Раздел III. Информационный анализ

УДК 004.056.52 DOI 10.18522/2311-3103-2020-5-150-158

В.В. Лапшичёв, О.Б. Макаревич

НАБОР ПРИЗНАКОВ УСТАНОВЛЕНИЯ HTTPS-СОЕДИНЕНИЯ TLS V1.3 ПРОГРАММНЫМ КОМПЛЕКСОМ «TOR»

Пресечение незаконной деятельности пользователей сети Интернет является одной из актуальных проблем обеспечения информационной безопасности в Российской Федерации. Пресечение деятельности лиц, совершающих противоправные действия с использованием цифровых технологий, в частности, при помощи анонимной сети «Tor», является одной из задач федеральных правоохранительных органов, обеспечивающих информационную безопасность. Сложность выявления и идентификации использования программного комплекса «Tor» в сетях передачи данных обусловлена целым рядом мер, предпринятых его разработчиками, направленными на маскирование потока данных комплекса, среди которых использование современных алгоритмов шифрования пакетов данных. Целью работы является создание и описание набора признаков установления https-соединения программным комплексом «Tor» в условиях применения TLS-шифрования данных протоколом версии v1.3. Задачами работы являются подготовка и анализ материалов трафика программного комплекса «Tor», а также создание на основе полученных данных набора признаков установления соединения между клиентом и сервером анонимной сети. В ходе анализа потока данных анонимной сети исследовался этап установления соединения между клиентом и входным сервером цепи узлов сети «Tor», так называемое «TLS-рукопожатие». Следует отметить, что данная работа дополняет предыдущие исследования по тематике анализа TLS-шифрования в части, касающейся применяемого с 2018 года протокола шифрования TLS v1.3, описывая его особенности как часть механизма реализации анонимизации программным комплексом «Tor». Авторы предлагают использовать размер пакетов «TLS-рукопожатия» в качестве основных признаков, несущих идентифицирующую информацию об установлении анонимного соединения между клиентом и узлом сети «Tor». Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) в рамках научного проекта №23/2020.

Программный комплекс «Tor»; обфускация данных; TLS-рукопожатие; протокол шифрования версии TLS v1.3; законное блокирование доступа.

V.V. Lapshichyov, O.B. Makarevich

SET OF DISTINCTIVE FEATURES OF TLS V1.3 HTTPS-CONNECTION ESTABLISHING BY TOR SOFTWARE COMPLEX

The suppression of illegal activities of Internet users is one of the urgent problems of information security in the Russian Federation. The suppression of the activities of persons committing illegal actions using digital technologies, in particular, using the Tor anonymous network, is one of the tasks of federal law enforcement agencies that ensure information security. The difficulty of detecting and identifying the use of the Tor software package in data transmission networks is due to a number of measures taken by its developers aimed at masking the data flow of the complex, including the use of modern algorithms for encryption of data packets. The aim of the work is to create and describe a set of attributes for establishing an https-connection by the Tor software

package in the context of using TLS data encryption using the version 1.3 protocol. The tasks of the work are the preparation and analysis of traffic materials of the Tor software package, as well as the creation, based on the data obtained, of a set of signs of establishing a connection between the client and the server of the anonymous network. In the course of analyzing the data flow of the anonymous network, the stage of establishing a connection between the client and the input server of the chain of nodes of the Tor network, the so-called "TLS handshake", was investigated. It should be noted that this work complements previous studies on the analysis of TLS encryption in terms of the TLS v1.3 encryption protocol used since 2018, describing its features as part of the mechanism for implementing anonymization by the Tor software package. The authors propose to use the size of the "TLS handshake" packets as the main features that carry identifying information about the establishment of an anonymous connection between the client and the Tor network node. The reported study was funded by Russian Ministry of Science (information security), project number 23/2020.

«Tor» software complex; obfuscation of data; TLS handshake; encryption protocol TLS v1.3; legal blocking of access.

Введение. В ряде работ, посвященных тематике выявления и идентификации использования программного комплекса «Tor», деанонимизации его пользователей, предлагается реализация анализа потока данных различными формами и методами: анализ действий злоумышленника с использованием открытых баз анонимизирующих ресурсов, в том числе, выходных узлов сети «Tor» [1], использованием гравитационной кластеризации [2], пассивного долгосрочного анализа трафика сети «Tor» [3], классической атаки «человек посередине», MITM (man-in-the-middle) [4–5], применением наиболее эффективного на сегодняшний момент «глубокого анализа пакетов», DPI (deep packet inspection) [6–7]. Благодаря утечке документов ограниченного распространения специальных служб Великобритании и США, ответственных за информационную безопасность, стало известно, что ими ведутся разработки собственных технологий выявления трафика сети «Tor» и деанонимизации её пользователей, а также содержание этих разработок и их принципы [8–15]. При этом в своих исследованиях они также используют вышеперечисленные приемы и методы. В отдельных работах внимание исследователей помимо всего прочего обращено на анализ свойств самоподписываемых сертификатов X.509, используемых сетью «Tor» в ходе установления соединения с клиентом, изучение которых и стало основной задачей исследований авторов статьи.

Авторами в ходе проведенных исследований, направленных на разработку метода обнаружения и идентификации использования программного комплекса «Tor», подготовлен ряд статей [16–20], в которых рассматриваются как отдельные характеризующие признаки соединений (размер сертификатов X.509, имена субъекта и объекта сертификации, используемые для подключения порты), устанавливаемых сетью «Tor», так и предлагается алгоритм, использующий эти признаки, для осуществления законного блокирования доступа клиента данной сети к входному узлу. В последние несколько лет в ходе подключения к сети Tor стали использоваться сервисы подключаемых транспортных протоколов (Pluggable Transports, PT) (обфускаторов), которые маскируют поток данных с целью предотвращения его анализа снифферами. В качестве дополнительной меры защиты данных от идентификации применяется TLS-шифрование версии v1.3, которое позволяет сократить процесс рукопожатия между клиентом и сервером сети «Tor» и шифрует пакеты данных, в том числе сертификат, при установлении соединения.

Учитывая, что авторами уже проведены исследования рукопожатия TLS-шифрования версии v1.2 и приведены наборы признаков и алгоритм блокирования подключения к сети [16-18, 20], предлагаемая статья содержит результаты исследования данных начального этапа реализации TLS-шифрования версии v1.3 в ходе установления соединения, а также признаков такого соединения.

Несмотря не то, что в Российской Федерации в настоящее время, вслед за Китаем, рассматривается вопрос законодательного ограничения использования протокола TLS-шифрования версии v1.3, выявление и идентификация протоколов обоих версий для законного блокирования установления соединения с сетью «Tor» не теряет своей актуальности.

Анализ соединения с сетью «Tor». В ходе анализа соединения с сетью «Tor» исследовалась стадия установления зашифрованного соединения т.н. «TLS-рукопожатия», которое в версии TLS v1.3 оказалось не менее информативным, чем в TLS v1.2, несмотря на практически изначальное шифрование передаваемых данных.

Для проведения исследования потока данных сети «Tor», а также процессов установления и осуществления соединения, в том числе рукопожатия между клиентом и сервером, через сервис сайта bridges.torproject.org был получен набор пар данных для подключения вида [`IP-адрес:порт`], заведомо не использующие обфускацию передаваемой информации:

```
[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].
```

Каждая из пар была добавлена в поле «Вставьте узлы из доверенных источников» на странице настроек браузера «Tor» `about:preferences#tor` в качестве адреса входного узла сети для подключения клиента. После чего было произведено соединение с сетью «Tor». Захват данных, передаваемых онлайн между клиентом и сервером «Tor», осуществлялся при помощи сниффера «Wireshark», которые затем сохранялись в дампы с расширением «.pcap» для дальнейшего анализа офлайн.

Для ограничения постороннего трафика данных исследование проводилось в программной среде «Kali Linux», установленной на виртуальной машине Oracle VM VirtualBox.

Следует отметить, что классическая схема рукопожатия версии протокола TLS v1.2 (полученная путем анализа этих же дампов, т.к. эта версия тоже используется в отдельных случаях) упрощенно состоит из следующих друг за другом пакетов: запрос на подключение клиента `client_hello`, ответ о возможности подключении к серверу `server_hello`, передача сертификата сервера клиенту `certificate`, передача ключей сервера для шифрования `server_key_exchange`, окончание процесса рукопожатия `server_hello_done`.

В ходе исследования выявлена схема рукопожатия версии TLS v1.3, применяемая в установлении соединения «Tor», которая характеризуется набором признаков, позволяющих отличить это соединение от других подобных. Следует отметить, что только фрейм `server_hello` передается незашифрованным, тогда как `change_cipher_spec` и фреймы `application_data` передаются в зашифрованном виде. Весь поток данных протокола TLS v1.3 содержит 5 описаний фреймов: `client_hello` (запрос на установление соединения клиентом), `server_hello` (ответ сервера об установлении соединения), `change_cipher_spec` (изменение наборов шифров, используемых при установлении соединения), `application_data` (зашифрованные данные приложения) и `continuation_data` (данные для продолжения соединения), при этом фреймы `application_data` занимают приблизительно 90% от всего количества передаваемых данных.

В табл. 1 представлены результаты анализа пакетов и фреймов соединений между клиентом и сетью «Tor», особенностью которых является прямой обмен между локальным IP-адресом 10.0.2.15 и IP-адресами сети «Tor».

Таблица 1

Результаты анализа пакетов рукопожатия «Tor»

Вид пакета	Размер пакета (размер TLS фрей-мов), байт	Размер TLS фреймов v1.3, байт					
		Server Hello	Change Cipher Spec	Application Data	Application Data	Application Data	Application Data
Соединение 10.0.2.15:443↔92.206.11.41:993							
Client Hello	385	-	-	-	-	-	-
Server Hello	1229 (1143)	155	1	23	614	281	69
Соединение 10.0.2.15:443↔ 45.155.157.193:9001							
Client Hello	378	-	-	-	-	-	-
Server Hello	1233 (1147)	155	1	23	618	281	69
Соединение 10.0.2.15:443↔ 81.202.93.10:9001							
Client Hello	376	-	-	-	-	-	-
Server Hello	1226 (1140)	155	1	23	611	281	69
Соединение 10.0.2.15:443↔ 95.217.197.205:11900							
Client Hello	377	-	-	-	-	-	-
Server Hello	1234 (1148)	155	1	23	619	281	69
Соединение 10.0.2.15:443↔ 144.76.185.37:9001							
Client Hello	379	-	-	-	-	-	-
Server Hello	1063 (987)	не учитываются из-за подключения по версии TLSv1.2					
Соединение 10.0.2.15:443↔ 185.220.101.77:5989							
Client Hello	375	-	-	-	-	-	-
Server Hello	1221 (1135)	155	1	23	606	281	69

Следует отметить, что одно из соединений использовало протокол TLS v1.2, в котором пакет `server_hello` меньше почти на 200 байт типичного для версии v1.3 размера пакета, хотя клиентский пакет был передан в версии v1.3. При этом было реализовано характерное для версии 1.2 рукопожатие, в ходе которого был передан в незашифрованном виде сертификат (593 байта).

Для верификации результатов анализа контрольной группы адресов из списка узлов сети «Tor» был взят случайный адрес `193.106.166.105`, не использующий обфускацию, который был добавлен в качестве входного узла. При этом сначала подключение велось путем запуска браузера «Tor» и его последующего закрытия, а затем производилась смена цепочки узлов нажатием на соответствующую команду меню. Таким образом были применены различные способы воздействия на программный комплекс для реализации иных вариантов соединения с анонимной сетью и достижения большего количества рукопожатий. Результаты представлены в табл. 2.

Таблица 2

Результаты анализа дополнительного набора пакетов «Tor»

Вид пакета	Размер пакета (размер TLS фрей-мов), байт	Размер TLS фреймов v1.3, байт					
		Server Hello	Change Cipher Spec	Application Data	Application Data	Application Data	Application Data
Запуск/закрытие браузера «Tor»							
Client Hello	371	-	-	-	-	-	-
Server Hello	1221 (1137)	155	1	23	608	281	69
Client Hello	389	-	-	-	-	-	-
Server Hello	1221 (1137)	155	1	23	608	281	69

Client Hello	390	-	-	-	-	-	-
Server Hello	1225 (1141)	155	1	23	612	281	69
Client Hello	387	-	-	-	-	-	-
Server Hello	1221 (1137)	155	1	23	608	281	69
Смена цепочки узлов сети «Tor»							
Client Hello	385	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69
Client Hello	382	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69
Client Hello	369	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69
Client Hello	389	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69
Client Hello	370	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69
Client Hello	380	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69
Client Hello	374	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69
Client Hello	381	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69
Client Hello	379	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69

В итоге размер пакета `client_hello` находится в пределах от 369 до 385 байт, а `server_hello` – в пределах от 1221 до 1234 байт. При этом часть `server_hello`, относящаяся непосредственно к TLS-шифрованию имеет постоянные размеры фреймов, за исключением 4-го фрейма, который предположительно, содержит зашифрованный файл сертификата, размер которого приближается к установленному размеру сертификата в TLS v1.2 [16–18]. Порядок расположения величин фреймов в пакете `server_hello` указан на рис. 1. Данный порядок размеров фреймов может служить частью набора признаков для осуществления блокирования путем сравнения размеров, где 619 байт ≥ n ≥ 606 байт.

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

Рис. 1. Структура пакета `server_hello` «Tor» с размерами фреймов

Сравнительный анализ https-соединения «vk.com». В целях сравнительного анализа свойств и данных отличного от «Tor» https-соединения, использующего версию протокола шифрования TLS v1.3, было проведено практическое рассмотрение https-соединений в сети «Интернет», которое указало на тот факт, что большинство сайтов на момент проведения исследования используют старую версию установления зашифрованного соединения по протоколу TLS v1.2. Тем не менее, такие сайты, как facebook.com, instagram.com, twitter.com, vk.com, используют всё

же новую версию – TLS v1.3. Поскольку исследование ориентировано на российский сегмент сети «Интернет», для изучения передачи данных был выбран сайт социальной сети «ВКонтакте» (vk.com). Для сравнения данных соединения сервера «Tor» после успешного подключения производился переход на заглавную страницу социальной сети «ВКонтакте» (vk.com).

Исследуя обмен данными браузера «Tor» с сайтом соцсети «ВКонтакте», использующей сертификаты X.509 для установления зашифрованного соединения по протоколу TLS v1.3, выявлено следующее. Пакет `client_hello`, передаваемый во время осуществления всех 6 указанных выше подключений между браузером «Tor» и соцсетью «ВКонтакте», имел размер 585 байт, а `server_hello` передавался также 6 фреймами, но они были разбиты на два пакета (3554 и 662 байта) по 3 фрейма каждый и имели другой размер. Структура пакета `server_hello` социальной сети «ВКонтакте» по результатам анализа представлена на рис. 2. Соединение с сервером vk.com осуществляется зеркалированием на виртуальный интерфейс – IP-адрес локального хоста 127.0.0.1, а не прямым соединением с IP-адресом соцсети.

1-й пакет	Server Hello	Change Cipher Spec	Application Data
	122	1	36
2-й пакет	Application Data	Application Data	Application Data
	3726	96	69

Рис. 2. Структура пакета `server_hello` соцсети «ВКонтакте»

Сравнение структуры пакетов сети «Tor» и соцсети «ВКонтакте» позволяет отметить схожесть пакетов `server_hello` обоих ресурсов, отличающихся наличием 6-ти фреймовой структурой, определенным порядком фреймов `server_hello-change_cipher_spec-application_data-application_data-application_data-application_data` и постоянством их величин. Однако есть и отличия, заключающиеся в разбиении `server_hello` социальной сети «ВКонтакте» на два пакета (в противоположность единому пакету у «Tor»), а также в переменном размере 4-го фрейма пакета сети «Tor», который по размерам соотносится с сертификатом «Tor», используемом в протоколе TLS v1.2 [16–18].

Таким образом набором признаков соединения сети «Tor» при шифровании данных с помощью алгоритма TLS v1.3 будут являться:

- размер пакета `client_hello` (369-385 байт);
- размер пакета `server_hello` (1221-1234 байт);
- структура фреймов пакета `server_hello` (`server_hello-change_cipher_spec-application_data-application_data-application _data-application_data`);
- величины 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).

Заключение. В работе представлены результаты подготовки и анализа снифферером Wireshark материалов трафика программного комплекса «Tor», а также созданный на основе полученных данных набор признаков установления соединения между клиентом и сервером анонимной сети.

Исследован этап установления соединения (TLS-рукопожатие) между клиентом и входным сервером цепи узлов сети «Tor», проведено описание структуры пакетов и сравнение их со структурой пакетов другого сервиса, использующего протокол TLS v1.3.

Проведена верификация результатов анализа различными способами воздействия на программный комплекс для реализации иных вариантов соединения с анонимной сетью.

В ходе верификации было установлено, что порядок фреймов в пакете, передаваемом сетью «Tor», и их размер остался неизменным, за исключением переменного значения n 4-го фрейма, которое соотносится с размером сертификата сети «Tor», шифруемого протоколом TLS v1.2.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *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.
2. *Rao Z., Niu W., Zhang X.S., Li H.* Tor anonymous traffic identification based on gravitational clustering. Peer-to-Peer Networking and Applications: Vol. 11, Issue 3. – New York: Springer Science+Business Media, 2017. – P. 592-601.
3. *Amann J., Sommer R*. Exploring Tor's Activity Through Long-term Passive TLS Traffic Measurement. Paper presented at the Passive and Active Measurement Conference (PAM), Heraklion, Crete, Greece, 2016.
4. *Makrushin D., Garnaeva M.* Uncovering Tor users: where anonymity ends in the Darknet. Kaspersky Lab SecureList. 18.06.2015. – URL https://securelist.com/uncovering-Tor-users-where-anonymity-ends-in-the-darknet/70673 (дата обращения: 03.11.2020).
5. *Лазаренко А.В.* Технологии деанонимизации пользователей «Tor» // Новые информационные технологии в автоматизированных системах. – 2016. – С. 19. – URL: https://cyberleninka.ru/article/v/tehnologii-deanonimizatsii-polzovateley-Tor (дата обращения: 01.11.2020).
6. *Sommer R., Amann J., Hall S*. Spicy: A Unified Deep Packet Inspection Framework Dissecting All Your Data (ICSI Technical Report), Berkeley, CA, USA, University of California, International Computer Science Institute, 2015.
7. *Ferry A.S., Isbat U.N., Balighani F.B.* Detecting and blocking onion router traffic using deep packet inspection. Paper presented at International Electronics Symposium (IES), Denpasar, Indonesia, 2017.
8. Government Communications Headquarters. A potential technique to deanonymise users of the Tor network. Snowden Surveillance Archive, 2011. – URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0d08.dir/doc.pdf (дата обращения: 01.11.2020).
9. Government Communications Headquarters. A potential technique to deanonymise users of the Tor network – Slides. Snowden Surveillance Archive, 2011. – URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HA SHf400.dir/doc.pdf (дата обращения: 02.11.2020).
10. Government Communications Headquarters. Tor Hidden Services How Hidden is 'Hidden'? Applied Research. Snowden Surveillance Archive, 2011. – URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH3ae6.dir/doc.pdf (дата обращения: 02.11.2020).
11. National Security Agency. Tor - 2006 CES Summer Program. Snowden Surveillance Archive, 2006. – URL: https://snowdenarchive.cjfe.org/greenstone/collect/ snowden1/index/ assoc/HASHbefc.dir/doc.pdf (дата обращения: 03.11.2020).
12. National Security Agency. TLS trends at GCHQ, Snowden Surveillance Archive, 2012. – URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH2236.dir/doc.pdf (дата обращения: 04.11.2020).
13. National Security Agency. Tor Stinks. Snowden Surveillance Archive, 2012. – URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH7920.dir/doc.pdf (дата обращения: 03.11.2020).

14. National Security Agency. Types of IAT - Advanced Open Source Multi-Hop. Snowden Surveillance Archive, 2012. – URL: https://snowdenarchive.cjfe.org/ greenstone/collect/snowden1/index/assoc/HASH01ad/bb7e08bf.dir/doc.pdf (дата обращения: 01.11.2020).
15. National Security Agency (2013). Peeling Back the Layers of Tor with EGOTISTICAL GIRAFFE. Snowden Surveillance Archive, 2013. – URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH32d5.dir/doc.pdf.
16. *Лапшичёв В.В. Макаревич О.Б.* Метод обнаружения и идентификации использования программного комплекса «Тор» // Информатизация и связь. – 2020. – № 3. – С. 17-20. – DOI: 10.34219/2078-8320-2020-11-3-17-20.
17. *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. – P. 92-97. – DOI: 10.1145/3357613.3357628.
18. *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. – P. 20-43. – DOI: 10.4018/IJSSSP.2019070102.
19. *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): Матер. 12-й Международной научной конференции. – 2019. – С. 24-27.
20. *Lapshichyov V., Makarevich O.* Algorithm for Analyzing And Blocking Access to the Tor Network // Безопасность информации и компьютерных сетей (SIN 2019): Матер.12-й Международной научной конференции. – 2019. – С. 27-30.

REFERENCES

1. *Basynya E.A., Khitsenko V.E., Rudkovskiy A.A.* Metod identifikatsii kiberprestupnikov, ispol'zuyushchikh instrumenty setevogo analiza informatsionnykh sistem s primeneniem tekhnologiy anonimizatsii [Method of identification of cybercriminals using tools of network analysis of information systems using anonymization technologies], *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.
2. *Rao Z., Niu W., Zhang X.S., Li H.* Tor anonymous traffic identification based on gravitational clustering. Peer-to-Peer Networking and Applications: Vol. 11, Issue 3. New York: Springer Science+Business Media, 2017, pp. 592-601.
3. *Amann J., Sommer R*. Exploring Tor's Activity Through Long-term Passive TLS Traffic Measurement. Paper presented at the Passive and Active Measurement Conference (PAM), Heraklion, Crete, Greece, 2016.
4. *Makrushin D., Garnaeva M.* Uncovering Tor users: where anonymity ends in the Darknet. Kaspersky Lab SecureList. 18.06.2015. Available at: https://securelist.com/uncovering-Tor-users-where-anonymity-ends-in-the-darknet/70673 (accessed 03 November 2020).
5. *Lazarenko A.V.* Tekhnologii deanonimizatsii pol'zovateley «Tor» [Technologies of deanonymization of users "Tor"], *Novye informatsionnye tekhnologii v avtomatizirovannykh sistemakh* [New information technologies in automated systems], 2016, pp. 19. Available at: https://cyberleninka.ru/article/v/tehnologii-deanonimizatsii-polzovateley-Tor (accessed 01 November 2020).
6. *Sommer R., Amann J., Hall S*. Spicy: A Unified Deep Packet Inspection Framework Dissecting All Your Data (ICSI Technical Report), Berkeley, CA, USA, University of California, International Computer Science Institute, 2015.
7. *Ferry A.S., Isbat U.N., Balighani F.B.* Detecting and blocking onion router traffic using deep packet inspection. Paper presented at International Electronics Symposium (IES), Denpasar, Indonesia, 2017.
8. Government Communications Headquarters. A potential technique to deanonymise users of the Tor network. Snowden Surveillance Archive, 2011. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0d08.dir/doc.pdf (accessed 01 November 2020).

9. Government Communications Headquarters. A potential technique to deanonymise users of the Tor network – Slides. Snowden Surveillance Archive, 2011. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASHf400.dir/doc.pdf (accessed 02 November 2020).
10. Government Communications Headquarters. Tor Hidden Services How Hidden is 'Hidden'? Applied Research. Snowden Surveillance Archive, 2011. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH3ae6.dir/doc.pdf (accessed 02 November 2020).
11. National Security Agency. Tor - 2006 CES Summer Program. Snowden Surveillance Archive, 2006. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/ snowden1/index/assoc/HASHbefc.dir/doc.pdf (accessed 03 November 2020).
12. National Security Agency. TLS trends at GCHQ, Snowden Surveillance Archive, 2012. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH2236.dir/doc.pdf (accessed 04 November 2020).
13. National Security Agency. Tor Stinks. Snowden Surveillance Archive, 2012. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH7920.dir/doc.pdf (accessed 03 November 2020).
14. National Security Agency. Types of IAT - Advanced Open Source Multi-Hop. Snowden Surveillance Archive, 2012. Available at: https://snowdenarchive.cjfe.org/greenstone/ collect/snowden1/index/assoc/HASH01ad/bb7e08bf.dir/doc.pdf (accessed 01 November 2020).
15. National Security Agency (2013). Peeling Back the Layers of Tor with EGOTISTICAL GIRAFFE. Snowden Surveillance Archive, 2013. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH32d5.dir/doc.pdf.
16. *Lapshichev V.V. Makarevich O.B.* Metod obnaruzheniya i identifikatsii ispol'zovaniya programmnogo kompleksa «Tor» [Method of detection and identification of the use of the software complex "Tor"], *Informatizatsiya i svyaz'* [Informatization and Communication], 2020, No. 3, pp. 17-20. DOI: 10.34219/2078-8320-2020-11-3-17-20.
17. *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.
18. *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.
19. *Lapshichyov V., Makarevich O.* Technology of Deep Packet Inspection For Recognition And Blocking Traffic of the Tor Network, *Bezopasnost' informatsii i komp'yuternykh setey (SIN 2019): Mater. 12-y Mezhdunarodnoy nauchnoy konferentsii* [Information Security and Computer Networks (SIN 2019): Proceedings of the 12th International Scientific Conference], 2019, pp. 24-27.
20. *Lapshichyov V., Makarevich O.* Algorithm for Analyzing And Blocking Access to the Tor Network, *Bezopasnost' informatsii i komp'yuternykh setey (SIN 2019): Mater. 12-y Mezhdunarodnoy nauchnoy konferentsii* [Information Security and Computer Networks (SIN 2019): Proceedings of the 12th International Scientific Conference], 2019, pp. 27-30.

Статью рекомендовала к опубликованию д.т.н., профессор Н.И. Червякова.

Лапшичёв Виталий Витальевич – Южный федеральный университет; e-mail: lapshichyov@sfedu.ru; г. Таганрог, ул. Чехова, 2; тел.: +79043467763; кафедра безопасности информационных технологий; аспирант.

Макаревич Олег Борисович – e-mail: obmakarevich@sfedu.ru; кафедра безопасности информационных технологий; д.т.н.; профессор.

Lapshichyov Vitaly Vitalyevich – South Federal University; e-mail: lapshichyov@sfedu.ru; 2, Chekhov street, Taganrog, Russia; phone: +79043467763; the department of IT Security; postgraduate student.

Makarevich Oleg Borisovich – e-mail: obmakarevich@sfedu.ru; the department of IT Security; dr. of eng. sc.; professor.