УДК 004.056
Doi: 10.31772/2712-8970-2023-24-4-663-672

Для цитирования: Кононов Д. Д., Исаев С. В. Анализ киберугроз корпоративной сети на основе параллельной обработки данных Netflow // Сибирский аэрокосмический журнал. 2023. Т. 24, № 4. С. 663–672. Doi: 10.31772/2712-8970-2023-24-4-663-672.

For citation: Kononov D. D., Isaev S. V. [Analysis of corporate network cyber threats based on parallel processing of Netflow data]. *Siberian Aerospace Journal.* 2023, Vol. 24, No. 4, P. 663–672. Doi: 10.31772/2712-8970-2023-24-4-663-672.

Анализ киберугроз корпоративной сети на основе параллельной обработки данных Netflow

Д. Д. Кононов*, С. В. Исаев

Институт вычислительного моделирования СО РАН
Российская Федерация, 660036, г. Красноярск, ул. Академгородок, 50/44
*E-mail: ddk@icm.krasn.ru

Публичные сервисы различных организаций подвергаются постоянным кибератакам, что повышает риски информационной безопасности. Анализ сетевого трафика является важной задачей для обеспечения безопасного функционирования сетевой инфраструктуры, в том числе корпоративных сетей. В данной работе представлен обзор основных подходов для анализа сетевого трафика, приведены смежные работы, указаны недостатки существующих работ. Одним из методов является анализ данных сетевого трафика с использованием протокола Netflow, который позволяет сохранять данные о трафике на уровне L3 модели OSI. Особенностью исследования является использование длительных периодов наблюдения. При сохранении данных на длительных временных интервалах журналы имеют большой объем, что требует распараллеливания для первичной обработки данных. Авторами разработан кросс-платформенный программный комплекс распределенной обработки журналов сетевой активности, который использовался для анализа сетевой активности корпоративной сети Красноярского научного центра за 2021–2022 гг. Показана схема программного комплекса, описаны его возможности и особенности функционирования. Приведены источники данных для анализа и методика обработки. В работе были сформулированы и формализованы эвристические критерии аномальности сетевого трафика, которые сигнализируют о наличии возможных атак на сеть, также выделены датасеты по сетевой активности различных протоколов прикладного уровня. Для полученных наборов данных были рассчитаны статистические показатели, на основе которых получена информация об аномальной сетевой активности в течение двух лет. В работе проверен предложенный ранее авторами метод сравнения рисков киберугроз для различных временных интервалов, показавший существенное увеличение рисков для 50 % показателей в 2022 г. Сравнение месячных интервалов за различные годы показало аналогичное увеличение риска. Таким образом, метод доказал свою работоспособность и может применяться в других областях, в которых существуют группы критериев независимых показателей. Авторы привели планы по дальнейшему развитию методики анализа сетевой активности.

Ключевые слова: интернет, сетевая безопасность, анализ сетевого трафика, киберугрозы, корпоративная сеть.

Analysis of corporate network cyber threats based on parallel processing of Netflow data

D. D. Kononov*, S. V. Isaev

Institute of Computational Modelling of SB RAS
50/44, Akademgorodok St., Krasnoyarsk, 660036, Russian Federation
*E-mail: ddk@icm.krasn.ru

Public services of various organizations are subject to constant cyber attacks, which increases information security risks. Network traffic analysis is an important task to ensure the safe operation of network infrastructure, including corporate networks. This paper provides an overview of the main approaches for analyzing network traffic, it provides the related work and points out the shortcomings of the existing work. Here is a method is to analyze network traffic data using the Netflow protocol, which allows traffic data to be stored at the L3 layer of the OSI model. A feature of the study is the use of long observation periods. When storing data over long time intervals, the logs become large, which requires parallelization for primary data processing. The authors developed a cross-platform software package for distributed processing of network activity logs, which was used to analyze the network activity of the corporate network of the Krasnoyarsk Scientific Center for 2021–2022. A diagram of the software package is shown, its capabilities and operating features are described. Data sources for analysis and processing methods are provided. In this paper the authors formulated and formalized heuristic criteria for the anomaly of network traffic, which identify the presence of possible network attacks, and extracted datasets on the network activity of various application-level protocols. For the obtained data sets, statistical indicators were calculated, information about anomalous network activity was obtained for two years. In this research, we tested the previously proposed method for comparing the cyber threats risks for different time intervals, which showed a significant increase in risks for 50% of indicators in 2022. Comparisons of monthly intervals over different years showed similar increases in risk. Therefore, the method has shown its efficiency and can be used in other areas in which there are groups of criteria for independent indicators. The authors have proposed plans for further development of methods for analyzing network activity.

Keywords: Internet, network security, network traffic analysis, risk assessment, cyber threats, corporate network.

Introduction

Currently information technology are used everywhere to organize the work of various services, including corporate ones. Publicly available services are subject to information security risks, which requires to organize comprehensive measures to protect information. One of the important parts ensuring information security is to monitor and analyse network activity (NTA - Network traffic analysis), it allows to detect anomalies in network operation, identify the cause (external or internal) and take appropriate measures. Analysis of network activity is a significant task and is used in various fields. For example, analyzing the network activity of IoT devices permits to identify their type [1] and identify security problems [2]. Fragmented standards and methods for collecting and analyzing network traffic do not often contribute to reproducing the results. Some authors are making attempts to develop universal formats and software for traffic analysis [3]. In spite of automating traffic processing and analysis processes can reduce the number of routine operations, identifying anomalies with the help of a human operator is a problem due to the large volume of data. Machine learning techniques presents the interest to identify anomalies in network activity [4; 5]. Using various techniques to analyse and identify traffic features is applied for mobile devices [6], in particular, the analysis of encrypted traffic allows to determine the mobile applications being used with high accuracy [7]. Therefore, analysis of network activity makes it possible to obtain much useful information that can be used to improve the performance and security of information systems, including corporate network services.

An important part of ensuring information security is assessing the risks of cyber threats. Applying various techniques to analyse network traffic affords to identify anomalies in network activity, which results in assessing the risks of cyber threats to which the network infrastructure is exposed. Risk assessments can be carried out at different time intervals, so it is necessary to be able to assess the dynamics of changes in cyber threat risks.

Related research

Network traffic analysis allows to identify anomalies in the operation of the network infrastructure. Methods to detect network traffic anomalies can be divided into three categories: unsupervised, supervised, and partially supervised. Unsupervised methods are quite common and do not require preliminary data preparation. The normal data are assumed to be found in datasets more often than anomalous ones [8]. Supervised methods involve building models by dividing data into two categories: normal and abnormal. The analyzed data are compared due to two models, and a conclusion is made about whether the data belongs to a certain category [9]. Partially supervised methods involve building a model only for normal data [10] and are simpler and more common than supervised models.

Cluster analysis and classification methods are the most common. Cluster analysis involves dividing the properties and attributes of data into clusters, from which normal and anomalous behavior are distinguished [11]. In general, large clusters are normal and small clusters are abnormal. Classification methods are used to divide data into previously known categories, they can be distributed into the following types: support vector machine (SVM), neural networks, decision tree, statistical methods. One type of classification using supervised learning is the support vector machine (SVM), which is used for training and testing a large amount of data. [12] uses the SVM method to analyze traffic, and high matching accuracy is achieved. Neural network methods use a model of neurons with connections that convert an input signal into an output signal. The method is widespread and used, for example, to identify malicious traffic [13] and build intrusion detection systems (IDS) [14]. Decision tree methods result in constructing a tree consisting of leaves, nodes and edges, which can be used for multi-stage data classification. Research [15] shows its high efficiency in analyzing malicious traffic of IoT devices. Statistical methods are based on Bayes theorem: if the class is known, it is possible to predict the attributes; if the class is unknown, the rules can determine the class based on the available attributes. In [16], a Bayesian network is used to analyze traffic and ensure the security of cloud services.

An important component in protecting information systems and data networks is to assess the risks of cyber threats. Risk assessment methods can be quantitative and qualitative [17]. Quantitative methods operate with numerical indicators, while qualitative methods use fixed categories of “high risk”, “medium risk”, “low risk”. Typically, qualitative methods are subjective and rely on expert judgment, while quantitative methods are objective and enable results to be reproduced. There are various methods to assess the risk of cyber threats [18]. In [19], the authors use various models of a quantitative method for assessing cloud computing cybersecurity risks. Hybrid risk assessment models are also used, combining different approaches [20]. Information security risk assessment is used in various areas: industrial networks [21], Supervisory Control and Data Acquisition (SCADA) management systems [22], Internet of Things (IoT) devices [23]. Some researchers consider risk assessment as a complex task that includes functional safety, physical safety and cybersecurity [24].

The existing research applies different approaches to traffic analysis and cyber threat risk assessment. For example, the authors develop a new technique and use standard test datasets, which does not allow to assess the effectiveness of the method on a real network infrastructure. Other authors apply real data with short time intervals, which does not result in a deep analysis and identification of the dynamics of ongoing processes.

The current research studies the security of the corporate network of the Krasnoyarsk Scientific Center (Federal Research Center KSC SB RAS) based on analyzing Netflow network traffic. The paper describes the use of a statistical method for comparing the risks of cyber threats proposed earlier

by the authors [25]. Unlike the existing research, the method uses long time intervals when analyzing real network traffic and enables to compare the risks of cyber threats at arbitrary intervals.

Data source and processing methodology

The data source to be analyzed is the Netflow network activity data of the edge router and proxy server of the corporate network of the Krasnoyarsk Scientific Center for 2021–2022 period (volume of 680 GB, 19.5 billion records). Data processing is carried out in several stages: 1) collecting statistics of network interfaces using nfcapd agents; 2) extracting data with the nfdump utility; 3) filtering and aggregating the required fields based on specified rules; 4) saving the obtained data for the analysis; 5) applying statistical analysis.

Data processing is performed using the GNetProc software package for distributed processing of network activity developed by the authors in the Go language. The software package consists of several parts: a client, a message broker, and a computing cluster (Fig. 1).

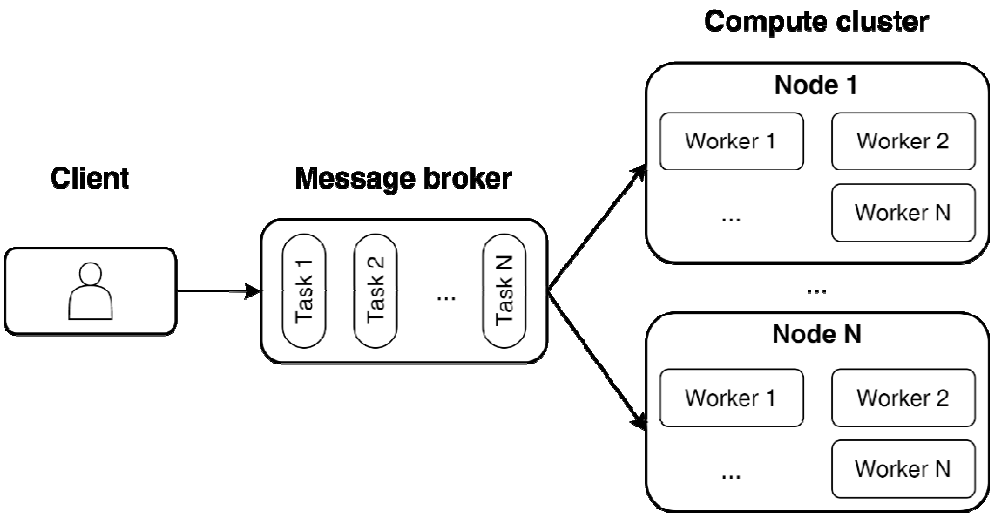

Рис. 1. Архитектура GNetProc

Fig. 1. GNetProc software architecture

The client part interacts with the message broker and allows to send assignments for processing to a common assignment queue, the server part retrieves the assignment from the queue and starts processing using workers. The server part consists of many nodes of a computing cluster; each node can run several workers in parallel, which ensures parallel data processing and reduces assignment execution time. The worker contacts the message broker, receives a new assignment, starts it for execution, saves the processing results, then receives a new assignment. The worker contacts the message broker, receives a new assignment, starts it for execution, saves the processing results, then receives a new assignment. An assignment consists of a list of <name, value> elements that include the data source, data sink, assignment type, aggregation parameters, start and end time intervals, filter, and data selector. A filter, using a special language, allows to specify a set of rules for filtering data. The selector specifies a list of fields that, after filtering and aggregation, will be retrieved and recorded as the result of the assignment. The message broker uses the Redis DBMS to process the assignment queue. YAML is used to describe assignments. The software package is cross-platform and supports work in heterogeneous configurations with Linux, *BSD, and Windows operating systems.

Data analysis

To assess the level of risk of cyber threats based on the principles of normal functioning of various protocols, heuristic criteria for traffic anomaly were formulated:

1. Incoming TCP flows with less than 4 packets indicate that the TCP connection was not completed in a controlled manner. Suspicion of a DoS attack.

2. Incoming TCP flows with a duration of 0 indicate that a TCP connection was not established. Suspicion of a DoS attack.

3. A large number of incoming UDP flows is a suspicion of a DDoS attack.

4. An excess of incoming UDP flows over outgoing ones is a suspicion of a DoS attack.

5. An excess of the number of incoming TCP flows over outgoing ones is a suspicion of a DoS attack.

6. Incoming TCP and UDP flows to unused but routable addresses are suspected of vulnerability scanning (Unused).

7. Incoming TCP flows to common services (MSSQL, MySQL, RDP, SMB, SMTP, SSH, Telnet) – unauthorized login attempts.

These criteria were formalized as rules for the primary traffic processing system according to a given syntax. Having processed the primary data using the created software, the aggregated data were obtained for further analysis. Each data set is a collection of pairs <time label, integral characteristic>. A typical yearly data set consists of 105 thousand records (the number of five-minute intervals in a year) and can be processed using desktop systems such as MS Excel. Figure 2 presents a diagram of the number of streams of zero duration for 2022. Anomalous values do not have a pronounced periodicity, they are several orders of magnitude higher than the average value (35256), due to which their identification can be automated.

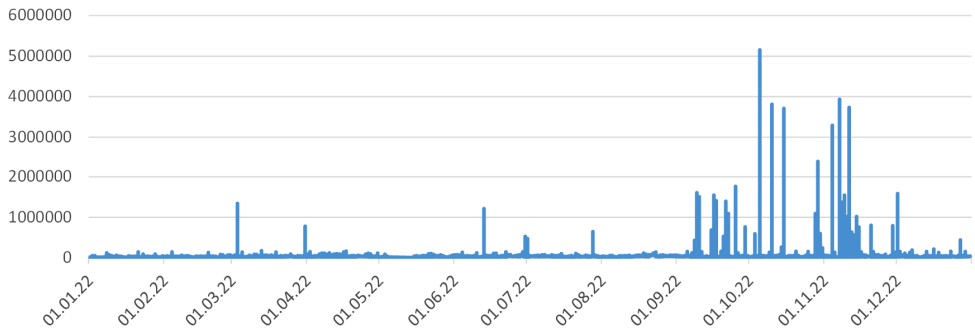

Рис. 2. Количество TCP-потоков нулевой длительностью

Fig. 2. Number of TCP flows with zero duration

The resulting distribution has a clearly expressed right asymmetry, that meets the following condition:

$$Mode < Median < Mean.$$

Figure 3 shows a histogram of the frequency distribution of TCP flows with a duration 0 s. More than 99% of the sample is contained in the interval $[\mu - 3*\sigma, \mu + 3*\sigma]$, which makes it possible to identify cyber threats based on outlier data.

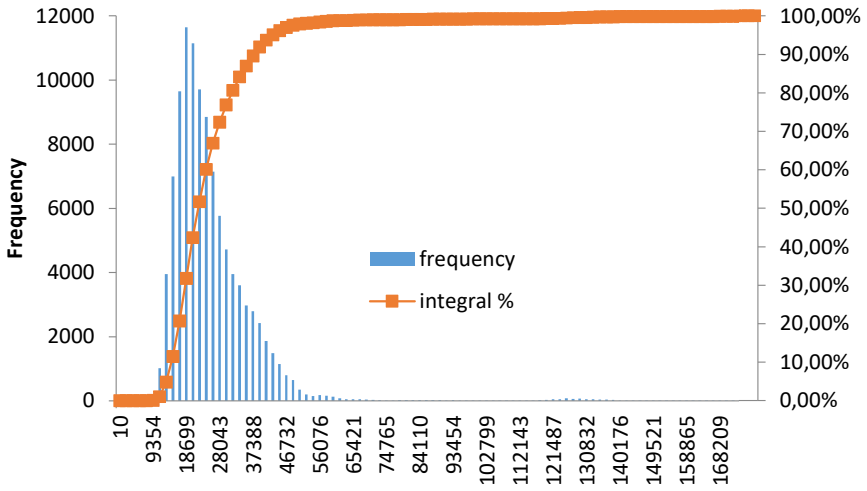

Рис. 3. Гистограмма распределения частот TCP-потоков длительностью 0

Fig. 3. Histogram of frequency distribution of TCP flows with zero duration

For all obtained data sets, the following indicators were calculated: mean, mode, median, standard deviation and percentage of outliers with values greater than 3 standard deviations from the mean. Additionally, the relative increase in the standard deviation of indicators was calculated in 2022 compared to 2021. The findings are in the table: Mean – sample average μ; S – standard deviation σ; Me – sample median; Mo – sample mode; P – percentage of data outside the range [μ – 3*σ, μ + 3*σ]; ΔS – average increase in S in 2022 relatively to 2021.

Indicator results calculated using traffic anomaly criteria

Name	2021					2022					ΔS, %
	Mean	S	Me	Mo	P, %	Mean	S	Me	Mo	P, %	
TCP-flows, duration 0	25205	8343	22079	18975	2.15	35257	14301	29059	22951	1.13	71
TCP-packages < 4 packages	34906	11608	30188	27535	2.35	45287	17732	37461	35331	1.02	53
UDP-flows	15071	5809	13541	13217	2.62	17221	6069	15589	13965	2.95	4
UDP (input-output)	1878	2114	1678	1532	2.08	3511	2428	3175	1325	1.90	15
TCP (input-output)	16759	8751	14846	12540	2.06	26087	11707	21363	16602	1.42	34
Unused TCP	20615	6357	18662	15287	2.30	22035	6736	20457	15148	0.98	6
Unused UDP	965	500	762	376	1.82	1519	1184	862	454	4.24	137
MSSQL	128	63	93	87	7.01	96	30	82	82	3.93	–52
MySQL	21	19	10	3	2.93	32	31	13	5	4.25	63
RDP	105	66	78	39	3.97	120	80	84	40	4.27	21
SMB	367	267	190	128	3.33	224	128	154	129	7.84	–52
SMTP	190	80	166	139	3.88	195	95	162	104	2.98	19
SSH	281	160	197	141	4.19	494	389	270	226	4.02	143
Telnet	405	70	384	363	4.10	922	259	953	1151	0.17	270

All distributions except Telnet 2022 demonstrate right asymmetry. The Telnet 2022 data set has two histogram maxima, which is due to reconfiguration of the data acquisition equipment. Figure 4 shows histograms for 2021 and 2022.

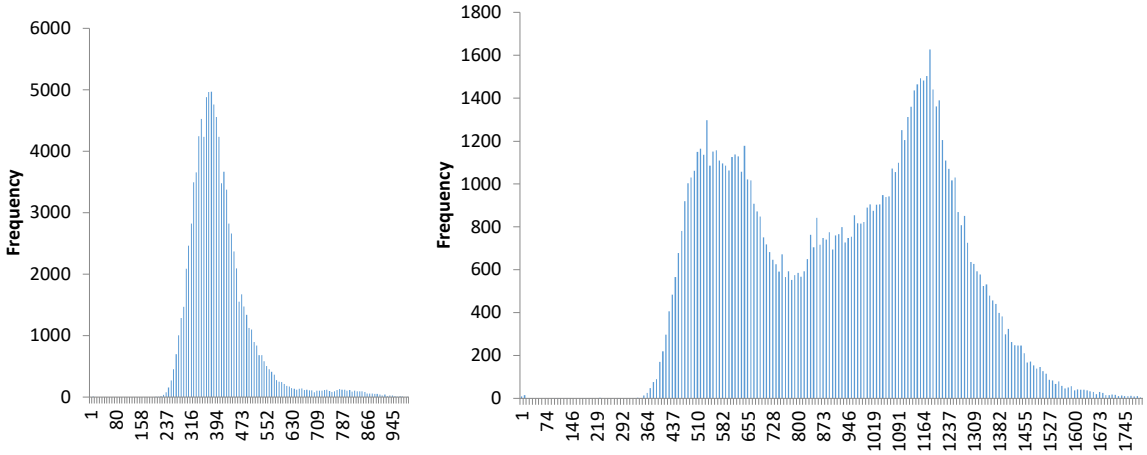

Рис. 4. Гистограмма наборов Telnet за 2021 и 2022 гг.

Fig. 4. Histogram of Telnet datasets for 2021 and 2022

The standard deviation for most data sets for 2022 has a significant increase compared to 2021, indicating an increase in the measure of uncertainty in the occurrence of various computer attacks. Using the risk comparison method described in [25] for the 2021 (V_1) and 2022 (V_2) samples, we calculate the R function for assessing risk changes:

$$R(V_1, V_2) = \frac{1}{N} * \sum_{i=1}^{N} K_i ,$$

where $K_i = \begin{cases} 1, \text{ if } \mu_{2i} > \mu_{1i} + 0,6745 * \sigma_{1i}, \\ 0, \text{ if } \mu_{1i} - 0,6745 * \sigma_{1i} \le \mu_{2i} \le \mu_{1i} + 0,6745 * \sigma_{1i}, \\ -1, \text{ if } \mu_{2i} < \mu_{1i} - 0,6745 * \sigma_{1i}; \end{cases}$ μ_{ji} – sample mean of *i-th* sample characteristic V_j; σ_{ji} – standard deviation of the sample V_j of the *i-th* sample characteristic.

Half of the studied indicators add up to 1, the rest add up to 0, resulting in R(2021, 2022) = 0.5. This can be interpreted as follows: the risk within the framework of the studied criteria as a whole in 2022 compared to 2021 increased significantly - by 50% of the indicators. When comparing March, 2021 and March, 2022 intervals, we get an R value of 0.43. Therefore, the proposed method makes it possible to compare risks both over long time intervals (a year) and over medium ones, provided there are sufficient samples.

Conclusion

The paper examined the risks of cyber attacks based on Internet traffic data from the network of the Krasnoyarsk Scientific Center SB RAS for 2021 and 2022. The cross-platform software for processing large volumes of data was developed, which had scaling capabilities through parallel processing and can perform data analysis in real time. Heuristic criteria for anomalous Internet traffic were formulated and formalized, signaling possible attacks on the network. Statistical indicators were calculated for the obtained data sets, based on them the conclusions were drawn about the shape of the distributions and the dynamics of attacks. The method proposed by the authors for comparing the risks of cyber threats for annual and monthly intervals was tested, which showed a similar increase in risks. Since the method does not depend on the time intervals and sample sizes being compared, it can be used in other areas in which groups of criteria for independent indicators exist. The next task is to expand the analysis criteria taking into account TCP connection flags and application level protocols, taking into ac-

count the logic of their operation. The developed software are planned to use while creating data sets for machine learning methods when solving problems of identifying cyber threats.

Библиографические ссылки

1. Shahid M. R., Blanc G., Zhang Z., and Debar H. IoT Devices Recognition Through Network Traffic Analysis // 2018 IEEE International Conference on Big Data (Big Data). 2018. P. 5187–5192.

2. Sairam R., Bhunia S. S., Thangavelu V., Gurusamy M. NETRA: Enhancing IoT security using NFV-based edge traffic analysis // IEEE Sensors Journal. 2019. No. 19(12). P. 4660–4671.

3. Towards Reproducible Network Traffic Analysis / J. Holland, P. Schmitt, P. Mittal, N. Feamster // arXiv preprint arXiv:2203. 2022. 12410 p.

4. Alqudah N., Yaseen Q. Machine learning for traffic analysis: a review // Procedia Computer Science. 2020. Vol. 170. P. 911–916.

5. Abbasi M., Shahraki A., Taherkordi A. Deep learning for network traffic monitoring and analysis (NTMA): A survey // Computer Communications. 2021. Vol. 170. P. 19–41.

6. The dark side (-channel) of mobile devices: A survey on network traffic analysis / M. Conti, Q. Q. Li, A. Maragno, R. Spolaor // IEEE communications surveys & tutorials. 2018. No. 20(4). P. 2658–2713.

7. Robust smartphone app identification via encrypted network traffic analysis / V. F. Taylor, R. Spolaor, M. Conti, I. Martinovic // IEEE Transactions on Information Forensics and Security. 2017. Vol. 13(1). P. 63–78.

8. Goldstein M., Uchida S. A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data // PloS one. 2016. Vol. 11(4). P.e0152173.

9. Garg R., Mukherjee S. A comparative study using supervised learning for anomaly detection in network traffic // Journal of Physics: Conference Series. 2022. Vol. 2161, No. 1. P. 012030.

10. Comparison of supervised, semi-supervised and unsupervised learning methods in network intrusion detection system (NIDS) application / N. S. Arunraj, R. Hable, M. Fernandes et al. // Anwendungen und Konzepte der Wirtschaftsinformatik. 2017. No. 6. P. 10–19.

11. Zhang P., Ma W., Qian S. Cluster analysis of day-to-day traffic data in networks // Transportation Research Part C: Emerging Technologies. 2022. Vol. 144. P. 103882.

12. Retracted: Traffic identification and traffic analysis based on support vector machine / W. Zhongsheng, W. Jianguo, Y. Sen, G. Jiaqiong // Concurrency and Computation: Practice and Experience. 2020. Vol. 32(2). P. e5292.

13. Malicious network traffic detection based on deep neural networks and association analysis / M. Gao, L. Ma, H. Liu et al. // Sensors. 2020. Vol. 20(5). P. 1452.

14. Vinayakumar R., Soman K. P., Poornachandran P. Evaluation of recurrent neural network and its variants for intrusion detection system (IDS) // International Journal of Information System Modeling and Design (IJISMD). 2017. Vol. 8(3). P. 43–63.

15. Comparing Malware Attack Detection using Machine Learning Techniques in IoT Network Traffic / Y. Z. Wei, M. Md-Arshad, A. A. Samad, N. Ithnin // International Journal of Innovative Computing. 2023. Vol. 13(1). P. 21–27.

16. Nie L., Jiang D., Lv Z. Modeling network traffic for traffic matrix estimation and anomaly detection based on Bayesian network in cloud computing networks // Annals of Telecommunications. 2017. Vol. 72. P. 297–305.

17. Landoll D. The security risk assessment handbook: A complete guide for performing security risk assessments // CRC Press. 2021.

18. Macek D., Magdalenic I., Redep N. B. A systematic literature review on the application of multicriteria decision making methods for information security risk assessment // International Journal of Safety and Security Engineering. 2020. Vol. 10, No. 2. P. 161–174.

19. Jouini M., Rabai L. B. A. Comparative study of information security risk assessment models for cloud computing systems // Procedia Computer Science. 2016. Vol. 83. P. 1084–1089.

20. Haji S., Tan Q., Costa R. S. A hybrid model for information security risk assessment // Int. j. adv. trends comput. sci. eng. 2019. ART-2019-111611.

21. Summary of research on IT network and industrial control network security assessment / L. Hu, H. Li, Z. Wei et al. // 2019 IEEE 3rd information technology, networking, electronic and automation control conference (ITNEC). 2019. P. 1203–1210.

22. A review of cyber security risk assessment methods for SCADA systems / Y. Cherdantseva, P. Burnap, A. Blyth et al. // Computers & security. 2016. Vol. 56. P. 1–27.

23. Mahak M., Singh Y. Threat modelling and risk assessment in internet of things: A review // Proceedings of Second International Conference on Computing, Communications, and Cyber-Security: IC4S 2020, 2021. Springer Singapore. P. 293–305.

24. Lyu X., Ding Y., Yang S. H. Safety and security risk assessment in cyber-physical systems // IET Cyber-Physical Systems: Theory & Applications, 2019. Vol. 4(3). P. 221–232.

25. Исаев С. В., Кононов Д. Д. Исследование динамики и классификация атак на веб-сервисы корпоративной сети // Сибирский аэрокосмический журнал. 2022. Т. 23, № 4. С. 593–600.

References

1. Shahid M. R., Blanc G., Zhang Z., Debar H. IoT Devices Recognition Through Network Traffic Analysis. *2018 IEEE International Conference on Big Data (Big Data)*. 2018, P. 5187–5192.

2. Sairam R., Bhunia S. S., Thangavelu V., Gurusamy M. NETRA: Enhancing IoT security using NFV-based edge traffic analysis. *IEEE Sensors Journal*. 2019, Vol. 19(12), P. 4660–4671.

3. Holland J., Schmitt P., Mittal P., Feamster N. Towards Reproducible Network Traffic Analysis. *arXiv preprint* arXiv:2203. 2022, P. 12410.

4. Alqudah N., Yaseen Q. Machine learning for traffic analysis: a review. *Procedia Computer Science*. 2020, Vol. 170, P. 911–916.

5. Abbasi M., Shahraki A., and Taherkordi A. Deep learning for network traffic monitoring and analysis (NTMA): A survey. *Computer Communications*. 2021, Vol. 170, P. 19–41.

6. Conti M., Li Q. Q., Maragno A., Spolaor R. The dark side (-channel) of mobile devices: A survey on network traffic analysis. *IEEE communications surveys & tutorials*. 2018, Vol. 20(4), P. 2658–2713.

7. Taylor V. F., Spolaor R., Conti M., Martinovic I. Robust smartphone app identification via encrypted network traffic analysis. *IEEE Transactions on Information Forensics and Security*. 2017, Vol. 13(1), P. 63–78.

8. Goldstein M., and Uchida S. A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. *PloS one*. 2016, Vol. 11(4), P. e0152173.

9. Garg R., Mukherjee S. A comparative study using supervised learning for anomaly detection in network traffic. *Journal of Physics: Conference Series*. 2022, Vol. 2161, No. 1, P. 012030.

10. Arunraj N. S., Hable R., Fernandes M., Leidl K., Heigl M. Comparison of supervised, semi-supervised and unsupervised learning methods in network intrusion detection system (NIDS) application. *Anwendungen und Konzepte der Wirtschaftsinformatik*. 2017, No. 6, P. 10–19.

11. Zhang P., Ma W., Qian S. Cluster analysis of day-to-day traffic data in networks. *Transportation Research Part C: Emerging Technologies*. 2022, Vol. 144, P. 103882.

12. Zhongsheng W., Jianguo W., Sen Y., Jiaqiong G. Retracted: Traffic identification and traffic analysis based on support vector machine. *Concurrency and Computation: Practice and Experience*. 2020, Vol. 32(2), P. e5292.

13. Gao M., Ma L., Liu H., Zhang Z., Ning Z., Xu J. Malicious network traffic detection based on deep neural networks and association analysis. *Sensors*. 2020, Vol. 20(5), P. 1452.

14. Vinayakumar R., Soman K. P., Poornachandran P. Evaluation of recurrent neural network and its variants for intrusion detection system (IDS). *International Journal of Information System Modeling and Design (IJISMD)*. 2017, Vol. 8(3), P. 43–63.

15. Wei Y. Z., Md-Arshad M., Samad A. A., Ithnin N. Comparing Malware Attack Detection using Machine Learning Techniques in IoT Network Traffic. *International Journal of Innovative Computing*. 2023, Vol. 13(1), P. 21–27.

16. Nie L., Jiang D., Lv Z. Modeling network traffic for traffic matrix estimation and anomaly detection based on Bayesian network in cloud computing networks. *Annals of Telecommunications*. 2017, Vol. 72, P. 297–305.

17. Landoll D. The security risk assessment handbook: A complete guide for performing security risk assessments. *CRC Press*, 2021.

18. Macek D., Magdalenic I., Redep N. B. A systematic literature review on the application of multicriteria decision making methods for information security risk assessment. *International Journal of Safety and Security Engineering*. 2020, Vol. 10, No. 2, P. 161–174.

19. Jouini M., Rabai L. B. A. Comparative study of information security risk assessment models for cloud computing systems. *Procedia Computer Science*. 2016, 83, P. 1084–1089.

20. Haji S., Tan Q., Costa R.S. A hybrid model for information security risk assessment. *Int. j. adv. trends comput. sci. eng.* 2019, ART-2019-111611.

21. Hu L., Li H., Wei Z., Dong S., Zhang Z. Summary of research on IT network and industrial control network security assessment. *2019 IEEE 3rd information technology, networking, electronic and automation control conference (ITNEC)*. 2019, P. 1203–1210.

22. Cherdantseva Y., Burnap P., Blyth A., Eden P., Jones K., Soulsby H., Stoddart K. A review of cyber security risk assessment methods for SCADA systems. *Computers & security*. 2016, Vol. 56, P. 1–27.

23. Mahak M., Singh Y. Threat modelling and risk assessment in internet of things: A review. *Proceedings of Second International Conference on Computing, Communications, and Cyber-Security: IC4S 2020*. 2021, Springer Singapore, P. 293–305.

24. Lyu X., Ding Y., Yang S. H. Safety and security risk assessment in cyber-physical systems. *IET Cyber-Physical Systems: Theory & Applications*. 2019, Vol. 4(3), P. 221–232.

25. Isaev S. V., Kononov D. D. A study of dynamics and classification of attacks on corporate network web services. *Siberian Aerospace Journal*. 2022, Vol. 23, No. 4, P. 593–601.

Кононов Дмитрий Дмитриевич – научный сотрудник; Институт вычислительного моделирования СО РАН. E-mail: ddk@icm.krasn.ru.

Исаев Сергей Владиславович – кандидат технических наук, доцент, заведующий отделом информационно-телекоммуникационных технологий; Институт вычислительного моделирования СО РАН. E-mail: si@icm.krasn.ru.

Kononov Dmitry Dmitrievich – scientific researcher; Institute of Computational Modelling SB RAS. E-mail: ddk@icm.krasn.ru.

Isaev Sergey Vladislavovich – Cand. Sc., associate professor, head of the Department of Information and Telecommunication Technologies; Institute of Computational Modelling SB RAS. E-mail: si@icm.krasn.ru.