БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2022. – № 2 (105). – 63–73

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056.53 DOI: 10.17212/2782-2230-2022-2-63-73

ОРГАНИЗАЦИЯ МОНИТОРИНГА СЕТЕВЫХ ВТОРЖЕНИЙ НА ОСНОВЕ СВОБОДНО РАСПРОСТРАНЯЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ*

В.А. СИТНИК[1], Д.Д. ВИШНЯКОВ[2], М.В. ЩЕРБА[3]

[1] *644050, РФ, г. Омск, пр. Мира, 11, Омский государственный технический университет, лаборант кафедры комплексной защиты информации. E-mail: viksitnick@yandex.ru*
[2] *644050, РФ, г. Омск, пр. Мира, 11, Омский государственный технический университет, ассистент кафедры комплексной защиты информации. E-mail: ddvishnyakov@omgtu.ru*
[3] *644050, РФ, г. Омск, пр. Мира, 11, Омский государственный технический университет, доцент кафедры комплексной защиты информации. E-mail: mvshcherba@omgtu.ru*

В настоящей работе представлены результаты подготовки виртуального стенда для моделирования и обнаружения сетевых атак с применением свободно распространяемой системы обнаружения вторжений (СОВ) уровня сети. Актуальность работы связана с растущей востребованностью СОВ в качестве источников событий информационной безопасности для систем управления событиями информационной безопасности (SIEM). В ходе работы был выполнен сравнительный анализ наиболее популярных свободно распространяемых сетевых СОВ с открытым исходным кодом и обоснован выбор системы Zeek для ее применения в рамках проекта. В работе используются сетевые журналы Zeek, которые содержат важную и структурированную информацию об анализируемом сетевом трафике. Построение лабораторного стенда выполнено на базе виртуальной машины под управлением ОС Linux и сетевого симулятора Mininet. Предложено графическое представление разработанного виртуального стенда. Продемонстрировано экспериментальное исследование эффективности системы обнаружения вторжений посредством моделирования сетевой атаки типа «отказ в обслуживании» и дальнейшего анализа полученного сетевого трафика средствами СОВ.

Ключевые слова: сетевая безопасность, система обнаружения вторжений, СОВ, виртуальный стенд, сетевая атака, обнаружение аномалий, отказ в обслуживании, Zeek

* Статья получена 10 апреля 2022 г.

ВВЕДЕНИЕ

В современном мире компьютерные сети используются во всех сферах жизни человеческого общества, и, как следствие, проблема обеспечения защищенности информационного пространства не теряет своей актуальности вовсе. Наряду с другими средствами обеспечения сетевой безопасности, включая межсетевые экраны и технологии построения виртуальных частных сетей, системы обнаружения сетевых вторжений разрабатываются и применяются с 80-х годов прошлого века [1] сегодня играют важнейшую роль в архитектуре системы обеспечения безопасности.

Система обнаружения вторжений (СОВ), или Intrusion Detection System (IDS), – программное или программно-техническое средство, реализующее функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней [2].

Система IDS отслеживает сетевой трафик на предмет нетипичной или подозрительной активности и генерирует оповещение об этом. По большому счету в этом и заключается основная функция СОВ – обнаружение аномальной активности в сети или на конкретном хосте и своевременное сообщение об этом пользователю IDS-системы (администратору СОВ, администратору сети и т. д.).

Согласно устоявшейся классификации, представленной в различных источниках [1, 3], выделяют два основных типа СОВ:

- СОВ уровня узла (HIDS – Host-based Intrusion Detection System). Датчики СОВ уровня узла представляют собой программные модули, устанавливаемые на защищаемые узлы информационной системы (ИС) и предназначенные для сбора информации о событиях, возникающих на этих узлах;
- СОВ уровня сети (NIDS – Network-based Detection System). Датчики (сенсоры) собирают информацию о пакетах данных, передаваемых в пределах информационной системы (ИС) (сегмента ИС), в которой (котором) установлены эти датчики. Датчики СОВ уровня сети могут быть реализованы в виде программного обеспечения (ПО), устанавливаемого на стандартные программно-технические платформы, а также в виде программно-технических устройств, подключаемых к ИС (сегменту ИС) [4].

Иными словами, СОВ уровня сети работают с пакетами данных, в то время как СОВ уровня узла / хоста также сфокусированы на том, какие события происходят на самом хосте.

1. ПОСТАНОВКА ЗАДАЧИ

В настоящее время СОВ приобретают особую роль как источники событий информационной безопасности для систем управления событиями информационной безопасности (Security Information and Event Management, SIEM) [5, 6]. При этом открытая архитектура и исходный код СОВ имеет определяющее значение как с точки зрения возможности подключения СОВ к различным SIEM-системам, так и с точки зрения обеспечения безопасности в условиях кибервойны на различных уровнях.

Организация мониторинга сетевых вторжений на основе свободно распространяемой СОВ с открытым исходным кодом в рамках виртуального стенда [7] может существенно повысить эффективность проведения образовательного процесса будущих специалистов, способных предложить интересные решения в области обнаружения сетевых вторжений.

Для подготовки виртуального стенда в целях моделирования и обнаружения сетевых атак были определены следующие задачи:

1) выбрать свободно распространяемую СОВ с открытым исходным кодом;

2) создать виртуальную машину (ВМ) с операционной системой, поддерживаемой выбранной СОВ, и установить необходимый инструментарий;

3) смоделировать сетевую атаку и апробировать работу СОВ.

Сравнительный анализ наиболее популярных свободно распространяемых сетевых СОВ с открытым исходным кодом, включая системы *Zeek* (Bro), *Suricata* и *Snort*, представлен в табл. 1.

Сравнительная характеристика систем обнаружения вторжений

Comparative characteristics of intrusion detection systems

Наименование	Snort	Suricata	Zeek (Bro)
Поддерживаемые операционные системы	Windows, Linux,Unix	Windows, Linux, Unix	Linux, Unix
Режим работы	IDS/IPS	IDS/IPS	IDS
Встроенный графический интерфейс	Отсутствует	Отсутствует	Отсутствует
Основной подход к обнаружению атак	Сигнатурный	Сигнатурный	Выявление аномалий
Лицензия	GPLv2	GPLv2	BSD

Несмотря на то что все рассмотренные СОВ поддерживают сигнатурный подход к обнаружению сетевых атак, развитый инструментарий системы Zeek

направлен на статистический анализ и обнаружение аномалий [8, 9], что определяет более высокие возможности этой системы по определению сетевых атак «нулевого дня». Таким образом, в качестве базовой СОВ для реализации виртуального стенда была выбрана система Zeek ввиду своей гибкости и мощного функционала. Помимо своей работы в качестве IDS система Zeek предоставляет целый ряд сетевых журналов, содержащих полезную и структурированную информацию об анализируемом сетевом трафике.

Для создания виртуальной машины была выбрана ОС Lubuntu версии 18.04.5. LTS. Создание ВМ производилось в среде виртуализации Oracle VM Virtual Box версии 6.1.16. Заданный объем оперативной памяти – 4096 Мб. Для инсталляции системы Zeek необходима предварительная установка некоторых зависимостей (библиотеки, инструменты, иные компоненты). Их перечень приведен в официальной документации Zeek [10].

Помимо системы обнаружения вторжений на виртуальном стенде требуется наличие симулятора компьютерной сети для построения виртуальной топологии. Данная виртуальная сеть используется для моделирования сетевых атак [11] и захвата сетевого трафика. Для построения виртуальной сети был выбран сетевой симулятор Mininet [12]. С помощью простейшего синтаксиса в интерпретаторе команд Mininet можно разворачивать сети из произвольного количества хостов, коммутаторов в различных топологиях, и всё это в рамках одной ВМ. В целях апробации виртуального стенда и моделирования сетевых атак были выбраны инструменты *nmap* для сканирования сети и *LOIC* для имитации DoS-активности.

Схема разрабатываемого виртуального стенда для моделирования и обнаружения сетевых атак выглядит следующим образом (рис. 1).

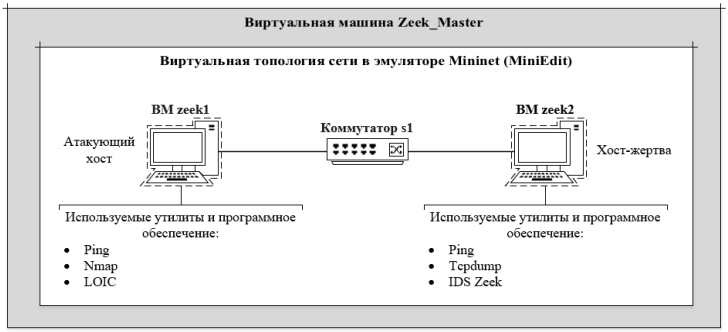

Рис. 1. Схема виртуального стенда

Fig. 1. Graphical representation of the virtual stand

Оба хоста в виртуальной топологии симулятора Mininet имеют доступ к программной среде родительской системы Zeek_Master. Атакующий хост zeek1 предназначен для проведения сетевых атак, в то время как хост-жертва zeek2 используется либо для захвата сетевого трафика в целях дальнейшего исследования, либо для анализа поступающего трафика в режиме реального времени с применением соответствующего режима Zeek.

2. АПРОБАЦИЯ ВИРТУАЛЬНОГО СТЕНДА

В целях апробации подготовленного лабораторного виртуального стенда был проведен эксперимент. На хост-жертву *zeek2* со стороны атакующего хоста *zeek1* была совершена DoS-атака типа *SYN Flood* [13]. Для моделирования атаки был использован программный инструмент *LOIC* [14]. Интерфейс и заданные параметры атаки представлены на рис. 2. Заданные параметры: IP-адрес жертвы – 10.0.0.2; целевой порт – 80; целевой метод (протокол) – TCP; число потоков – 20; число сокетов на поток – 25; полезная нагрузка пакета – TCP TEST.

Для захвата сетевого трафика виртуальной машиной *zeek2* была использована утилита *tcpdump*. В результате захвата сетевого трафика была зафиксирована нетипичная сетевая активность.

Для анализа захваченного сетевого трафика файл захвата *tcptraffic.pcap* был обработан механизмом событий *Zeek* посредством выполнения команды *zeek –C –r tcptraffic.pcap*. Здесь ключ *–r* используется для считывания данных из соответствующего файла, а ключ *–C* для отключения проверки контрольных сумм.

После обработки захваченный сетевых пакетов *Zeek* генерирует ряд файлов журналов, содержащих исчерпывающую информацию об установленных соединениях. Одним из самых информативных является лог-файл *conn.log*, который содержит информацию об IP-адресах и портах источника / назначения, данные о длительности установленных соединений и т. д. (рис. 2).

С помощью встроенной в *Zeek* утилиты *zeek-cut* из полученных файлов журналов можно сделать необходимую выборку по различным полям, задавая соответствующие параметры. К файлу *conn.log* был выполнен запрос на вывод в порядке убывания IP-адресов назначения, которые получили большую часть сетевого трафика (рис. 3).

Также был сформирован практически идентичный запрос к лог-файлу conn.log, но уже на вывод целевых портов (рис. 4):

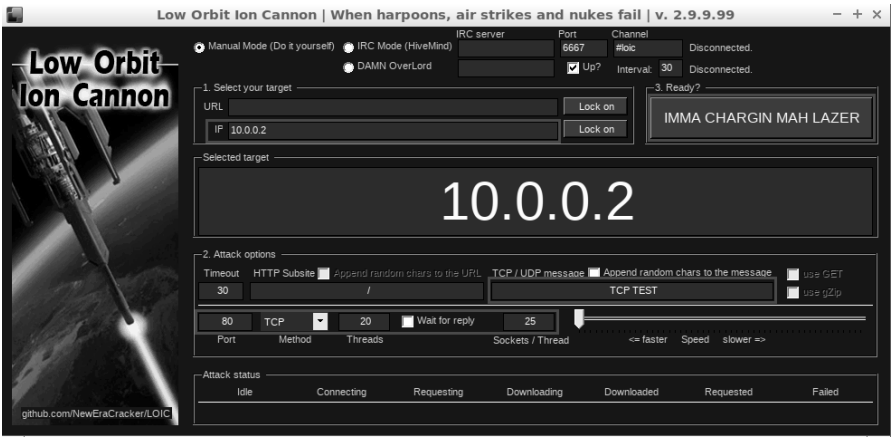

Рис. 2. Окно задания параметров атаки

Fig. 2. Window for setting attack parameters

```
zeek@admin:~/Zeek-Labs/TCP-Traffic$ zeek-cut id.resp_h < conn.log | sort | uniq
-c | sort -rn | head -n 10
  91577 10.0.0.2
      4 ff02::2
```

Рис. 3. Результат выполнения запроса на вывод IP-адресов

Fig. 3. Query result

```
zeek@admin:~/Zeek-Labs/TCP-Traffic$ zeek-cut id.resp_p < conn.log | sort | uniq
-c | sort -rn | head -n 10
  91577 80
      4 134
```

Рис. 4. Результат выполнения запроса на вывод целевых портов

Fig. 4. Query result

Фактически в результате первичного анализа захваченного сетевого трафика были получены значения IP-адреса атакуемого узла – 10.0.0.2 и целевого порта – 80, что совпадает с заданными ранее параметрами проведения *SYN Flood* атаки.

ЗАКЛЮЧЕНИЕ

Таким образом, в результате выполненной работы был подготовлен виртуальный лабораторный стенд для моделирования и обнаружения сетевых атак. В целях апробации данного стенда была смоделирована DoS-атака типа *SYN Flood* и продемонстрированы базовые возможности системы *Zeek* по обработке захваченного сетевого трафика. При этом полное описание продвинутого функционала системы *Zeek* выходит за рамки настоящей работы, но может быть изучено на базе предложенного виртуального стенда.

Предложенный виртуальный стенд в дальнейшем может быть дополнен новым инструментарием для проведения различных сетевых атак [15], а виртуальная топология сети может быть изменена в соответствии с решаемой задачей.

СПИСОК ЛИТЕРАТУРЫ

1. *Bruneau G.* The history and evolution of intrusion detection: Technical report. – The SANS Institute, 2001. – URL: https://www.sans.org/white-papers/344/ (accessed: 20.03.2022).

2. Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты: утв. ФСТЭК России 03.02.2012. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty (дата обращения: 03.06.2022).

3. *Котов В.Д., Васильев В.И.* Современное состояние проблемы обнаружения сетевых вторжений // Вестник Уфимского государственного авиационного технического университета. – 2012. – Т. 16, № 3 (48). – С. 198–204.

4. *Комаров А.* Системы обнаружения вторжений, сертифицированные по новым требованиям. – 2018, 22 августа. – URL: https://zlonov.com/new-fstec-ips (дата обращения: 03.06.2022).

5. *Haas S., Sommer R., Fischer M.* Zeek-osquery: Host-network correlation for advanced monitoring and intrusion detection // IFIP International Conference on ICT Systems Security and Privacy Protection. – Maribor, Slovenia, 2020. – P. 248–262.

6. *Скорых М.А.* Применение фреймворка Zeek и ELK-стека для анализа рассылок вредоносного программного обеспечения // Актуальные проблемы инфотелекоммуникаций в науке и образовании, АПИНО 2021: X юбилейная международная научно-техническая и научно-методическая конференция: в 4 т. – СПб.: СПбГУТ, 2021. – Т. 1. – С. 658–661.

7. *Жданов Н.С., Матерухин А.В.* Использование виртуальной лабораторной среды для обучения студентов навыкам тестирования на проникновение // Безопасность информационных технологий. – 2020. – Т. 27, № 4. – С. 95–107. – DOI: 10.26583/bit.2020.4.08.

8. Comparing machine learning techniques for Zeek log analysis / D.K. Andrews, R.K. Agrawal, S.J. Matthews, A.S. Mentis // 2019 IEEE MIT Undergraduate Research Technology Conference (URTC). – Cambridge, MA, 2019. – P. 1–4.

9. *Красненков А.М., Чернокнижный Г.М.* Учебный практикум по изучению систем обнаружения вторжений на базе нейронной сети // Актуальные вопросы информационной безопасности и защиты информации. – СПб., 2021. – С. 40–48.

10. Installing Zeek. – URL: https://docs.zeek.org/en/current/install.html#id2 (accessed: 03.05.2022).

11. *Shcherba E.V.* Boolean-valued models of telecommunication systems in some problems of network security // 2015 International Siberian Conference on Control and Communications (SIBCON). – Omsk, Russia, 2015. – P. 1–5.

12. *Xiang Z., Seeling P.* Mininet: an instant virtual network on your computer // Computing in Communication Networks. – London: Academic Press, an imprint of Elsevier, 2020. – P. 219–230.

13. *Щерба Е.В., Щерба М.В.* Разработка архитектуры системы обнаружения распределенных сетевых атак типа «отказ в обслуживании» // Омский научный вестник. – 2012. – № 3 (113). – С. 280–283.

14. *Fadhlillah A., Karna N., Irawan A.* IDS performance analysis using anomaly-based detection method for DOS attack // 2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS). – Bali, Indonesia, 2021. – P. 18–22.

15. *Litvinov A.G., Shcherba E.V.* Modeling message spoofing attacks on the OLSR routing protocol // 2019 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). – Yekaterinburg, Russia, 2019. – P. 299–302.

Ситник Виктория Амангельдиновна, лаборант кафедры комплексной защиты информации Омского государственного технического университета. Основное направление научных исследований – проблемы обеспечения безопасности сетевой инфраструктуры. E-mail: viksitnick@yandex.ru

Вишняков Денис Дмитриевич, ассистент кафедры комплексной защиты информации Омского государственного технического университета. Основное направление научных исследований – проблемы обеспечения безопасности сетевой инфраструктуры. E-mail: ddvishnyakov@omgtu.ru

Щерба Мария Витальевна, доцент кафедры комплексной защиты информации Омского государственного технического университета. Основное направление научных исследований – проблемы обеспечения безопасности сетевой инфраструктуры. E-mail: mvshcherba@omgtu.ru

DOI: 10.17212/2782-2230-2022-2-63-73

Organization of monitoring of network intrusions on the basis of freely distributable software*

V.A. Sitnik[1], D.D. Vishnyakov[2], M.V. Shcherba[3]

[1] *Omsk State Technical University, 11 Mira Prospekt, Omsk, 644050, Russian Federation, laboratory assistant of the Complex Information Protection Department. E-mail: viksitnick@yandex.ru*
[2] *Omsk State Technical University, 11 Mira Prospekt, Omsk, 644050, Russian Federation, assistant of the Complex Information Protection Department. E-mail: ddvishnyakov@omgtu.ru*
[3] *Omsk State Technical University, 11 Mira Prospekt, Omsk, 644050, Russian Federation, associate professor of the Complex Information Protection Department. E-mail: mvshcherba@omgtu.ru*

This paper presents the results of preparing a virtual bench for modeling and detecting network attacks using a freely distributed intrusion detection system (IDS). The relevance of the work is related to the growing demand for IDS as sources of information security events for security information and event management (SIEM) systems. A comparative analysis of the most popular freely distributed open-source network IDSs was carried out and the choice of the Zeek system for its use in the project was substantiated. The work uses Zeek network logs, which contain important and structured information about the analyzed network traffic. The laboratory bench was built on the basis of a Linux virtual machine and a Mininet network simulator. A graphical representation of the developed virtual stand is proposed. An experimental study of the effectiveness of an intrusion detection system is demonstrated by simulating a network denial of service attack and further analyzing the received network traffic using IDS tools.

Keywords: network security, intrusion detection system, IDS, virtual stand, network attack, anomaly detection, denial of service, Zeek

REFERENCES

1. Bruneau G. *The history and evolution of intrusion detection*. Technical report. The SANS Institute, 2001. Available at: https://www.sans.org/white-papers/344/ (accessed 20.03.2022).

* *Received 10 April 2022.*

2. *Methodological document of the FSTEC of Russia. Protection profile of the intrusion detection system of the network level of the fourth class of IT security*. Approved by the FSTEC of Russia on February 03, 2012. (In Russian). Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty (accessed 03.06.2022).

3. Kotov V.D., Vasilyev V.I. Sovremennoe sostoyanie problemy obnaruzheniya setevykh vtorzhenii [Current state of network intrusion detection]. *Vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta = Vestnik USATU*, 2012, vol. 16, no. 3 (48), pp. 198–204.

4. Komarov A. *Sistemy obnaruzheniya vtorzhenii, sertifitsirovannye po novym trebovaniyam* [Intrusion detection systems certified according to new requirements]. 2018, August 22. Available at: https://zlonov.com/new-fstec-ips (accessed 03.06.2022).

5. Haas S., Sommer R., Fischer M. Zeek-osquery: Host-network correlation for advanced monitoring and intrusion detection. *IFIP International Conference on ICT Systems Security and Privacy Protection*, Maribor, Slovenia, 2020, pp. 248–262.

6. Skorykh M.A. [Using of the Zeek framework and ELK-stack for malware distribution analysis]. *Aktual'nye problemy infotelekommunikatsii v nauke i obrazovanii*. V 4 t. [10th International Conference on Advanced Infotelecommunications, ICAIT 2021. In 4 vols]. St. Petersburg, 2021, vol. 1, pp. 658–661. (In Russian).

7. Zhdanov N., Materukhin A. Ispol'zovanie virtual'noi laboratornoi sredy dlya obucheniya studentov navykam testirovaniya na proniknovenie [Using a virtual laboratory environment for penetration-testing skills training]. *Bezopasnost' informatsionnykh tekhnologii = IT Security (Russia)*, 2020, vol. 27, no. 4, pp. 95–107. DOI: 10.26583/bit.2020.4.08.

8. Andrews D.K., Agrawal R.K., Matthews S.J., Mentis A.S. Comparing machine learning techniques for Zeek log analysis. *2019 IEEE MIT Under-graduate Research Technology Conference (URTC)*, Cambridge, MA, 2019, pp. 1–4.

9. Krasnenkov A.M., Chernoknizhnyi G.M. Uchebnyi praktikum po izucheniyu sistem obnaruzheniya vtorzhenii na baze neironnoi seti [Training workshop on the study of intrusion detection systems based on a neural network]. *Aktual'nye voprosy informatsi-onnoi bezopasnosti i zashchity informatsii* [Topical issues of information security and information protection]. St. Petersburg, 2021, pp. 40–48.

10. *Installing Zeek*. Available at: https://docs.zeek.org/en/current/install.html#id2 (accessed 03.05.2022).

11. Shcherba E.V. Boolean-valued models of telecommunication systems in some problems of network security. *2015 International Siberian Conference on Control and Communications (SIBCON)*, Omsk, Russia, 2015, pp. 1–5.

12. Xiang Z., Seeling P. Mininet: an instant virtual network on your computer. *Computing in Communication Networks*. London: Academic Press, an imprint of Elsevier, 2020, pp. 219–230.

13. Shcherba E.V., Shcherba M.V. Razrabotka arkhitektury sistemy obnaruzheniya raspredelennykh setevykh atak tipa «otkaz v obsluzhivanii» [Architecture development for DDoS attack detection system]. *Omskii nauchnyi vestnik = Omsk Scientific Bulletin*, 2012, no. 3 (113), pp. 280–283.

14. Fadhlillah A., Karna N., Irawan A. IDS performance analysis using anomaly-based detection method for DOS attack. *2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*, Bali, Indonesia, 2021, pp. 18–22.

15. Litvinov A.G., Shcherba E.V. Modeling message spoofing attacks on the OLSR routing protocol. *2019 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, Yekaterinburg, Russia, 2019, pp. 299–302.

Для цитирования:

Ситник В.А., Вишняков Д.Д., Щерба М.В. Организация мониторинга сетевых вторжений на основе свободно распространяемого программного обеспечения // Безопасность цифровых технологий. – 2022. – № 2 (105). – С. 63–73. – DOI: 10.17212/2782-2230-2022-2-63-73.

For citation:

Sitnik V.A., Vishnyakov D.D., Shcherba M.V. Organizatsiya monitoringa setevykh vtorzhenii na osnove svobodno rasprostranyaemogo programmnogo obespecheniya [Organization of monitoring of network intrusions on the basis of freely distributable software]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2022, no. 2 (105), pp. 63–73. DOI: 10.17212/2782-2230-2022-2-63-73.