Константин Г. Когос¹, Михаил А. Фиошин²
Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе, 31, Москва, 115409, Россия
¹e-mail: KGKogos@mephi.ru, <https://orcid.org/0000-0002-8090-678X>
²e-mail: MAFinoshin@mephi.ru, <https://orcid.org/0000-0003-4374-1645>

ПЕРСПЕКТИВНЫЕ ПОДХОДЫ К ОБНАРУЖЕНИЮ СЕТЕВЫХ СКРЫТЫХ КАНАЛОВ

DOI: <http://dx.doi.org/10.26583/bit.2021.2.05>

Аннотация. Целью данной статьи является анализ существующих методов обнаружения сетевых скрытых каналов по времени. Для противодействия сетевым скрытым каналам по памяти зачастую применяют превентивные меры, такие как шифрование трафика и нормализация длин передаваемых пакетов. В случае скрытых каналов по времени более предпочтительны методы, не влияющие на функционирование легитимных каналов связи, так как превентивные меры приводят к более ощутимым последствиям для работы всей системы в целом. Одной из не превентивных мер является обнаружение. Задача обнаружения функционирующих скрытых каналов в защищаемой системе сводится либо к задаче поиска закономерностей в потоке трафика, либо к задаче сравнения тестируемой выборки с «эталонной». «Эталонная» выборка — это выборка с гарантированным отсутствием функционирующего скрытого канала. В статье рассматривается вопрос места алгоритмов машинного обучения в контексте задачи обнаружения сетевых скрытых каналов. Выделяются три случая работы методов обнаружения сетевых скрытых каналов по времени, основанных на алгоритмах машинного обучения, в зависимости от знаний о защищаемой системе. Приводится общая схема работы таких методов для трех случаев. Результатом анализа существующих методов является вывод о необходимости их усовершенствования для наиболее реалистичного случая — отсутствия как «эталонного» трафика, так и трафика с гарантированным присутствием скрытого канала. Описанная проблематика показывает перспективное направление в области исследований методов противодействия утечке информации по сетевым скрытым каналам.

Ключевые слова: скрытые каналы, каналы по времени, утечка информации, обнаружение, машинное обучение.

Для цитирования: КОГОС, Константин Г.; ФИОШИН, Михаил А. ПЕРСПЕКТИВНЫЕ ПОДХОДЫ К ОБНАРУЖЕНИЮ СЕТЕВЫХ СКРЫТЫХ КАНАЛОВ. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 54–61, 2021. ISSN 2074-7136. Доступно на: <<https://bit.mephi.ru/index.php/bit/article/view/1340>>. Дата доступа: 14 apr. 2021. DOI: <http://dx.doi.org/10.26583/bit.2021.2.05>.

Благодарности. Работа выполнена при поддержке Министерства науки и высшего образования РФ (проект государственного задания № 0723-2020-0036).

Konstantin G. Kogos¹, Mihail A. Finoshin²
National Research Nuclear University MEPHI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
¹e-mail: KGKogos@mephi.ru, <https://orcid.org/0000-0002-8090-678X>
²e-mail: MAFinoshin@mephi.ru, <https://orcid.org/0000-0003-4374-1645>

Prospective approaches to detecting network covert channels

DOI: <http://dx.doi.org/10.26583/bit.2021.2.05>

Abstract. The purpose of this study is to analyze the existing timing covert channels detection methods. Preventive measures are often used to counteract storage covert channels, such as traffic encryption and transmitted packets length normalization. Methods, that do not affect the functioning of legitimate communication channels are more preferable in the case of timing covert channels, since preventive measures lead to more tangible consequences for the operation of the entire system. One of the non-preventative measures is detection. The task of detecting covert channels in the protected system is

reduced either to the task of searching for patterns in the traffic flow, or to the task of comparing the tested sample with the "reference" one. A "reference" sample is a sample with a guaranteed absence of a functioning covert channel. The machine learning algorithms in the context of the problem of network covert channels detection are discussed. There are three cases of work of methods for detecting network timing covert channels, based on machine learning algorithms. The cases differ depending on the knowledge of the protected system. The general scheme of operation of such methods for three cases is given. The result of the analysis of existing methods is the conclusion about the need to improve them for the most realistic case – the absence of both "reference" traffic and traffic with a guaranteed presence of a covert channel. The described problems show a promising direction in the field of research on methods of countering information leakage through network covert channels.

Keywords: covert channels, timing channels, information leakage, detection, machine learning.

For citation: KOGOS, Konstantin G.; FINOSHIN, Mihail A. Prospective approaches to detecting network covert channels. *IT Security (Russia)*, [S.l.], v. 28, n. 2, p. 54–61, 2021. ISSN 2074-7136. Available at: <<https://bit.mephi.ru/index.php/bit/article/view/1340>>. Date accessed: 14 apr. 2021. DOI: <http://dx.doi.org/10.26583/bit.2021.2.05>.

Acknowledgement. This work was supported by the Ministry of Science and Higher Education of the Russian Federation (draft state assignment No. 0723-2020-0036).

Введение

Понятие скрытого канала впервые использовали авторы в [1]. Согласно им, канал называется скрытым, если он не проектировался и не предназначался для передачи информации. Отечественный стандарт¹ вводит следующее определение: «скрытый канал – это непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности». Высокоскоростные сетевые технологии позволяют строить скрытые каналы с пропускной способностью, позволяющей нелегитимно передавать критичную информацию в ограниченные сроки. Существование скрытого канала в системе представляет собой серьезную угрозу безопасности, так как стандартные меры и средства сетевой защиты, такие как шифрование канала связи, межсетевые экраны и средства анализа защищенности, не способны противодействовать утечке информации по скрытым каналам.

Известны различные способы передачи информации по сетевым скрытым каналам: скрытая информация может передаваться в заголовках полей передаваемых пакетов [2, 3], посредством изменения длин передаваемых пакетов [4, 5], а также с помощью изменения длин межпакетных интервалов и скоростей передаваемых пакетов [6, 7]. Первые два способа составляют группу скрытых каналов, называемую скрытыми каналами по памяти. Вторые два способа относят к скрытым каналам по времени.

1. Подходы к противодействию утечке информации по скрытым каналам

В отношении скрытых каналов применяются различные контрмеры [8]. Общая схема противодействия утечке информации по скрытым каналам включает в себя несколько шагов:

- идентификация скрытого канала – выявление скрытых каналов, которые могут быть потенциально реализованы в исследуемой системе;
- анализ идентифицированных скрытых каналов, включающий в себя определение количества информации, которое можно передать по выявленным скрытым каналам;

¹ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов – Введ. 2009-10-01. М.: Стандартинформ, 2009. – 13 с.

– принятие решения о контрмерах в отношении идентифицированных и проанализированных скрытых каналов.

К превентивным контрмерам относят:

– ограничение – снижение пропускной способности скрытого канала до значения, которое считается не опасным;

– подавление – архитектурные ограничения, устраняющие возможность построения скрытого канала.

На рис. 1 представлена общая схема противодействия утечке информации по скрытым каналам.

Рис. 1. Схема противодействия утечке информации по скрытым каналам
Fig. 1. The scheme of counteracting information leakage through covert channels

2. Методы обнаружения сетевых скрытых каналов по времени

Множество работ посвящено разработке и анализу статистических методов обнаружения скрытых каналов по времени [6, 10–19]. Условно данные методы можно разделить на требующие и не требующие «эталонную» выборку. Выборка получается из трафика путем извлечения длин межпакетных интервалов. Возможны три случая при снятии трафика из канала связи:

- гарантированное отсутствие скрытно передаваемой информации в трафике;
- гарантированное присутствие скрытно передаваемой информации в трафике;
- невозможность гарантировать как отсутствие, так и присутствие скрытно передаваемой информации в трафике.

Исходя из трех случаев, назовем таким образом получаемый трафик «эталонным», «скрытым» и «неизвестным» соответственно. Следовательно, выборка, получаемая из «эталонного» трафика, будет «эталонной» выборкой, аналогично для двух оставшихся случаев.

В [6] предлагается метод обнаружения скрытых каналов, основанный на изменении длин межпакетных интервалов, не требующий «эталонной» выборки. В [11] рассматриваются методы, основанные на анализе закономерностей в потоке трафика: метод на основе дисперсии, метод «ε-близости» и метод на основе Колмогоровской сложности, которые не требуют «эталонную» выборку, однако для них не оценены количественные характеристики. Кроме того, большое распространение в литературе получили методы, основанные на анализе энтропии трафика [12–14]. Данные методы требуют наличие «эталонной» выборки.

Среди методов обнаружения сетевых скрытых каналов в отдельную группу можно выделить те, которые основаны на методах математической статистики. Для методов данной группы необходимо наличие «эталонной» выборки. Например, в [12] для сравнения распределения длин межпакетных интервалов трафика в системе с аналогичным распределением в «эталонной» выборке используется критерий Колмогорова-Смирнова. Также существует возможность построения метода обнаружения на основе критерия согласия Пирсона [15, 16]. Существуют и другие статистические методы обнаружения сетевых скрытых каналов по времени [17–19].

Стоит отметить ограничения описанных выше методов. В случае параметрических методов выбор конкретных значений параметров не всегда определен, либо же определен только для конкретных типов скрытых каналов [20]. Таким образом, каждый конкретный метод можно применять для обнаружения только ограниченного спектра скрытых каналов. Очевидным недостатком многих методов является требование наличия «эталонной» выборки. В реальных условиях зачастую внедрение системы защиты происходит в уже функционирующую информационную систему, и невозможно гарантировать отсутствие скрытого канала при сборе данных для «эталонной» выборки.

В настоящее время получили развитие методы обнаружения сетевых скрытых каналов по времени на основе алгоритмов машинного обучения. В зависимости от наличия исходных данных, применяются различные подходы на основе машинного обучения [21]: обучение с учителем, обучение без учителя и обучение с подкреплением. Обучение с подкреплением можно рассматривать как область, имеющую отношение к обучению с учителем.

Сложность задачи обнаружения сетевых скрытых каналов по времени на основе алгоритмов машинного обучения зависит от начальных условий. Наиболее простым является случай, когда возможно получение «эталонной» и «скрытой» выборок. Общим подходом для первого случая является применение алгоритмов машинного обучения с учителем. Однако, при реализации системы защиты затруднительно получение таких выборок. Во-первых, как было отмечено выше, сбор «эталонной» выборки представляет серьезную проблему. Во-вторых, для различных типов сетевых скрытых каналов по времени «скрытые» выборки могут сильно различаться, что приводит к необходимости иметь большое число образцов трафика для каждого конкретного типа скрытого канала.

Более сложным является случай, когда имеется возможность получения только «эталонной» выборки. Для второго случая применяются алгоритмы обнаружения аномалий. Исследование первого и второго случаев широко представлено в зарубежной литературе [20, 22–26].

Наконец, наиболее сложным для исследования является случай, когда отсутствует возможность сбора «эталонной» выборки, в таком случае предлагается применять алгоритмы кластеризации.

Необходимым условием для решения задач с помощью алгоритмов машинного обучения является наличие сформированного набора признаков исследуемого объекта. Данный вектор признаков подается на вход алгоритму машинного обучения. В случае задачи обнаружения сетевых скрытых каналов по времени из трафика выделяется массив значений длин межпакетных интервалов. Признаки от данного массива могут вычисляться как на основе формул математической статистики, так и на основе отдельных параметров, анализируемых методами обнаружения сетевых скрытых каналов.

Например, в [22] используют в качестве признаков значение теста Колмогорова-Смирнова, энтропию, условную энтропию и значение теста на определение регулярности, а в качестве метода машинного обучения – метод опорных векторов. В другом случае

строится классификатор, а в качестве признаков используется автокорреляция и энтропия [23]. Классификатор также может строиться на основе Вейвлет-преобразования [20]. Построение методов обнаружения не ограничено данными способами [24–26].

Таким образом, работа метода обнаружения сетевых скрытых каналов по времени включает в себя три этапа:

- анализ трафика и выделение из него массива значений длин межпакетных интервалов;
- обработка массива значений длин межпакетных интервалов и получение на его основе вектора признаков;
- применение алгоритма машинного обучения исходя из типа трафика («эталонный», «скрытый», «неизвестный»), на основе которого принимается решение о наличии или отсутствии скрытого канала в системе.

В зависимости от одного из трех случаев наличия или отсутствия «эталонной» и «скрытой» выборок меняется алгоритм машинного обучения. Данная схема представлена на рис. 2 (где введены обозначения: ССК – сетевой скрытый канал, ДМИ – длины межпакетных интервалов).

Рис. 2. Схема работы метода обнаружения скрытых каналов по времени на основе алгоритмов машинного обучения

Fig.2. Scheme of the timing covert channels detection method based on machine learning algorithms

Как было отмечено выше, исследования в настоящее время ведутся исходя из условий наличия «эталонной» выборки. Однако, зачастую невозможно гарантировать отсутствие скрытого канала в системе при проведении исследований. Таким образом, актуальной является разработка метода обнаружения сетевых скрытых каналов по времени на основе алгоритмов машинного обучения в случае, когда отсутствует обучающая выборка. Такой метод позволит внедрять систему противодействия утечке информации по сетевым скрытым каналам по времени в уже функционирующую систему без предварительного обучения системы защиты.

Заключение

В работе приведен краткий обзор подходов к противодействию утечке информации по сетевым скрытым каналам, при этом особое внимание уделяется методам обнаружения сетевых скрытых каналов по времени. Рассматривается перспективное направление построения методов обнаружения, основанных на алгоритмах машинного обучения. Вводятся понятия «скрытого» и «эталонного» трафика, на основе которых выделяются три возможных случая работы методов обнаружения. Случаи различаются в зависимости от наличия или отсутствия «скрытого» и «эталонного» трафика. Приводится общая схема работы методов обнаружения сетевых скрытых каналов, основанных на алгоритмах машинного обучения. По результатам работы делается вывод о необходимости усовершенствования существующих методов обнаружения с целью их применения для наиболее реалистичного сценария, когда невозможно гарантировать как наличие, так и отсутствие скрытого канала в системе.

СПИСОК ЛИТЕРАТУРЫ:

1. Lampson B.W. A note on the confinement problem //Communications of the ACM. 1973. Vol. 16, no. 10. P. 613–615.
2. Millen J.K. Security kernel validation in practice //Communications of the ACM. 1976. Vol. 19. no. 5. C. 243–250.
3. Zander, Sebastian & Armitage, Grenville & Branch, Philip. (2007). Covert channels in the IP time to live field. URL: https://www.researchgate.net/publication/228875924_Covert_channels_in_the_IP_time_to_live_field (дата обращения: 01.02.2021).
4. M. Hussain and M. Hussain. A high bandwidth covert channel in network protocol. International Conference on Information and Communication Technologies, Karachi, Pakistan, 2011. P. 1–6. DOI: <https://doi.org/10.1109/ICICT.2011.5983562>.
5. L. Ji, H. Liang, Y. Song and X. Niu, A Normal-Traffic Network Covert Channel, 2009 International Conference on Computational Intelligence and Security, Beijing, China, 2009. P. 499–503. DOI: <https://doi.org/10.1109/CIS.2009.156>.
6. Berk V., Giani A., Cybenko G. Detection of covert channel encoding in network packet delays (2005). URL: <https://www.semanticscholar.org/paper/Detection-of-Covert-Channel-Encoding-in-Network-Berk-Giani/58a022c5ff528efa142c1452952c6043d916ffab> (дата обращения: 01.02.2021).
7. S.H. Sellke, C. Wang, S. Bagchi and N. Shroff, TCP/IP Timing Channels: Theory to Implementation, IEEE INFOCOM 2009, Rio de Janeiro, Brazil, 2009. P. 2204–2212. DOI: <https://doi.org/10.1109/INFCOM.2009.5062145>.
8. S. Zander, G. Armitage and P. Branch. A survey of covert channels and countermeasures in computer network protocols, in IEEE Communications Surveys & Tutorials. Vol. 9, no. 3. P. 44–57, Third Quarter 2007. DOI: <https://doi.org/10.1109/COMST.2007.4317620>.
9. Грушо А.А. Скрытые каналы и безопасность в компьютерных системах. Дискретная математика. 1998. Т. 10, вып. 1. С. 3–9. DOI: <https://doi.org/10.4213/dm411>.
10. Epishkina A., Kogos K. A random traffic padding to limit packet size covert channels //2015 Federated Conference on Computer Science and Information Systems (FedCSIS). IEEE, 2015. P. 1107–1111. DOI: <http://dx.doi.org/10.15439/2015F88>.
11. Serdar Cabuk, Carla E. Brodley, and Clay Shields. 2004. IP covert timing channels: design and detection. In Proceedings of the 11th ACM conference on Computer and communications security (CCS '04). Association for Computing Machinery, New York, NY, USA. P. 178–187. DOI: <https://doi.org/10.1145/1030083.1030108>.
12. Walls R. J., Kothari K., Wright M. Liquid: A detection-resistant covert timing channel based on IPD shaping // Computer networks. 2011. Vol. 55. Issue 6. P. 1217–1228.
13. Steven Gianvecchio and Haining Wang. 2007. Detecting covert timing channels: an entropy-based approach. In Proceedings of the 14th ACM conference on Computer and communications security (CCS '07). Association for Computing Machinery, New York, NY, USA. P. 307–316. DOI: <https://doi.org/10.1145/1315245.1315284>.
14. O. Darwish, A. Al-Fuqaha, M. Anan and N. Nasser. The role of hierarchical entropy analysis in the detection and time-scale determination of covert timing channels. International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, 2015. P. 153–159. DOI: <https://doi.org/10.1109/IWCMC.2015.7289074>.

15. Никулин М.С. Критерий хи-квадрат для непрерывных распределений с параметрами сдвига и масштаба, Теория вероятн. и ее примен., 18:3 (1973), С. 583–591. DOI: <https://doi.org/10.1137/1118069>.
16. C. Zhiyong, S. Ying and S. Changxiang. Detection of Insertional Covert Channels Using Chi-square Test. International Conference on Multimedia Information Networking and Security, Wuhan, China, 2009. P. 432–435. DOI: <https://doi.org/10.1109/MINES.2009.296>.
17. F. Rezaei, M. Hempel, P.L. Shrestha, S.M. Rakshit and H. Sharif. Detecting covert timing channels using non-parametric statistical approaches. International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, 2015. P. 102–107. DOI: <https://doi.org/10.1109/IWCMC.2015.7289065>.
18. F. Rezaei, M. Hempel and H. Sharif. Towards a Reliable Detection of Covert Timing Channels over Real-Time Network Traffic, in IEEE Transactions on Dependable and Secure Computing. Vol. 14, no. 3. P. 249–264, 1 May–June 2017. DOI: <https://doi.org/10.1109/TDSC.2017.2656078>.
19. F. Rezaei, M. Hempel, P. L. Shrestha, S. M. Rakshit and H. Sharif. A novel Covert Timing Channel detection approach for online network traffic, 2015 IEEE Conference on Communications and Network Security (CNS), Florence, Italy, 2015. P. 737–738. DOI: <https://doi.org/10.1109/CNS.2015.7346911>.
20. Archibald R., Ghosal D. A comparative analysis of detection metrics for covert timing channels //Computers & security. 2014. Vol. 45. P. 284–292.
21. Рашка С. Python и машинное обучение / С. Рашка, перевод с англ. А.В. Логунова // М.: ДМК Пресс. 2017. – 418 с.
22. P.L. Shrestha, M. Hempel, F. Rezaei and H. Sharif. A Support Vector Machine-Based Framework for Detection of Covert Timing Channels, in IEEE Transactions on Dependable and Secure Computing. Vol. 13, no. 2. P. 274–283, 1 March–April 2016. DOI: <https://doi.org/10.1109/TDSC.2015.2423680>.
23. P.L. Shrestha, M. Hempel, F. Rezaei and H. Sharif. Leveraging Statistical Feature Points for Generalized Detection of Covert Timing Channels. IEEE Military Communications Conference, Baltimore, MD, USA, 2014. P. 7–11. DOI: <https://doi.org/10.1109/MILCOM.2014.10>.
24. İ.G. Çavuşoğlu, H. Alemdar and E. Onur. Covert Channel Detection Using Machine Learning. 28th Signal Processing and Communications Applications Conference (SIU), Gaziantep, Turkey, 2020. P. 1–4. DOI: <https://doi.org/10.1109/SIU49456.2020.9302098>.
25. M. Chourib. Detecting Selected Network Covert Channels Using Machine Learning. International Conference on High Performance Computing & Simulation (HPCS), Dublin, Ireland, 2019. P. 582–588. DOI: <https://doi.org/10.1109/HPCS48598.2019.9188115>.
26. Y. Sun, L. Zhang and C. Zhao. A Study of Network Covert Channel Detection Based on Deep Learning. 2nd IEEE Advanced Information Management, Communication, Electronic and Automation Control Conference (IMCEC), Xi'an, China, 2018. P. 637–641. DOI: <https://doi.org/10.1109/IMCEC.2018.8469669>.

REFERENCES:

- [1] Lampson B.W. A note on the confinement problem. Communications of the ACM. 1973. Vol. 16, no. 10. P. 613–615.
- [2] Millen J.K. Security kernel validation in practice. Communications of the ACM. 1976. Vol. 19. no. 5. P. 243–250.
- [3] Zander, Sebastian & Armitage, Grenville & Branch, Philip. (2007). Covert channels in the IP time to live field. URL: https://www.researchgate.net/publication/228875924_Covert_channels_in_the_IP_time_to_live_field (accessed: 01.02.2021).
- [4] M. Hussain and M. Hussain. A high bandwidth covert channel in network protocol. International Conference on Information and Communication Technologies, Karachi, Pakistan, 2011. P. 1–6. DOI: <https://doi.org/10.1109/ICICT.2011.5983562>.
- [5] L. Ji, H. Liang, Y. Song and X. Niu, A Normal-Traffic Network Covert Channel, 2009 International Conference on Computational Intelligence and Security, Beijing, China, 2009. P. 499–503. DOI: <https://doi.org/10.1109/CIS.2009.156>.
- [6] Berk V., Giani A., Cybenko G. Detection of covert channel encoding in network packet delays (2005). URL: <https://www.semanticscholar.org/paper/Detection-of-Covert-Channel-Encoding-in-Network-Berk-Giani/58a022c5ff528efa142c1452952c6043d916ffab> (accessed: 01.02.2021).
- [7] S.H. Sellke, C. Wang, S. Bagchi and N. Shroff, TCP/IP Timing Channels: Theory to Implementation, IEEE INFOCOM 2009, Rio de Janeiro, Brazil, 2009. P. 2204–2212. DOI: <https://doi.org/10.1109/INFCOM.2009.5062145>.
- [8] S. Zander, G. Armitage and P. Branch. A survey of covert channels and countermeasures in computer network protocols, in IEEE Communications Surveys & Tutorials. Vol. 9, no. 3. P. 44–57, Third Quarter 2007. DOI: <https://doi.org/10.1109/COMST.2007.4317620>.

- [9] Grusho, A.A. Covert channels and security in computer systems. Discrete mathematics. 1998. Vol. 10, issue. 1. P. 3–9. DOI: <https://doi.org/10.4213/dm411> (in Russian).
- [10] Epishkina A., Kogos K. A random traffic padding to limit packet size covert channels. 2015 Federated Conference on Computer Science and Information Systems (FedCSIS). IEEE, 2015. P. 1107–1111. DOI: <http://dx.doi.org/10.15439/2015F88>.
- [11] Serdar Cabuk, Carla E. Brodley, and Clay Shields. 2004. IP covert timing channels: design and detection. In Proceedings of the 11th ACM conference on Computer and communications security (CCS '04). Association for Computing Machinery, New York, NY, USA. P. 178–187. DOI: <https://doi.org/10.1145/1030083.1030108>.
- [12] Walls R.J., Kothari K., Wright M. Liquid: A detection-resistant covert timing channel based on IPD shaping. Computer networks. 2011. Vol. 55. Issue 6. P. 1217–1228.
- [13] Steven Gianvecchio and Haining Wang. 2007. Detecting covert timing channels: an entropy-based approach. In Proceedings of the 14th ACM conference on Computer and communications security (CCS '07). Association for Computing Machinery, New York, NY, USA. P. 307–316. DOI: <https://doi.org/10.1145/1315245.1315284>.
- [14] O. Darwish, A. Al-Fuqaha, M. Anan and N. Nasser. The role of hierarchical entropy analysis in the detection and time-scale determination of covert timing channels. International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, 2015. P. 153–159. DOI: <https://doi.org/10.1109/IWCMC.2015.7289074>.
- [15] Nikulin M.S. Chi-Square Test for Continuous Distributions with Shift and Scale Parameters. Theory Probab. Appl., 18:3 (1974). P. 559–568. DOI: <https://doi.org/10.1137/1118069>.
- [16] C. Zhiyong, S. Ying and S. Changxiang. Detection of Insertional Covert Channels Using Chi-square Test. International Conference on Multimedia Information Networking and Security, Wuhan, China, 2009. P. 432–435. DOI: <https://doi.org/10.1109/MINES.2009.296>.
- [17] F. Rezaei, M. Hempel, P. L. Shrestha, S. M. Rakshit and H. Sharif. Detecting covert timing channels using non-parametric statistical approaches. International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, 2015. P. 102–107. DOI: <https://doi.org/10.1109/IWCMC.2015.7289065>.
- [18] F. Rezaei, M. Hempel and H. Sharif. Towards a Reliable Detection of Covert Timing Channels over Real-Time Network Traffic, in IEEE Transactions on Dependable and Secure Computing. Vol. 14, no. 3. P. 249–264, 1 May–June 2017. DOI: <https://doi.org/10.1109/TDSC.2017.2656078>.
- [19] F. Rezaei, M. Hempel, P. L. Shrestha, S. M. Rakshit and H. Sharif. A novel Covert Timing Channel detection approach for online network traffic. IEEE Conference on Communications and Network Security (CNS), Florence, Italy, 2015. P. 737–738. DOI: <https://doi.org/10.1109/CNS.2015.7346911>.
- [20] Archibald R., Ghosal D. A comparative analysis of detection metrics for covert timing channels. Computers & security. 2014. Vol. 45. P. 284–292.
- [21] Rashka, S. Python and machine learning. S. Rashka. M.: DMK Press. 2017. – 418 p. (in Russian)
- [22] P.L. Shrestha, M. Hempel, F. Rezaei and H. Sharif. A Support Vector Machine-Based Framework for Detection of Covert Timing Channels, in IEEE Transactions on Dependable and Secure Computing. Vol. 13, no. 2. P. 274–283, 1 March–April 2016. DOI: <https://doi.org/10.1109/TDSC.2015.2423680>.
- [23] P.L. Shrestha, M. Hempel, F. Rezaei and H. Sharif. Leveraging Statistical Feature Points for Generalized Detection of Covert Timing Channels. IEEE Military Communications Conference, Baltimore, MD, USA, 2014. P. 7–11. DOI: <https://doi.org/10.1109/MILCOM.2014.10>.
- [24] İ.G. Çavuşoğlu, H. Alemdar and E. Onur. Covert Channel Detection Using Machine Learning. 28th Signal Processing and Communications Applications Conference (SIU), Gaziantep, Turkey, 2020. P. 1–4. DOI: <https://doi.org/10.1109/SIU49456.2020.9302098>.
- [25] M. Chourib. Detecting Selected Network Covert Channels Using Machine Learning. International Conference on High Performance Computing & Simulation (HPCS), Dublin, Ireland, 2019. P. 582–588. DOI: <https://doi.org/10.1109/HPCS48598.2019.9188115>.
- [26] Y. Sun, L. Zhang and C. Zhao. A Study of Network Covert Channel Detection Based on Deep Learning. 2nd IEEE Advanced Information Management, Communication, Electronic and Automation Control Conference (IMCEC), Xi'an, China, 2018. P. 637–641. DOI: <https://doi.org/10.1109/IMCEC.2018.8469669>.

*Поступила в редакцию – 25 марта 2021 г. Окончательный вариант – 07 апреля 2021 г.
Received – March 25, 2021. The final version – April 07, 2021.*