UDC 004.056.5

A SHORT SURVEY OF THE CAPABILITIES OF NEXT GENERATION FIREWALLS

Sichkar Mykhailo, Pavlova Larysa

V.N. Karazin National University, Kharkiv, 61022, Ukraine
sichkar2020kb13@student.karazin.ua, l.v.pavlova@karazin.ua

Received: on October 2023. Accepted: on November 2023.

Abstract: *This article examines the history, types, capabilities, and advantages of next-generation firewall (NGFW) technology. Firewalls are an important tool for protecting network resources from various information security threats. With the development of technology and the changing nature of attacks, especially those involving artificial intelligence, firewalls have also evolved, acquiring new functions and capabilities. This work provides a short survey of the main types, capabilities and benefits of next-generation firewall (NGFW) technology, which is a modern solution for comprehensive network protection against complex and sophisticated security threats. The work also analyzes the distinct features of NGFW and differences between NGFW and previous generations of firewalls, as well as examples of NGFW from well-known vendors that dominate the market, such as Palo Alto Networks, Fortinet and Cisco. The article highlights the main trends, prospects for the development and implementation of NGFW, including the impact of artificial intelligence, machine learning, cloud technologies and the Internet of Things, advantages and disadvantages, capabilities, important aspects, purpose and sphere of application. The article also addresses the significant impact this technology will have on network security. It is emphasized that the introduction of NGFW does not replace other security technologies and tools, but effectively expands the existing arsenal of countering new security threats (primarily as an instrument of proactive countermeasures and rapid response to complex network incidents). The article may be useful for students, researchers, and information security professionals who seek to expand their competencies related to the development of modern firewall technologies and their capabilities.*

Keywords*: NGFW, Firewalls, Information Security, Cybersecurity, Malware.*

1. Introduction

Ensuring the security of modern computer networks is one of the most important aspects of information security (IS), as both the number and complexity of computer threats are increasing every day. Amidst the measures and activities used to counteract the modern cyber attacks, firewalls are undoubtedly one of the most powerful tools for protecting network resources from a number of different threats [1-6]. They provide the ability to administer network access, effectively filter network traffic, and timely detect and block potentially dangerous network activity [7-8, 5].

2. Main part

A firewall is a network security tool that controls and administers incoming and outgoing network traffic and determines whether to allow or block specific traffic based on a set of security rules. Firewalls have been acting as a conditional "first line of defense" in the field of network security for more than 25 years. They establish a kind of barrier between secure and controlled internal networks and untrusted, i.e. "external" to the controlled resources, networks and/or their users. In general, a firewall can be: - hardware, software, software as a service (*SaaS*), public-cloud or private-cloud (*virtual*) [9]. To understand the principles of functioning of different types of firewalls, it is important to realize their place and role at the appropriate levels of the OSI model [10].

The evolution of firewall filtering technologies. 1988 - the first generation, packet filtering firewalls; 1989 - the second generation, the so-called "Stateful Firewall"; 1991 - the third generation, the appliance-level firewall; 2004 - IDC (International Data Corporation) introduces the term "Unified Threat Management" (UTM); 2009 - Gartner defines the next-generation firewall (NGFW) [11].

In 1988, the Digital Equipment Corporation (*DEC*) introduced the first generation of internetwork traffic filtering technology called the Packet-Filter Firewall [12]. These firewalls analyzed

packets of information that circulated between computers on the network. If a packet did not meet the rules of the packet filtering firewall, it was rejected. Packets that met the filtering criteria were allowed to be transmitted. The filtering rules were based on various parameters, such as: source and destination addresses, protocols used, and port numbers on both of the communicating computers. It is important to note that this type of firewall did not take into account the connection state of the packet and did not store its state. Because of this, it was called *«Stateless Firewalls»*. They functioned at the network layer of the OSI model and were also known as *«Network Layer Firewalls»* [10].

In 1989, AT&T Bell Labs first developed a second-generation firewall technology called Circuit Level Gateway, which was the first to introduce firewall, known as *Stateful Firewall*. *Stateful Firewall* keeps track of active network sessions and connection states. These firewalls use information about the state of the connection to control the packet filtering process. If a packet that is to be transmitted does not match an active connection, it is evaluated against a set of filtering rules that are set up for creating new connections. *Stateful Firewalls*, once a connection is established, transmit only packets that are associated with the connections specified in the dynamic state tables. Sessions stored in these tables are automatically closed if there has been no data transmission for a certain time interval to prevent state tables from overflowing. *Stateful Firewalls* are the second type of network-level firewalls, but they also function at a transport layer [10].

In 1991, Digital Equipment Corporation introduced the 3rd generation of firewall technology (*SEAL - Secure External Access Link*), which was called the *«Application Layer Firewall»*. These firewalls operate at the *OSI* application layer [10], and their main goal is to protect computers from malicious software. Thus, application-level firewalls (*Gauntlet by Trusted Information Systems and FireWall-1 by Check Point in 1994*) control the traffic of applications, such as web browsers and others, that connect to the Internet and/or other "external networks" and transmit or receive data from them. It also regulates traffic on the FTP, Telnet, and HTTP protocols [7,10].

In 2004, IDC introduced a new term - Unified Threat Management (*UTM*). Under the new terminology, the evolution of traditional (*i.e., previous models*) firewalls should be viewed as an attempt to create a new integrated solution for network security. UTM involves the simultaneous use of technologies such as a network firewall, web page filtering, gateway antivirus, intrusion prevention system (*IPS*), anti-spam, VPN, etc. [7,10].

In 2009, Gartner introduced the concept of «Next-Generation FireWall» (*NGFW*). The *NG* firewall simultaneously uses the concepts of a traditional firewall and some new technologies: – IPS, Deep Packet Inspection (*DPI*), sandboxing, application control, URL filtering, protection against complex/integrated malware, network profiling, identity policy, VPN, etc. At the same time, the most distinctive feature of NGFW is the *DPI* function at the application level, not only within the framework of port and protocol inspection, which was typical for previous solutions [10,13].

In this way, software and hardware NGFWs combine the functions of a traditional firewall and an intrusion prevention system. The use of such software and hardware NGFWs helps to increase the level of security of network traffic.

Let us briefly consider the key features and benefits of NGFW solutions (Fig. 1).

Capabilities.

1. Analyzing and filtering traffic not just by port, but at the application level.

2. Implementing IPS, which allows blocking unwanted traffic in a timely manner or disconnect part of the network to prevent the spread of the threat.

3. DPI, which analyzes the smallest details of data packets, including the data sender and receiver.

4. Supporting application traffic control lists.

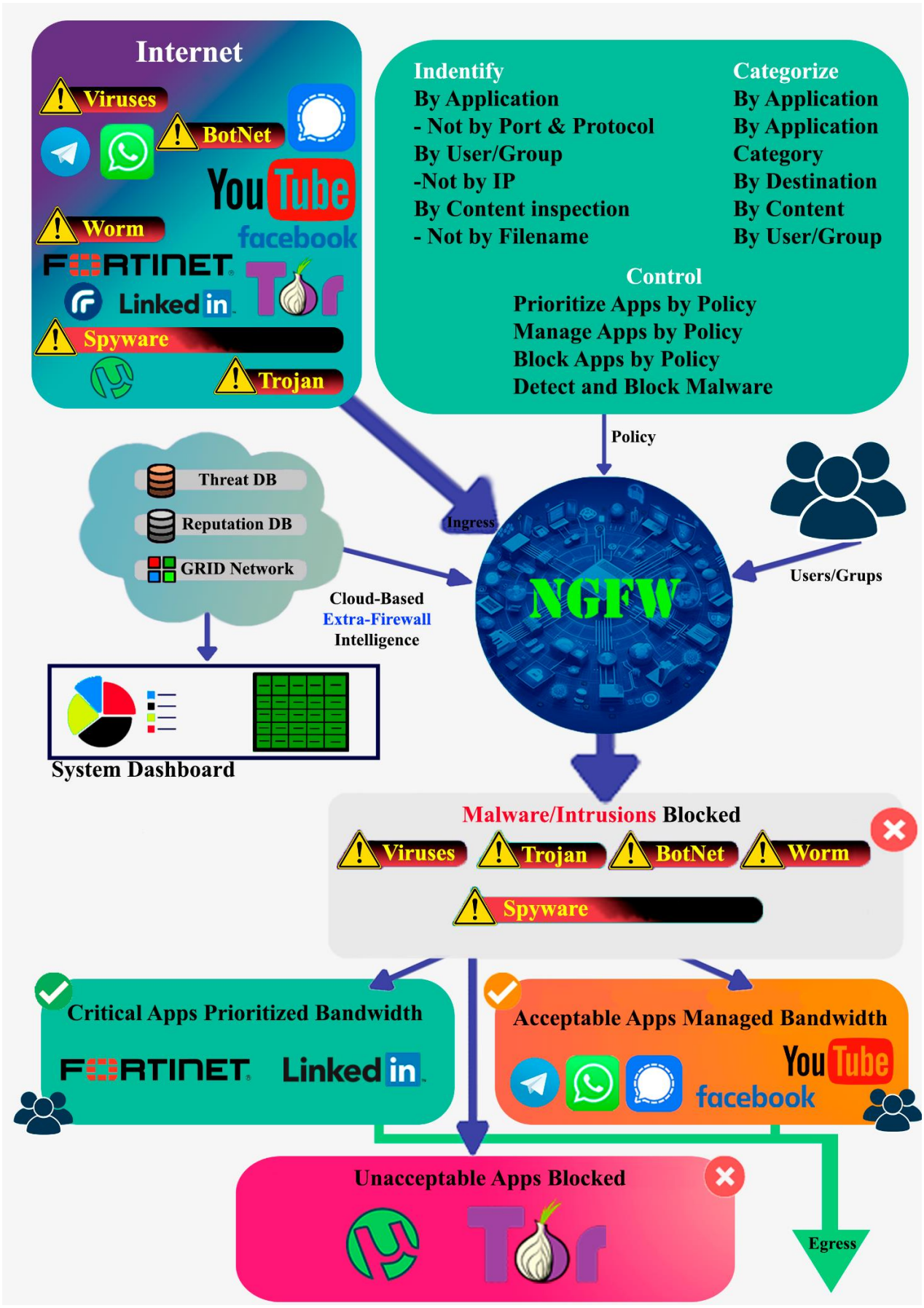

Fig. 1 - Generalized interpretation of the NGFW concept

5. Implementing a centralized network management console that simplifies network configuration and monitoring.

Benefits.

1. Increased performance: - is achieved through the use of DPI, which allows identifying and managing applications regardless of their IP port.

2. Multifunctionality: - as the result of integrating IDS and IPS systems that detect attacks based on network behavior analysis (*NBA*), threat signatures, and anomalous activity, while retaining all the functions of traditional firewalls. That provides for in-depth inspection of network traffic and improves filtering of the packet content at the application level.

3. Content filtering: - the ability to filter content is very useful for preventing unauthorized data leakage in real time.

4. Visibility and manageability makes it possible for security administrators to control the network and to identify users. Integration with third-party user directories makes it easier to control and identify users and groups.

5. Prevention and mitigation of the effects of security threats: - antivirus and anti-malware software that is automatically updated whenever new security threats appear [14]. Also, it is possible to restrict the running applications by checking them for potential vulnerabilities [2,6].

6. Advanced security policy control provides a detailed level of control over applications, blocking negative aspects of their operation (*for example, excessive traffic during peak times*).

7. Low cost: as the result of deep integration of several solutions under the control of a single management console [15].

Solutions based on NGFW technology are offered by most large companies, such as: Palo Alto Networks Fortinet, Cisco and others [6,13], where each of them offers a wide range of functions and capabilities to protect against various threats (network security gateways). Common security features are: *firewall protection; IPS; URL filtering; malware protection; DLP; identity matching (IDP); role-based access control (RBAC); content control. In general, such solutions are used in the following areas: large organizations and government agencies; small and medium-sized enterprises; banks and financial institutions; ordinary organizations and businesses* [5-8,13].

For example, Palo Alto Networks offers NGFWs for different enterprise environments and in several variants: physical, virtual, and containerized. Physical firewalls are hardware devices that are directly installed in a data center or office. Virtual solutions are software products that can run on virtual machines, and container solutions are specially designed products for protecting container environments. For enhanced performance, Panorama is a configuration and policy management solution that allows network security administrators to centrally manage all Palo Alto firewalls, regardless of type and/or location. That allows network security administrators to create and edit security policies easily [16].

Fortinet's solutions are available in several variants, including physical, virtual, and containerized. The proprietary FortiOS operating system supports unified policy configuration, enabling network administrators to manage all policies, including access to Zero Trust Networks (*ZTNA*). FortiGuard security services are available to Fortigate users, providing such features as IP geotracking and IoT device detection. The cloud sandbox feature addresses potential security threats (*e.g., the so-called "zero-day"* [2]).

FortiGuard's capabilities allow monitoring specific device and network policies, including operational technology policies, and its *IPS* accesses threat signature libraries and uses artificial intelligence and machine learning (*AI/LM*) capabilities to block these threats based on existing IPS rules. Fortigate is a versatile NGFW solution that is suitable for businesses with multiple data centers as well as single branch offices.

Thus, NGFW Fortigate has the following key differences: a wide range of deployment options and firewall bandwidth; a cloud-based sandbox; its own operating system that allows administering network security policies [15].

Cisco Secure Firewall focuses on extending policy enforcement to all distributed applications on your network, making the network infrastructure a part of the firewall security.

Cisco has several hardware firewalls (*e.g., Firepower and Meraki MX series*), and Cisco Secure Firewall (*CSF*) is available as a virtualized private cloud solution that provides protection in VMware ESXi, Microsoft Hyper-V, and KVM (*Kernel-based Virtual Machine*) environments [15]. It also exists as a public cloud solution for data and application security on Azure and AWS (*Amazon Web Services*).

Cisco's NGFW solutions use behavioral analytics to respond to threats faster, and for the log management data from all CSF firewalls in the enterprise network (*even geographically disrtibuted*) are used. Cisco Transport Layer Security (*TLS*) Server Identity and Discovery allows supporting OSI Layer 7 security policies for the encrypted traffic (TLS 1.3). In this case, network administrators have an opportunity to monitor the traffic, even if it is not decrypted, and Layer 7 security policies remaining unchanged.

Thus, Cisco's NGFW has the following key differences: - firewall log management with behavioral analytics; immutable OSI Layer 7 policies for encrypted traffic; virtual firewall with support for multiple virtual environments.

3. Conclusions

1. *NGFW* solutions have a good potential: They offer a broader range of security features than previous iterations, and they can be deployed in the cloud to detect and block malicious traffic, phishing attacks [3], denial-of-service attacks, and other security threats [2,6-8].

2. *NGFWs* use *AI* and *LM* technologies to detect both new and evolving threats [2,14], which greatly facilitates the task of countering them when they cannot be detected by traditional methods *(e.g., signature scanning).*

3. The main trends that will directly influence the development and implementation of *NGFW* include the following

- growing influence of *AI* and *LM* technologies. That is, *NGFWs* will increasingly rely on *AI* and *LM* capabilities to identify new and evolving types of security threats [2,5];
- increasing adoption of cloud technologies. *NGFWs* will increasingly gravitate towards cloud deployment, which may make them more affordable and easier to maintain and use;
- the increased scale of application and integration of modern *IS* threats. Obviously, *NGFWs* have greater potential against network bot systems that generate complex polymorphic and/or targeted malware.

References

[1] Азаров, С., Нємцев, М., & Малахов, С. Огляд аналогій та обгрунтування принципів створення демон юнітів відстеження мережевої активності користувачів. Proceedings of the XX International Scientific and Practical Conference. Graz, Austria. 2023. Pp. 447-453. https://isg-konf.com/technologies-innovative-and-modern-theories-of-scientists/

[2] Богданова, Є., Чорна, Т., & Малахов, С. (2022). Огляд поточного стану загроз, що обумовлені впливом експлойтів. *Комп'ютерні науки та кібербезпека,* (2), 35-40. https://periodicals.karazin.ua/cscs/article/view/21039/19745

[3] Лєсная, Ю., Малахов, С. Узагальнення основних передумов реалізації фішингових атак. Proceedings of the XVII International Scientific and Practical Conference. Ankara, Turkey. 2023. Pp.453-457. https://isg-konf.com/system-analysis-and-intelligent-systems-for-management/

[4] Мелкозьорова, О., Лєсная, Ю., & Малахов, С. (2022). Особливості інтеграції систем захисту від несанкціонованих дій в сучасних інформаційних системах. *Комп'ютерні науки та кібербезпека,* (1), 39-44. https://periodicals.karazin.ua/cscs/article/view/20912/19616

[5] Михайленко Д., Нємцев М. Особливості технології мережевих пасток як інструменту активного захисту та аналізу дій атакуючої сторони. Proceedings of the XXI International Scientific and Practical Conference. Melbourne, Australia. 2023. Pp. 483-487. https://isg-konf.com/scientists-and-methods-of-using-modern-technologies/
[6] Погоріла К.В., Богданова Є.С., Колованова Є.П. Огляд можливостей та узагальнення специфіки реалізації XDR-технології, як засобу комплексної протидії актуальним загрозам інформаційної безпеки. Технології, інструменти та стратегії реалізації наукових досліджень: матеріали IV Міжнародної наукової конференції, м. Суми, 07.10.2022 р. / МЦНД. – Вінниця: Європейська наукова платформа, 2022. - 142 с. DOI 10.36074/mcnd-07.10.2022
[7] Джон Маллери, & Джейсон Занн (2007). Безопасная сеть вашей компании. (Е. Линдеманн, пер. с англ.). – М.: НТ Пресс
[8] Рондалєв, Д., Мелкозьорова, О., & Нарєжній, О. (2019). Особливості функціонування корпоративного міжмережевого екрану та питання взаємодії з системою IDS. *Комп'ютерні науки та кібербезпека,* (3), 11-21. https://periodicals.karazin.ua/cscs/article/view/15614/14707
[9] Next-Generation Firewalls. Вилучено з https://www.paloaltonetworks.com/network-security/next-generation-firewall
[10] Who Invented the Firewall? History, Types, and Generations of Firewall. (2023). Вилучено з https://www.thepcinsider.com/who-invented-firewall-history-evolution-types-generations/
[11] What Is a Firewall? Вилучено з https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html
[12] 8 Types of Firewalls: Know Which One Is Best for Your Network By John Villanueva. (2022). Вилучено з https://techgenix.com/types-of-firewalls
[13] Information Technology Gartner Glossary. Вилучено з https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws
[14] Яремчук, К., Воскобойников, Д., & Мелкозьорова , О. (2022). Сучасні загрози та способи забезпечення безпеки веб-застосунків. *Комп'ютерні науки та кібербезпека,* (2), 28-34. https://periodicals.karazin.ua/cscs/article/view/21038/19744
[15] What is a Next-Generation Firewall (NGFW)? Вилучено з https://www.zenarmor.com/docs/network-security-tutorials/next-generation-firewall
[16] Top Next Next-Generation Firewall (NGFW) Software (2022). Вилучено з https://www.cioinsight.com/security/ngfw-software/#What-is-a-next-generation-firewall.

Надійшла: Жовтень 2023. **Прийнята**: Листопад 2023.

Автори:
Михайло Січкар, студент факультету комп'ютерних наук (бакалавріат), Харківський національний університет імені В.Н. Каразіна, Україна.
E-mail: sichkar2020kb13@student.karazin.ua

Лариса Павлова, ст. викладач кафедри іноземних мов професійного спрямування, факультет іноземних мов, Харківський національний університет імені В.Н. Каразіна, Україна.
ORCID ID https://orcid.org/0000-0002-5854-4209
E-mail: l.v.pavlova@karazin.ua

Бліц-огляд можливостей міжмережевих екранів покоління NG (*Next-Generation*).

Анотація. У рамках цієї роботи коротко розглядається історія, типи, можливості та переваги технології брандмауерів наступного покоління (*NGFW*). Брандмауери є важливим засобом захисту мережевих ресурсів від різноманітних загроз інформаційній безпеці. З розвитком технологій і зміною характеру атак, особливо тих, що включають штучний інтелект, брандмауери також еволюціонували, набуваючи нових функцій і можливостей. У межах цієї роботи представлений короткий огляд основних типів, можливостей та переваг технології брандмауерів наступного покоління *NGFW*, яка є сучасним рішенням для комплексного захисту мережі від складних і комплексних загроз безпеки. У статті, також, аналізуються особливості та відмінності *NGFW* від брандмауерів попередніх поколінь, а також приклади *NGFW* від відомих вендорів, які займають основну частину ринку, таких як *Palo Alto Networks, Fortinet* та *Cisco*. У статті висвітлено основні тенденції, перспективи розвитку та впровадження *NGFW*, зокрема вплив штучного інтелекту, машинного навчання, хмарних технологій та Інтернету речей, переваги та недоліки можливості, важливі аспекти, призначення та галузь використання. У роботі також йдеться про те, який значний слід залишить ця технологія у проблематиці мережевої безпеки. Підкреслено, що впровадження *NGFW* не підміняє собою інших технологій і інструментів безпеки, а лише ефективно розширює наявний арсенал протидії новим загрозам безпеки (насамперед як інструмент проактивної протидії та швидкого реагування на складні мережеві інциденти). Стаття може бути корисною для студентів, науковців та фахівців з інформаційної безпеки, які прагнуть розширити рівень своїх компетенцій, пов'язаних із розробкою сучасних технологій міжмережевого захисту та їх можливостей.

Ключові слова: *NGFW, брандмауер, інформаційна безпека, кібербезпека, зловмисне програмне забезпечення.*