КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.703
УДК 004.021

Цехмейстер Ростислав Денисович
студент Факультету інформаційних технологій та математики
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0009-0001-6269-0321
rdtsekhmeister.fitm23m@kubg.edu.ua

Платоненко Артем Вадимович
кандидат технічних наук, доцент
доцент кафедри інформаційної та кібернетичної
безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-2962-5667
a.platonenko@kubg.edu.ua

Ворохоб Максим Віталійович
PhD in Cybersecurity
старший викладач кафедри інформаційної та кібернетичної
безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0001-5160-7134
m.vorokhob@kubg.edu.ua

Черевик В'ячеслав Михайлович
кандидат технічних наук, доцент
доцент кафедри інформаційної та кібернетичної
безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-2735-5341
v.cherevyk@kubg.edu.ua

Семеняка Світлана Олексіївна
кандидат фізико-математичних наук, доцент
завідувач кафедри математики і фізики
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0001-5083-1433
s.semeniaka@kubg.edu.ua

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ВІРТУАЛЬНОМУ СЕРЕДОВИЩІ

Анотація. В сучасному світі розвитку технологій та залежності від них, на жаль, більшість IT-активів компаній залишаються вразливими, через поєднання технічних і організаційних факторів, таких як застарілі технології, помилки конфігурації та людський фактор. Дані слабкі місця стають основними точками входу для кіберзагроз, що дозволяють зловмисникам отримувати несанкціонований доступ до даних, порушувати роботу сервісів або запускати масштабні атаки. Відсутність системного підходу до забезпечення безпеки значно підвищує ризики втрати критичної інформації та простоїв у роботі. Аналіз існуючих загроз, таких як DDoS-атаки, витоки даних і компрометація гіпервізора, засвідчує необхідність комплексного, багаторівневого підходу до захисту. Використання фаєрволів, систем виявлення та запобігання вторгненням (IDS/IPS), SIEM-рішень, а також платформ моніторингу дозволяє ефективно контролювати трафік, виявляти аномалії та оперативно реагувати на інциденти. У даній статті розглядаються питання забезпечення інформаційної безпеки у віртуалізованих середовищах із використанням систем захисту мережі, виявлення вторгнень, проксі-сервера, моніторингу безпеки та контролю інфраструктури. Також зосереджено увагу на вразливостях інформаційних систем, пов'язаних із використанням застарілих технологій, недостатньою

сегментацією мереж, а також помилками в конфігурації безпекових рішень. Комплексне застосування сучасних технологій безпеки та гнучкі архітектурні підходи формують надійне підґрунтя для подальшого удосконалення систем захисту інформаційних ресурсів у віртуалізованих середовищах. Запропоновано багаторівневу архітектуру захисту, яка інтегрує сучасні системи та базується на концепціях Zero Trust, мікросегментації та багаторівневого захисту (Defense in Depth). Проведені тестування підтвердили ефективність впроваджених заходів безпеки для розробленої системи, результати яких підтвердили ефективність у виявленні та запобіганні сучасним кіберзагрозам, забезпечуючи надійний захист критичних інформаційних ресурсів у динамічному середовищі.

Ключові слова: інформаційна безпека; віртуалізовані середовища; системи захисту мережі; виявлення вторгнень; проксі-сервер; моніторинг безпеки; контроль інфраструктури; zero trust; мікросегментація.

ВСТУП

Сучасний розвиток інформаційних технологій супроводжується зростанням кількості кіберзагроз [1], [3], що стає суттєвим викликом для захисту критичних систем. За інформацією, наданою Державною службою спецзв'язку України [4], за останні півроку в Україні спостерігається зменшення кількості інцидентів високого та критичного рівня завдяки впровадженню сучасних технологій кіберзахисту, зменшенню поверхні атаки та активній співпраці з вендорами й міжнародними партнерами. Ці досягнення демонструють ефективність комплексного підходу до забезпечення безпеки, однак залишаються питання, які потребують уваги.

Постановка проблеми. РНБО [5] ділиться інформацією, що попри інновації в галузі, такі як штучний інтелект та квантові технології, однією з ключових проблем залишається використання застарілих систем у державному та приватному секторах. Як зазначає корпорація MITRE, функціонування таких систем, зокрема тих, яким понад 60 років, створює довгострокові ризики.

Аналіз останніх досліджень і публікацій. Основна проблема пов'язана не лише з технічними вразливостями, а й із дефіцитом кваліфікованих фахівців для їх обслуговування. Аналогічну проблему окреслюють експерти SANS Institute, які включають застарілі технології до п'ятірки найбільших загроз кібербезпеці. Ці виклики актуалізують необхідність створення нових підходів до побудови захищених інформаційних систем. На відміну від загальних підходів, у даній роботі запропоновано вирішення проблем через розробку багаторівневої системи інформаційної безпеки для віртуалізованих середовищ, що базується на сучасних принципах захисту, таких як Zero Trust, мікросегментація та багаторівневий захист (Defense in Depth).

Мета статті. Метою цієї роботи є дослідження, впровадження та розробка рекомендацій для забезпечення інформаційної безпеки у віртуалізованих середовищах, зокрема шляхом інтеграції систем виявлення загроз, моніторингу та запобігання атакам.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Методи дослідження. Для дослідження було розроблено та інтегровано систему інформаційної безпеки з метою захисту віртуалізованих середовищ, таких як платформи на базі ESXi та контейнеризація Kubernetes.

На основі принципів захисту, таких як Zero Trust [2], [8], [9], мікросегментація [6] та багаторівневий захист (Defense in Depth), було змодельовано архітектуру захищеної

інфраструктури, яка включає різні сегменти мережі та політики доступу. Віртуальне середовище було побудоване із застосуванням технологій, що забезпечують ізоляцію та контроль трафіку, що дало змогу відтворити реалістичні умови роботи корпоративної мережі.

Для створення комплексної системи інформаційної безпеки [1], [11], [12] було інтегровано ключові інструменти, зокрема маршрутизатор із функціями файрволу PfSense, систему виявлення та запобігання вторгнень (IDS/IPS) Snort, проксі-сервер Squid, платформу SIEM Wazuh та систему моніторингу мережі Zabbix [3]. Інтеграція цих рішень забезпечила синергію захисту на різних рівнях мережевої інфраструктури.

МЕТОДИКА ДОСЛІДЖЕННЯ

Було проведено експерименти у лабораторному віртуальному середовищі, спрямовані на тестування розробленої системи безпеки. Випробування включали сканування вразливостей, перевірку проникливості, симуляцію атак, зокрема DoS, та моніторинг подій у реальному часі. Результати експериментів дали змогу оцінити ефективність захисних механізмів у виявленні та запобіганні кіберзагрозам.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

В рамках дослідження було розроблено та інтегровано багаторівневу систему інформаційної безпеки. Проведені тестування підтвердили результативність запропонованого підходу до захисту інформаційної інфраструктури [12], [13].

Кожен компонент виконує специфічні функції, що доповнюють один одного, забезпечуючи синергію між окремими інструментами.

PfSense виступає центральним елементом управління мережевим трафіком і доступом, реалізуючи політику фільтрації трафіку та маршрутизації між сегментами мережі. Він також забезпечує безпечний периметр, обмежуючи доступ до ресурсів ззовні. Інтеграція Snort у PfSense підвищила функціональність фаєрволу за рахунок глибокого аналізу мережевого трафіку та виявлення вторгнень.

Як вказано у [7], Snort здійснює аналіз пакетів у реальному часі, порівнюючи їх зі своєю базою сигнатур для ідентифікації підозрілої активності.

Squid як проксі-сервер і кешуючий механізм зменшує навантаження на зовнішні канали зв’язку, покращує швидкість доступу до ресурсів і водночас забезпечує фільтрацію небажаного контенту. Його інтеграція дозволила посилити контроль мережевого трафіку.

SIEM-платформа Wazuh стала основним інструментом для аналізу подій безпеки, централізованого збору логів та оцінки стану систем.

Zabbix забезпечив моніторинг усіх компонентів інфраструктури, включаючи сервери, мережеві пристрої та сервіси безпеки. Він відстежує продуктивність системи в реальному часі, сигналізуючи про будь-які збої або перевищення критичних параметрів.

Інтеграція цих інструментів дозволила реалізувати комплексний підхід до безпеки, який охоплює виявлення загроз, запобігання їм, моніторинг і аналіз у реальному часі. Завдяки чітко визначеним ролям кожного компонента вдалося створити взаємо доповнювану систему, яка забезпечує високу стійкість до сучасних кіберзагроз.

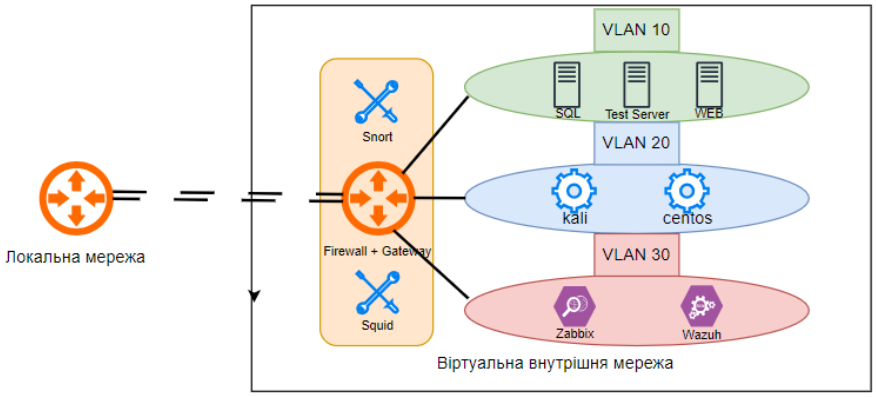

Рис. 1. Архітектура захищеної віртуальної інфраструктури

Реалізація концепцій Zero Trust та мікросегментації

Сегментація мережі за допомогою VLAN та політик доступу стала ключовим елементом у реалізації концепцій Zero Trust та мікросегментації [14], [15].

Було створено три окремі підмережі: VLAN 10 для серверів, VLAN 20 для машин тестування, та VLAN 30 для моніторингових систем.

Кожна VLAN мала чітко визначені функції та налаштовані політики безпеки, що забезпечило ізоляцію між сегментами мережі та мінімізувало поверхню атаки.

Кожна підмережа отримала набір дозволених портів, що відповідають лише тим сервісам, які необхідні для виконання її функцій.

Наприклад, VLAN 10 для серверів використовувала підмережу 10.114.10.0/24, з обмеженням доступу до портів 80, 443, 3306, 1514, 1515 та інших, необхідних для базової взаємодії.

У VLAN 20 для машин тестування дозволені порти були обмежені до мінімально необхідних (80, 443, 3306), щоб зменшити можливості потенційного зловмисника для несанкціонованого доступу.

VLAN 30, призначена для моніторингових систем, підтримувала підмережу 10.114.30.0/24 з портами, необхідними для роботи інструментів моніторингу та аналізу, таких як Zabbix і Wazuh.

Таблиця 1

Налаштування VLAN-підмереж

VLAN	Назва	Підмережа	Дозволені порти
10	Сервери	10.114.10.0/24	80, 3306, 443, 1514, 1515, 514, 67, 10050, 10051, 53
20	Машини тестування	10.114.20.0/24	80, 443, 3306, 53, 67
30	Моніторингові системи	10.114.30.0/24	1514, 1515, 514, 10050, 10051, 53, 67, 80, 443

Механізми мікросегментації дозволили розділити інфраструктуру на ізольовані сегменти з жорсткими політиками доступу, які контролюються файрволом PfSense. Цей підхід унеможливив переміщення зловмисників між сегментами мережі навіть у випадку компрометації одного з компонентів. Використання VLAN і політик мінімізації доступу значно ускладнило реалізацію мережевих атак.

Тестування вразливостей та запобігання атакам

Основні методи включали сканування вразливостей із використанням Nmap та імітацію атак, таких як DoS. На початковому етапі тестування за допомогою Nmap було виконано сканування серверів до налаштування файрволу PfSense. Результати показали,

ISSN 2663 - 4023

що всі порти серверів були відкриті, що значно підвищувало ризик атак. Зловмисники могли використовувати ці порти для експлуатації вразливостей у програмному забезпеченні серверів, отримуючи несанкціонований доступ. Така ситуація є типовою для систем без попередньо налаштованих заходів безпеки.

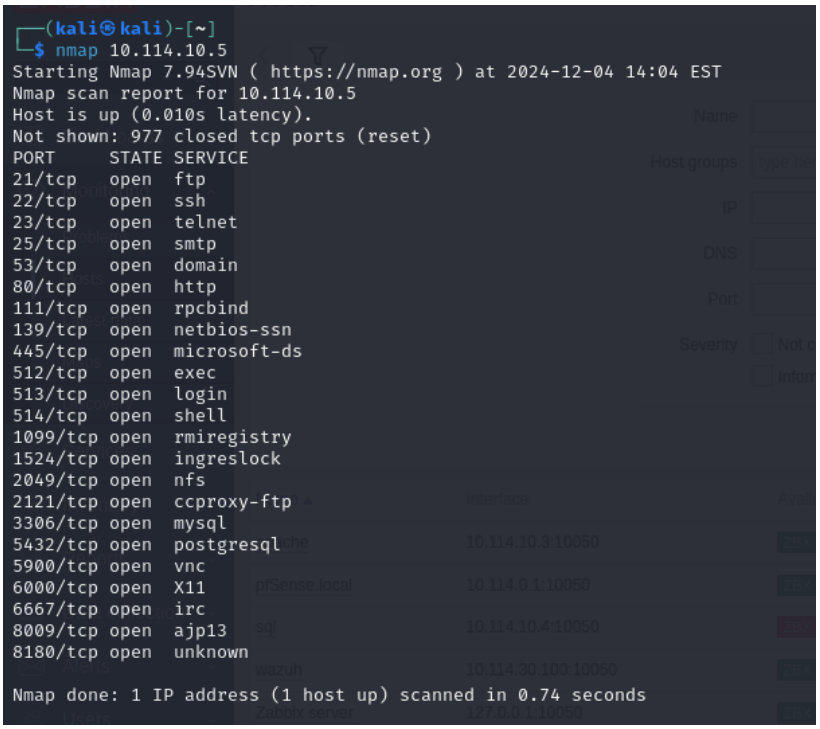

Рис. 2. Сканування тестового серверу до налаштування брандмауеру

Після налаштування файрволу PfSense повторне сканування виявило, що кількість відкритих портів суттєво зменшилася. У конфігурації файрволу було дозволено лише ті порти, які необхідні для роботи основних сервісів, наприклад, порт 80 для HTTP або 443 для HTTPS. Це дозволило значно знизити поверхню атаки, обмежуючи можливості для проникнення зловмисників.

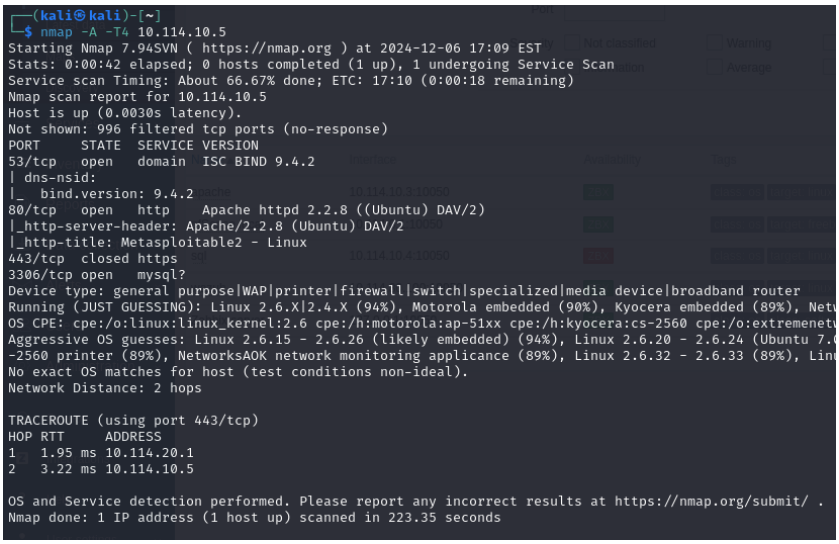

Рис. 3. Сканування тестового сервера після налаштування брандмауера

Для перевірки стійкості системи було виконано імітацію DoS-атаки [10] з використанням Kali Linux. Імітація атаки тривала кілька секунд, після чого Snort, інтегрований із PfSense, ідентифікував аномальну активність і автоматично заблокував IP-адресу зловмисника. Таким чином, будь-яка подальша комунікація з атакуючого пристрою була неможливою, що підтвердило ефективність реалізованих заходів реагування.

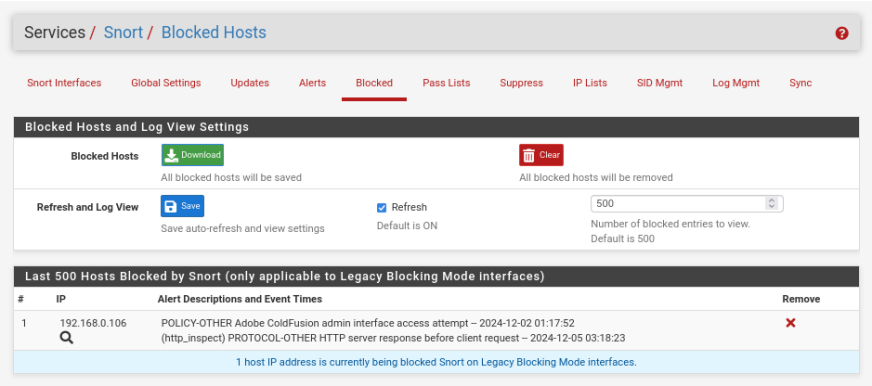

Рис. 4. Автоматичне внесення IP адреси тестувальника в список заблокованих пристроїв за допомогою сигнатур (rulesets) IDS/IPS Snort

Додатково було перевірено, як система справляється із запобіганням руху зловмисника в мережі. Завдяки сегментації VLAN і політикам доступу спроби проникнення з однієї підмережі в іншу були заблоковані на рівні файрволу PfSense, що підтвердило надійність реалізованих механізмів ізоляції.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Запровадження ефективних методик для захисту IT-систем є одним із ключових завдань, оскільки безпека інформації стала фундаментальним аспектом діяльності будь-якої організації. Швидка інтеграція нових технологій та сервісів часто здійснюється на шкоду їхній безпеці.

У гонитві за конкурентними перевагами компанії нерідко нехтують критично важливими етапами перевірки захищеності інфраструктури, що створює серйозні ризики. Основна проблема полягає у відсутності системного підходу до безпеки.

Наприклад, впровадження сервісів без попереднього тестування на вразливості або недотримання принципів, таких як Zero Trust і мікросегментація, може призвести до витоків даних, компрометації систем та поширення загроз у внутрішній мережі. Зловмисники, використовуючи вразливості в таких сервісах, отримують можливість проникати в критичні системи, викрадати конфіденційну інформацію або завдавати фінансових збитків.

Наслідки нехтування безпекою виходять за рамки втрат бюджету. Вони включають втрату репутації, зменшення довіри з боку клієнтів та партнерів, а також потенційні юридичні наслідки. Особливо це стосується компаній, які працюють із чутливими даними, такими як фінансові установи або медичні організації.

Щоб мінімізувати ці ризики, організації повинні впроваджувати стандартизовані методики забезпечення безпеки. Лише системний та проактивний підхід дозволяє забезпечити стабільну роботу сервісів і захистити IT-системи від загроз, що постійно еволюціонують.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Захист інформації. Технічний захист інформації. Основні положення.* (ДСТУ 3396.0-96). (б. д.). Державна служба спеціального зв'язку та захисту інформації України.
2. *Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою.* (ДСТУ ISO/IEC 27001:2023). (б. д.). ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ»).
3. *Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки хмарних послуг, що ґрунтуються на ISO/IEC 27002.* (ДСТУ ISO/IEC 27017:2016). (б. д.). Технічний комітет стандартизації «Інформаційні технології» (ТК 20).
4. *Cyber operations by russia: new goals, tools and groups. Analytics on the hacker attacks against Ukraine in H1 2024.* (2024). State Service of Special Communications and Information Protection of Ukraine. https://cip.gov.ua/en/news/cyber-operations-rf-h1-2024-report
5. *National Security and Defense Council of Ukraine. Major international and Ukrainian cybersecurity news in September 2024.* (2024). https://www.rnbo.gov.ua/en/Diialnist/7027.html
6. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access, 10,* 57144–57145. https://doi.org/10.1109/ACCESS.2022.3174679
7. Mukhopadhyay, M., Chakraborty, S., Chakrabarti. A. (2022). Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems. *Journal of Information Security, 2(1),* 28–38. https://doi.org/10.4236/jis.2011.21003
8. Ghasemshirazi, S., Shirvani, G., Alipour, M. (2022). Zero Trust: Applications, Challenges, and Opportunities. *Graduate University of Advanced Technology,* 16–17. https://doi.org/10.48550/arXiv.2309.03582
9. Campbell, M. (2020). Beyond Zero Trust: Trust Is a Vulnerability. *Computer, 53(10),* 110–113. https://doi.org/10.1109/MC.2020.3011081
10. Buqing, W. (2023). Analysis of a new firewall constructed on Pfsense with Snort to defend against common internet intrusions. *Applied and Computational Engineering, 43,* 244–250. https://doi.org/10.54254/2755-2721/43/20230841
11. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise.* Textbook. Lviv: Publisher Marchenko T. V.
12. Skladannyi, P., et al. (2023). Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept. In: *Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421,* 97–106.
13. Syrotynskyi R., et al. (2024). Methodology of Network Infrastructure Analysis as Part of Migration to Zero-Trust Architecture. In: *Cyber Security and Data Protection, vol. 3800,* 97–105.
14. Vorokhob, M., Kyrychok, R., Yaskevych, V., Dobryshyn, Y., & Sydorenko, S. (2023). Modern perspectives of applying the concept of zero trust in building a corporate information security policy. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(21),* 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233
15. Kriuchkova, L., Skladannyi, P., & Vorokhob, M. (2023). Pre-project solutions for building an authorization system based on the zero trust concept. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 3(19),* 226–242. https://doi.org/10.28925/2663-4023.2023.13.226242

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Rostyslav Tsekhmeister
Student of Faculty of Information Technologies and Mathematics
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0009-0001-6269-0321
rdtsekhmeister.fitm23m@kubg.edu.ua

Artem Platonenko
PhD, Associate Professor, Docent of the Department of Information and
Cyber Security named after Professor Volodymyr Buryachok,
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-2962-5667
a.platonenko@kubg.edu.ua

Maksym Vorokhob
PhD in Cybersecurity
Senior Teacher of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0001-5160-7134
m.vorokhob@kubg.edu.ua

Vyacheslav Cherevyk
PhD, Associate Professor,
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-2735-5341
v.cherevyk@kubg.edu.ua

Svitlana Semeniaka
Candidate of Physical and Mathematical Sciences, Associate Professor
Head of the Department of Mathematics and Physics
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0001-5083-1433
s.semeniaka@kubg.edu.ua

RESEARCH OF INFORMATION SECURITY PROVISION METHODS IN A VIRTUAL ENVIRONMENT

Abstract. In today's world of technological development and dependence, unfortunately, most IT assets of companies remain vulnerable due to a combination of technical and organizational factors, such as outdated technologies, configuration errors and the human factor. These weaknesses become the main entry points for cyber threats, allowing attackers to gain unauthorized access to data, disrupt services or launch large-scale attacks. The lack of a systematic approach to security significantly increases the risks of losing critical information and downtime. Analysis of existing threats, such as DDoS attacks, data leaks and hypervisor compromise, demonstrates the need for a comprehensive, multi-layered approach to protection. The use of firewalls, intrusion detection and prevention systems (IDS/IPS), SIEM solutions, as well as monitoring platforms allows you to effectively control traffic, detect anomalies and respond quickly to incidents. This article examines the issues of ensuring information security in virtualized environments using network protection systems, intrusion detection, proxy server, security monitoring and infrastructure control. Attention is also focused on the vulnerabilities of information systems associated with the use of outdated technologies, insufficient network segmentation, as well as errors in the configuration of security solutions. The comprehensive application of modern security technologies and flexible architectural approaches form a reliable basis for further improvement of information resource protection systems in virtualized environments. A multi-level protection architecture is proposed that integrates modern systems and is based on the concepts of Zero Trust, micro-segmentation and multi-level protection (Defense in Depth). The tests conducted confirmed the effectiveness of the implemented security

measures for the developed system, the results of which confirmed the effectiveness in detecting and preventing modern cyber threats, ensuring reliable protection of critical information resources in a dynamic environment.

Keywords: information security; virtualized environments; network protection systems; intrusion detection; proxy server; security monitoring; infrastructure control; zero trust; micro segmentation.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. *Protection of information. Technical protection of information. Basic provisions.* (DSTU 3396.0-96). (b.d.). State Service of Special Communications and Information Protection of Ukraine.
2. *Information security, cybersecurity and privacy protection. Information security management systems*. (DSTU ISO/IEC 27001:2023). (b.d.). State Enterprise "Ukrainian Research and Training Centre for Standardisation, Certification and Quality" (SE "UkrNDNC").
3. *Information technologies. Methods of protection. Code of Practice on Information Security Measures for Cloud Services Based on ISO/IEC 27002*. (DSTU ISO/IEC 27017:2016). Technical Committee for Standardisation "Information Technology" (TC 20).
4. *Cyber operations by russia: new goals, tools and groups. Analytics on the hacker attacks against Ukraine in H1 2024.* (2024). State Service of Special Communications and Information Protection of Ukraine. https://cip.gov.ua/en/news/cyber-operations-rf-h1-2024-report
5. *National Security and Defense Council of Ukraine. Major international and Ukrainian cybersecurity news in September 2024.* (2024). https://www.rnbo.gov.ua/en/Diialnist/7027.html
6. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access, 10,* 57144–57145. https://doi.org/10.1109/ACCESS.2022.3174679
7. Mukhopadhyay, M., Chakraborty, S., Chakrabarti. A. (2022). Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems. *Journal of Information Security, 2(1),* 28–38. https://doi.org/10.4236/jis.2011.21003
8. Ghasemshirazi, S., Shirvani, G., Alipour, M. (2022). Zero Trust: Applications, Challenges, and Opportunities. *Graduate University of Advanced Technology,* 16–17. https://doi.org/10.48550/arXiv.2309.03582
9. Campbell, M. (2020). Beyond Zero Trust: Trust Is a Vulnerability. *Computer, 53(10),* 110–113. https://doi.org/10.1109/MC.2020.3011081
10. Buqing, W. (2023). Analysis of a new firewall constructed on Pfsense with Snort to defend against common internet intrusions. *Applied and Computational Engineering, 43,* 244–250. https://doi.org/10.54254/2755-2721/43/20230841
11. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise.* Textbook. Lviv: Publisher Marchenko T. V.
12. Skladannyi, P., et al. (2023). Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept. In: *Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421,* 97–106.
13. Syrotynskyi R., et al. (2024). Methodology of Network Infrastructure Analysis as Part of Migration to Zero-Trust Architecture. In: *Cyber Security and Data Protection, vol. 3800,* 97–105.
14. Vorokhob, M., Kyrychok, R., Yaskevych, V., Dobryshyn, Y., & Sydorenko, S. (2023). Modern perspectives of applying the concept of zero trust in building a corporate information security policy. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(21),* 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233
15. Kriuchkova, L., Skladannyi, P., & Vorokhob, M. (2023). Pre-project solutions for building an authorization system based on the zero trust concept. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 3(19),* 226–242. https://doi.org/10.28925/2663-4023.2023.13.226242