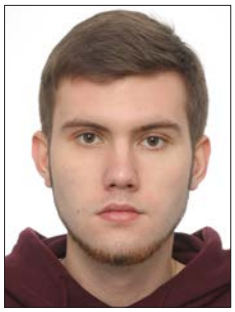

Maksym V. Kopytovskiy
Копитовський Максим Валерійович

Valerii H. Pavlov
Павлов Валерій Георгійович

УДК 656.61+004.7

HIGH-AVAILABILITY CLUSTER ON THE BASIS OF APPLICATIONS SERVERS "GLASSFISH"

ВІДМОВОСТІЙКИЙ КЛАСТЕР НА БАЗІ СЕРВЕРІВ ДОДАТКІВ "GLASSFISH"

DOI https://doi.org/10.15589/smi2019.1(11).13

Maksym V. Kopytovskiy Копитовський Максим Валерійович, магістр кафедри комп'ютеризованих систем захисту інформації
m.kopytovskiy@gmail.com
ORCID ID: 0000-0001-7502-1058

National Aviation University, Kyiv
Національний авіаційний університет, м. Київ

Valerii H. Pavlov Павлов Валерій Георгійович, канд. техн. наук, доц., доцент кафедри обчислювальної техніки
pavlovvg@ukr.net
ORCID ID: 0000-0002-4299-0319

National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ

Abstract. The development of maritime infrastructure is impossible without the use of powerful information and analytical systems like operation of logistics systems, risk management in maritime transport, the provision of crewing services, etc. In the first place, they become the targets of attacks, which result in the loss of access to information and stop the server applications. To solve this problem, it is necessary to analyze the possible threats to information in computer systems, and to determine ways to increase the high availability of the servers. *Purpose of the study:* The most useful information that is used on the Internet and uses server-based "Oracle Glassfish Open Server". *The research method* is preliminary theoretical analysis and subsequent practical implementation. *The object of the research* is the process of building a secure cluster system using modern technologies. *The subject* of the study is a clustered server system that provides resource allocation and enhanced security of information storage. Hardware and Software: "Oracle Glassfish", "NGINX". *The results obtained and their novelty.* A cluster system based on Oracle Glassfish Open Server. Work results. The analysis of the basic programs of threat information in computer systems, the solution of securely protected servers for use of the cluster system, the realization of the cluster system with 5 nodes and the load balancer based on NGINX, the detailed description of each server's configuration. *Usage Guidelines.* This system can be used in the largest companies, due to its security and system performance. *Estimated assumptions about the development of the object and object of the study* possible implementation of this system on a larger scale, the addition of various additional systems, such as cloud storage, to maintain the integrity and availability in the downfall of the network.

Key words: protected system, SSH, SSL, encryption, Glassfish Open Server, load balancing.

Анотація. Розвивати морську інфраструктуру неможливо без застосування потужних інформаційно-аналітичних систем, за допомогою яких здійснюється, зокрема, функціонування логістичних систем, управління ризиками на морському транспорті, надання крюїнгових послуг тощо. Саме вони стають об'єктами атак, внаслідок яких втрачається доступ до інформації та зупиняється робота серверних додатків. Для вирішення цієї проблеми потрібно здійснити аналіз можливих загроз інформації в комп'ютерних системах та визначити шляхи підвищення відмовостійкості серверів. *Мета дослідження* – підвищення ефективності захисту інформаційно-комунікаційної мережі на базі серверів додатків зі застосуванням "Oracle Glassfish Open Server". *Методика дослідження* – попередній теоретичний аналіз та наступна практична реалізація. *Об'єктом дослідження* є процес побудови захищеної кластерної системи зі застосуванням сучасних технологій. *Предмет дослідження* – кластерна серверна система, яка забезпечує розподіл ресурсів та завдяки цьому має підвищену надійність зберігання інформації та захищеність. Використано такі технічні та програмні засоби: "Oracle Glassfish", "NGINX". *Отримані результати та їх новизна.* Ми отримали кластерну систему на базі "Oracle Glassfish Open Server". Значущість

виконаної роботи та висновки. Проаналізовано основні загрози інформації в комп'ютерних системах, розглянуто шляхи підвищення рівня захищеності серверів через застосування кластерної системи, на практиці реалізовано відмовостійку систему з кластеру із 5-ти вузлів та з балансуванням навантаження на базі "NGINX", здійснено докладний опис конфігурації кожного з серверів, що використовується в системі. *Рекомендації щодо використання результатів.* Інформація щодо налаштування кластерної системи на базі "Oracle Glassfish" може бути корисна для застосування фахівцям з інформаційних технологій. *Галузь застосування та ступінь впровадження матеріалів досліджень.* Наше дослідження може впроваджуватися на підприємствах морського транспорту або будь-якої іншої сфери, де є необхідність в безперервній роботі системи. *Прогнозовані припущення про розвиток об'єкта та предмета дослідження.* Можлива реалізація даної системи у більш масштабних мірах, додавання таких додаткових систем, як хмарне сховище, для збереження цілісності та доступності при падінні даної мережі.

Ключові слова: захищена система, SSH, SSL, шифрування, "Glassfish Open Server", балансувальник навантаження.

References

[1] Maritime Information Infrastructure. A Key Component of the U.S. 21st Century Freight Movement Network. Retrieved from http://aapa.files.cms-plus.com/PDFs/PolicyPositions/Maritime Information Infrastructure.pdf.

[2] What are Denial of Service (DoS) attacks? DoS attacks explained. Retrieved from https://us.norton.com/internet-security-emerging-threats-dos-attacks-explained.html.

[3] DDoS Attacks. Retrieved from https://www.imperva.com/learn/application-security/ddos-attacks/.

[4] Saltzer H., Schroeder D. The Protection of Information in Computer Systems. IEEE, 1975. Vol. 63, no. 09 (September). P. 1278-1308. ISSN: 1558–2256.

[5] ISO/IEC 27000:2018. Information technology. Security techniques. Information security management systems. Overview and vocabulary. Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=2ahUKEwj2wtLnpZzlAhUjAxAIHdyrDqsQFjADegQIBxAC&url=https%3A%2F%2Fwww.sis.se%2Fapi%2Fdocument%2Fpreview%2F80001198%2F&usg=AOvVaw1tWFIo1ZigiLm_eqAC3K4D.

[6] Prince Matthew. The DDoS That Almost Broke the Internet. 2013. Retrieved from: https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet.

[7] Q2 2018 DDoS Trends report: 52 percent of attacks employed multiple attack types. Retrieved from: https://blog.verisign.com/security/ddos-protection/q2-2018-ddos-trends-report-52-percent-of-attacks-employed-multiple-attack-types.

[8] Network attacks. Retrieved from https://www.geeksforgeeks.org/basic-network-attacks-in-computer-network/.

[9] Qijun Gu, Peng Liu. Denial of Service Attacks. University Park. 2004. Retrieved from: s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf.

[10] How to Defend Against DDoS Attacks: Six Steps. Retrieved from: https://www.a10networks.com/blog/how-defend-against-ddos-attacks-six-steps.

[11] General information about cybersecurity and network security. Retrieved from: https://www.technewsworld.com/perl/section/cyber-security/.

[12] Deep cybersecurity digest. Retrieved from: https://proglib.io/p/security-digest/.

[13] Dokumentatsiya po Ubuntu [Ubuntu documentation] Retrieved from http://help.ubuntu.ru/.

[14] Dokumentatsiya po nalashtuvannyu Oracle Glassfish Open Server [Oracle Glassfish Open Server Configuration Documentation]. Retrieved from http://www.oracle.com/technetwork/middleware/glassfish/overview/index.html.

[15] Nalashtuvannya Oracle Glassfish Open Server pid operatsiynoyu systemoyu Ubuntu [Oracle Glassfish Open Server setup under Ubuntu operating system]. Retrieved from

https://community.vscale.io/hc/ru/community/posts/208345489-Установка-и-настройка-GlassFish4-на-Ubuntu-16-04.

[16] Basic Oracle Glassfish Open Server configuration. Retrieved from http://148.211.145.149:8090/docs/quickstart.html.

[17] Nalashtuvannya vidmovostiykoho klasteru na bazi Oracle Glassfish Open Server [Configure Oracle Glassfish Open Server High Availability Cluster]. Retrieved from https://javaee.github.io/glassfish/doc/4.0/ha-administration-guide.pdf.

[18] Posibnyk po nalashtuvannyu NGINX [NGINX Configuration tutorial]. Retrieved from

https://www.nginx.com/resources/wiki/.

[19] What is NGINX? Retrieved from https://kinsta.com/knowledgebase/what-is-nginx/.

[20] NGINX Advanced configuration. Retrieved from https://devdocs.io/nginx/.

Постановка проблеми. Вирішення задач транспортних перевезень вимагає застосування потужних інформаційних ресурсів, які повинні задовольняти вимоги доступності, достовірності та своєчасності отримання необхідної інформації [1]. Це накладає додаткові вимоги на безпеку комп'ютерних систем. З огляду на складність та високу вартість більшості процесів і методів захисту цифрового обладнання, інформації та комп'ютерних систем від ненавмисного чи несанкціонованого доступу вразливість комп'ютерних систем становить значну проблему для користувачів. Для цього потрібно здійснити аналіз можливих загроз інформації в комп'ютерних системах та підвищити відмовостійкість серверів.

Зокрема, ідеться про усім відомі різновиди атак типу «відмова в обслуговуванні» [2]. Подібна загроза особливо небезпечна в ситуаціях, коли затримка з наданням ресурсів мережі абоненту може призвести до тяжких для нього наслідків. Наприклад, відсутність у абонента даних, необхідних для прийняття рішень, може бути причиною його нераціональних або неоптимальних дій.

Крім того, останні тенденції вказують на появу нових типів атак – прихованих атак [3]. У такому разі підконтрольні атакуючому комп'ютери отримують доступ до цільового сервісу на цілком законних підставах (наприклад, відвідують вебсайт компанії) і завантажують канал ресурсоємними операціями (атака погіршення якості) або в певний момент «вибухають» беззмістовним трафіком, що ставить перед системами захисту нові нетривіальні задачі виявлення і протидії.

Аналіз останніх досліджень і публікацій. Відомо, що головними завданнями інформаційної безпеки є забезпечення конфіденційності, доступності і цілісності інформації, а також захищеності інформації від несанкціонованого доступу [4; 5]. Зазначені вище атаки впливають на доступність інформаційних ресурсів, тобто на можливість отримати необхідну інформацію у будь-який час з максимальною швидкістю [6]. Сьогодні доводиться констатувати, що надійного комплексного засобу протидії цим атакам немає, бо найчастіше вони мають комбінований характер [7].

Існують численні публікації на цю тему, у яких пропонується розглядати три основні типи атак [8]:

– атаки на рівні мережних каналів;
– атаки на рівні мережних додатків;
– атаки на рівні мережних сервісів.

Останні види атак пов'язані з WEB, PROXY, SSL, DNS та іншими серверами, до яких можливий доступ ззовні мережі [9]. Зазвичай надаються рекомендації щодо контролю над запитами, що здійснюють користувачі, а також щодо фільтрації трафіку тощо [10]. Але жодне наявне на цей момент обладнання не забезпечує 100% захист [11].

Водночас з'являються численні пропозиції, що надходять від таких потужних компаній, як "Google", "Xelent", "Yandex", щодо використання їхніх хмарних ресурсів для розміщення та резервування інформації. Однак ці storage-рішення не вирішують проблему. Наприклад, атака, яка була здійснена у 2017 році на хмарну інфраструктуру компанії "Kaye Financial Corporation", згідно з даними звіту "Check Point Research" за 2017 рік нанесла збитків більше 2 млн доларів США [12].

Виокремлення не вирішених раніше частин загальної проблеми. Як одне з можливих рішень пропонується підвищити рівень безпеки у інформаційно-комунікаційній мережі шляхом побудови відмовостійкого кластеру. Потрібний ефект досягається завдяки автоматичному перезапуску додатку на будь-якому іншому вузлі кластеру, якщо певний вузол внаслідок апаратного або програмного збою чи атаки стає непрацездатним. У такий спосіб доступність інформаційних ресурсів забезпечується завдяки апаратній надлишковості та резервуванню.

Мета дослідження. Метою даної роботи є підвищення ефективності захисту інформаційно-комунікаційної мережі на базі серверів додатків зі застосуванням "Oracle Glassfish Open Server".

Методи, об'єкт та предмет дослідження. Метод дослідження – попередній теоретичний аналіз та наступна практична реалізація.

Об'єктом дослідження є процес побудови захищеної кластерної системи зі застосуванням сучасних технологій.

Предмет дослідження – кластерна серверна система, яка забезпечує розподіл ресурсів та завдяки цьому має підвищену надійність зберігання інформації та захищеність.

Основний матеріал. Як відомо, переваги кластеру визначаються високою продуктивністю обчислень, а також стійкістю до апаратних або програмних відмов. Завдяки цьому кластерна серверна система стає привабливим рішенням, яке забезпечує більш високий рівень захисту за рахунок резервування та розподілення інформації. Оскільки основним програмним рішенням зі створення професійної розподіленої бази даних вважається "Oracle Parallel Server", то для розгортання серверів додатків було запропоновано використати "Oracle GlassFish Server" тієї ж компанії-розробника.

"GlassFish" – сервер додатків з відкритим вихідним кодом, який реалізує специфікації "Java EE", спочатку розроблений у "Sun Microsystems". Нині він спонсорується корпорацією "Oracle". В основу "GlassFish" лягли частини коду "Java System Application Server" компанії "Sun" і "ORM TopLink" (рішення для зберігання джава-об'єктів в реляційних БД було надане "Oracle"). Як сервлет-контейнер в ньому використовується модифікований "Apache Tomcat", доповнений компонентом "Grizzly", що використовує технологію "Java NIO".

Крім зрозумілих переваг, які мають програмні продукти, що розповсюджуються за безкоштовною ліцензією (CDDL), "GlassFish" має ще такі доповнення:

– найбільш повну підтримку специфікації "Java EE", що забезпечує використання найбільш сучасних її версій;

– еталонну реалізацію специфікації "Java EE", оскільки має того ж розробника;

– можливість використання як засобу пошуку помилок у інших серверах додатків;

– підтримку серверу "GlassFish" усіма основними середовищами розробки на "Java", такими як "Netbeans", "IDEA" та "Eclipse";

Розглянемо основні етапи побудови та налагоджування відмовостійкого кластеру такої структури:

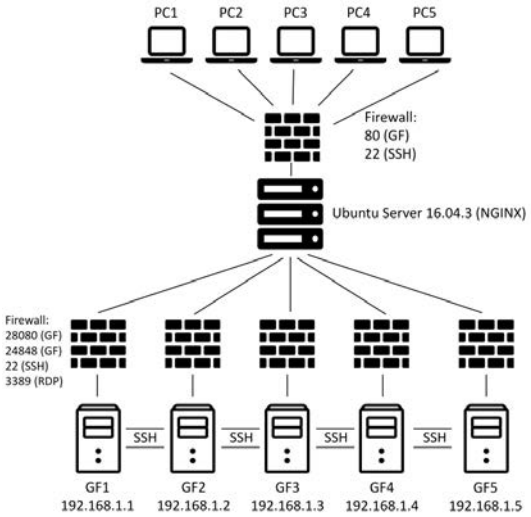

Рис. 1. Схема кластеру

Дана система складається із 5-ти серверів GF1 – GF5 ("Glassfish 4.0"), одного серверу з балансуванням навантаження ("Ubuntu Server" – "NGINX") [13] та 5-ти клієнтів (PC1 – PC5).

Для створення кластеру та розгортання програмного забезпечення використовувалися комп'ютери з такими характеристиками:

GF1 – GF5 ("Glassfish 4.0")
Процесор AMD A8-3870K
Оперативна пам'ять 4xKingston DDR3-1866 8192MB
Операційна система Windows Server 2012 R2
"Ubuntu Server" ("NGINX")
Процесор AMD A8-3870K
Оперативна пам'ять 1xKingston DDR3-1866 4096MB
Операційна система Ubuntu Server 18.04.2

Налаштування "Oracle Glassfish 4.0" [14]

Після встановлення "Oracle Glassfish 4.0" необхідно відкрити командну строчку, перейти до папки **…\glassfish\bin** та виконати таку команду:

asadmin start-domain domain1.

Наступним кроком виконуємо таку команду:

asadmin change-admin-password,

тим самим встановлюємо пароль на користувача ***admin***. Після вводу команди треба ввести ім'я користувача ("admin"), після чого замість порожнього старого пароля вводимо новий. Після встановлення пароля вводимо таке:

asadmin enable-secure-admin.

При запиті пароля вводимо той, що нещодавно встановили [15].

Перезапускаємо сервер **GF1** за допомогою команди asadmin restart-domain domain1.

Аналогічні дії виконуємо на інших серверах (GF2 – GF5).

На серверах "Windows" **GF1 – GF5** у файлі ***hosts***, що знаходиться у **C:\Windows\System32\drivers\etc**, дописуємо такі параметри:

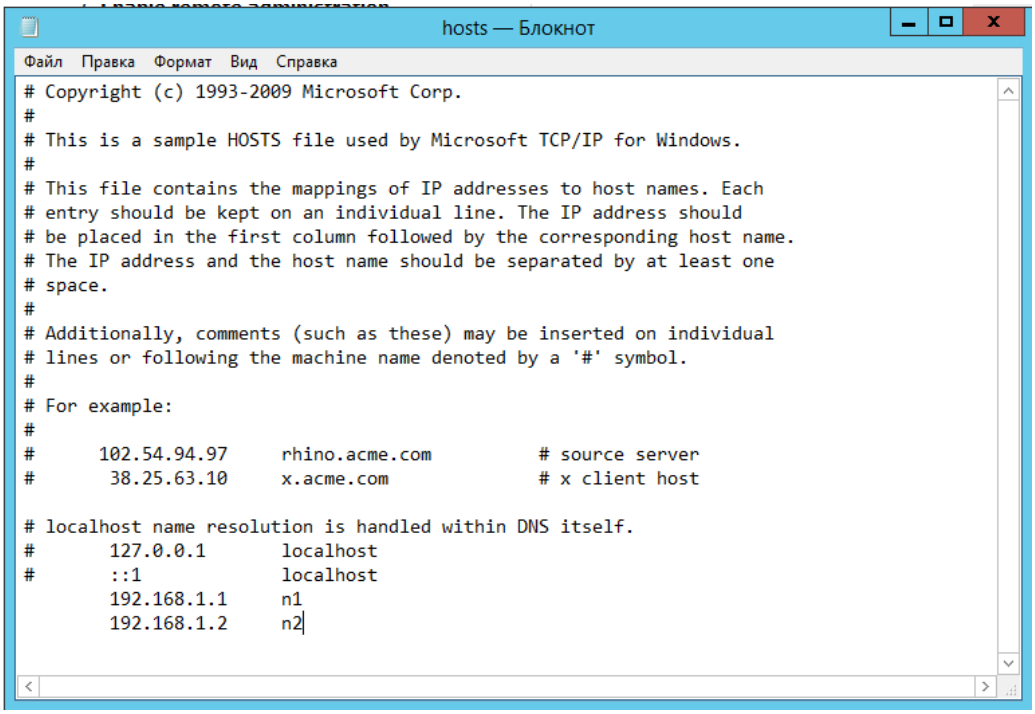

Рис. 2. Налаштування файлу *hosts* на "Windows Server"

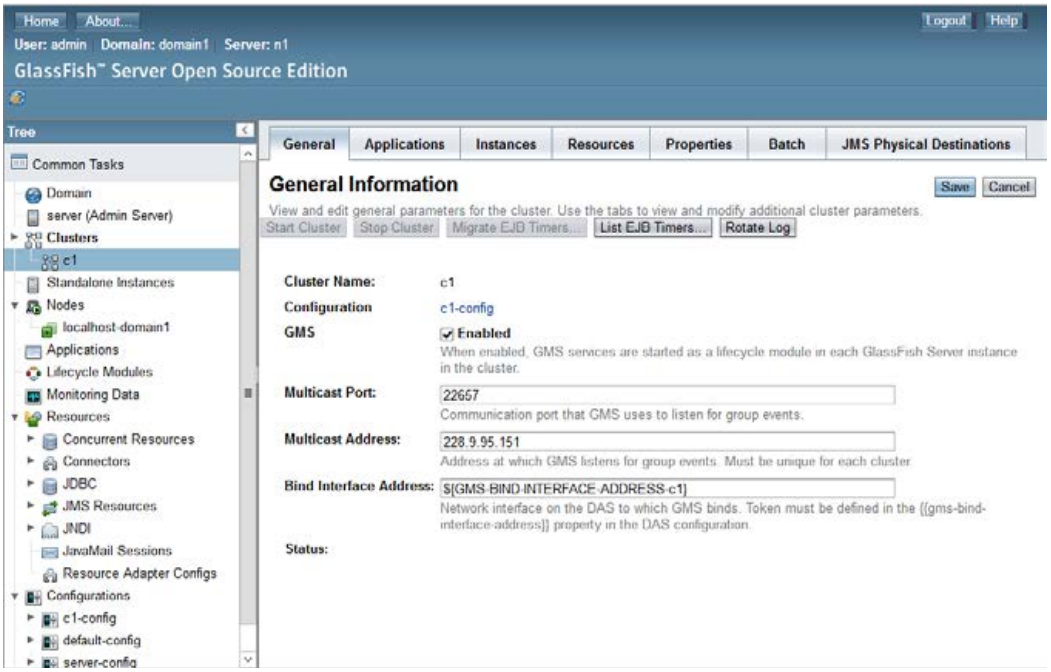

Рис. 3. Створення кластеру та його налаштування

<ip-адреса першого сервера (GF1)> n1
<ip-адреса другого сервера (GF2)> n2
<ip-адреса п'ятого сервера (GF5)> n5.

На інших серверах (GF2 – GF5) виконуємо команду asadmin --host n1 --port 4848 list-instances.

Після вводу команди побачимо запит на довіру сертифікату, на який відповідаємо ствердно "**Y**" в полі відповіді. Потім вводимо ім'я та пароль вашого користувача (**"admin"**). Якщо усе виконано правильно, то у відповідь ми отримаємо таке: "***Nothing to list. Command list-instances executed successfully***".

Переходимо за адресою http://n1:4848/ та авторизуємося. Створюємо кластер з ім'ям "**c1**". У самому кластері створюємо з'єднання з іменем "**i1**", яке вузол "**localhost-domain1**".

На інших серверах (GF2 – GF5) прописуємо таку команду:

asadmin --host n1 --port 4848 create-local-instance --cluster c1 i1.

Якщо все було виконано правильно, то побачимо повідомлення: "**Command create-local-instance executed successfully"**. Після цього ми на першому сервері (GF1) створюємо SSH-сервер за допомогою додатка "Cygwin" та під'єднуємо сервери GF2 – GF5 за допомогою SSH до першого сервера. Зберігаємо налаштування на натискаємо «старт» біля кожного вузла кластеру [16; 17]. Налаштування кластеру завершено.

Обговорення отриманих результатів. У ході роботи були повністю виконані налаштування системи. Ми побудували кластер та додали балансувальника навантаження для більш стабільного з'єднання з серверами для клієнтів [18; 19; 20].

Дана відмовостійка кластерна система може використовуватися у більшості компаній, у яких віддається перевага захищеності.

ВИСНОВКИ. 1. Проаналізовано основні загрози інформації в комп'ютерних системах.

2. Розглянуто шляхи підвищення рівня захищеності серверів завдяки застосуванню кластерної системи.

3. На практиці реалізована відмовостійка система з кластеру із 5-ти вузлів та із балансуванням навантаження на базі "NGINX".

4. Здійснено докладний опис конфігурації кожного сервера, що використовується в системі.

Список літератури:

[1] Maritime Information Infrastructure. A Key Component of the U.S. 21st Century Freight Movement Network. URL: http://aapa.files.cms-plus.com/PDFs/PolicyPositions/Maritime Information Infrastructure.pdf.

[2] What are Denial of Service (DoS) attacks? DoS attacks explained. URL: https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html

[3] DDoS Attacks. URL: https://www.imperva.com/learn/application-security/ddos-attacks/.

[4] Saltzer H., Schroeder D. The Protection of Information in Computer Systems. *IEEE*, 1975. Vol. 63, no. 09 (September). P. 1278–1308. ISSN: 1558–2256.

[5] ISO/IEC 27000:2018. Information technology. Security techniques. Information security management systems. Overview and vocabulary. URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja

&uact=8&ved=2ahUKEwj2wtLnpZzlAhUjAxAIHdyrDqsQFjADegQIBxAC&url=https%3A%2F%2Fwww.sis.se%2Fapi%2Fdocument%2Fpreview%2F80001198%2F&usg=AOvVaw1tWFIo1ZigiLm_eqAC3K4D.

[6] Prince Matthew. The DDoS That Almost Broke the Internet. 2013. URL: https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet.

[7] Q2 2018 DDoS Trends report: 52 percent of attacks employed multiple attack types. URL: https://blog.verisign.com/security/ddos-protection/q2-2018-ddos-trends-report-52-percent-of-attacks-employed-multiple-attack-types.

[8] Network attacks. URL: https://www.geeksforgeeks.org/basic-network-attacks-in-computer-network/.

[9] Qijun Gu, Peng Liu. Denial of Service Attacks. University Park. 2004. URL: s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf.

[10] How to Defend Against DDoS Attacks: Six Steps. URL: https://www.a10networks.com/blog/how-defend-against-ddos-attacks-six-steps.

[11] General information about cybersecurity and network security. URL: https://www.technewsworld.com/perl/section/cyber-security/.

[12] Deep cybersecurity digest. URL: https://proglib.io/p/security-digest/.

[13] Документація по Ubuntu. URL: http://help.ubuntu.ru/.

[14] Документація по налаштуванню Oracle Glassfish Open Server. URL: http://www.oracle.com/technetwork/middleware/glassfish/overview/index.html.

[15] Налаштування Oracle Glassfish Open Server під операційною системою Ubuntu. URL:

https://community.vscale.io/hc/ru/community/posts/208345489-Установка-и-настройка-GlassFish4-на-Ubuntu-16-04.

[16] Basic Oracle Glassfish Open Server configuration. URL: http://148.211.145.149:8090/docs/quickstart.html.

[17] Налаштування відмовостійкого кластеру на базі Oracle Glassfish Open Server. URL: https://javaee.github.io/glassfish/doc/4.0/ha-administration-guide.pdf.

[18] Посібник з налаштування NGINX. URL: https://www.nginx.com/resources/wiki/.

[19] What is NGINX? URL: https://kinsta.com/knowledgebase/what-is-nginx/.

[20] NGINX Advanced configuration. URL: https://devdocs.io/nginx/.