. Association for Computing Machinery, New York, NY, USA, 2013, pp. 201–212. DOI: 10.1145/2517840.2517851.
12. Florian Platzer, Marcel Schäfer, and Martin Steinebach. 2020. Critical traffic analysis on the tor network. In Proceedings of the 15th International Conference on Availability, Reliability and Security. ARES '20. Association for Computing Machinery, New York, NY, USA, art. 77, pp. 1–10. DOI: 10.1145/3407023.3409180
13. Lapshichyov V.V. Makarevich O.B. Metod obnaruzheniya i identifikatsii ispol'zovaniya programmnogo kompleksa «Tor» // Informatizatsiya i svyaz' [Informatization and communication], 2020, No 3, pp. 17-20. DOI: 10.34219/2078-8320-2020-11-3-17-20.
14. Lapshichyov V.V., Makarevich O.B. TLS Certificate As A Sign Of Establishing A Connection With The Network Tor. In proceedings of the 12th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 12-15, 2019). SIN'19. ACM New York, NY, USA, 2019, pp. 92-97. DOI: 10.1145/3357613.3357628.
15. Lapshichev V.V. TLS Certificates of The Tor Network And Their Distinctive Features // International Journal of Systems and Software Security and Protection, 2019, vol. 10, No 2. pp. 20-43. DOI: 10.4018/IJSSSP.2019070102.
16. Lapshichyov V., Makarevich O. Technology of Deep Packet Inspection For Recognition And Blocking Traffic Of The Tor Network In proceedings of the 12th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 12-15, 2019). SIN'19. Sochi State University, Sochi, Russia, 2019, pp. 24-27.