КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.954
УДК 004.056

Скуратовський Євгеній Олегвич
здобувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-2973-6033
yoskuratovskyi.fitm24m@kubg.edu.ua

Аносов Андрій Олександрович
кандидат військових наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-2973-6033
a.anosov@kubg.edu.ua

Козачок Валерій Анатолійович
кандидат технічних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0003-0072-2567
v.kozachok@kubg.edu.ua

Бржевська Зореслава Михайлівна
PhD, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-7029-9525
z.brzhevska@kubg.edu.ua

РОЗРОБКА ТЕСТОВОГО СЕРЕДОВИЩА ДЛЯ ПЕРЕВІРКИ ЕФЕКТИВНОСТІ ВПРОВАДЖЕНИХ ЗАХОДІВ БЕЗПЕКИ НА РІВНІ ДОДАТКІВ

Анотація. У статті розглядається проблема забезпечення кібербезпеки корпоративних інформаційно-комунікаційних систем на рівні додатків, де зосереджується найбільша кількість сучасних атак. Автори підкреслюють обмеженість традиційних засобів, таких як мережеві брандмауери чи антивірусне ПЗ, у протидії загрозам, що експлуатують уразливості веб-додатків, API та мікросервісної архітектури. Обґрунтовано необхідність створення тестового середовища, яке дозволяє комплексно перевіряти ефективність упроваджених механізмів захисту, включно з контролем доступу, шифруванням, моніторингом активності користувачів, виявленням та запобіганням уразливостям, а також реагуванням на інциденти в режимі реального часу. Запропонована модель середовища побудована на базі віртуалізації із використанням VMware Workstation Pro та Oracle VirtualBox і включає три логічні зони (DMZ, внутрішню мережу та інструментальну). Використання інструментів Burp Suite, OWASP ZAP, sqlmap, Splunk, Wazuh, Metasploit забезпечує проведення як активного пентестування, так і пасивного моніторингу. У середовищі реалізовано сценарії типових атак (SQL-ін'єкції, XSS, CSRF, brute force, мережеве сканування тощо), що дозволяє оцінити точність виявлення загроз, рівень хибнопозитивних спрацювань, продуктивність системи та інтеграцію різних засобів. Середовище відповідає міжнародним стандартам ISO/IEC 27001 та NIST SP 800-53, а його ключовими перевагами є гнучкість у масштабуванні, відтворюваність експериментів і можливість застосування як у наукових дослідженнях, так і в освітньому процесі. Результати підтверджують доцільність інтеграції концепції DevSecOps і сучасних технологій SIEM, XDR, SOAR для підвищення рівня захисту додатків. Запропонований підхід формує надійну основу для оцінювання та вдосконалення заходів кіберзахисту в умовах реальних корпоративних середовищ.

Ключові слова: методи забезпечення безпеки, веб-додаток, API-інтерфейса, мікросерверна архітектура, механізми контролю доступу, моніторинг активності користувачів, тестове

середовище, рівень додатків, ефективність заходів безпеки.

ВСТУП

Безпека на рівні додатків відіграє досить критичну та важливу роль у загальній стратегії кіберзахисту, адже саме в цьому сегменті часто можуть відбуватися атаки на дані користувачів. Традиційні методи забезпечення безпеки, а саме мережеві брандмауери та антивірусне програмне забезпечення не можуть повністю захищати корпоративні мережі від атак, які спрямовані на вразливості у веб-додатках, API-інтерфейсах та мікросерверній архітектурі. Саме тому починає зростати необхідність у впровадженні комплексних методів захисту на рівні додатків із використанням механізмів контролю доступу, шифрування, виявлення та запобігання уразливостям, моніторинг активності користувачів та реагування на загрози у реальному часі.

Ефективність впровадження цих рішень значною мірою залежить від можливості адаптації до специфіки конкретної організації, рівня підготовки персоналу та відповідності сучасним безпековим стандартам (OWASP, NIST, ISO/IEC 27001). Що вимагає інтеграціїї механізмів безпеки вже у процесі розробки програмного забезпечення. Аналіз існуючих рішень дозволив сформувати базу для подальшого вибору найбільш релевантних інструментів і побудови ефективної моделі захисту на рівні додатків вже на етапі проектування захищеної мережі. Тому виникає необхідність у тестовому середовищі для перевірки ефективності впроваджених заходів безпеки на рівні додатків, методів захисту даних, що будуть використані в корпоративних додатках конкретної організації, їх ефективності, можливості впровадження та вплив на продуктивність системи [1-3].

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Загрози безпеки додатків можуть мати різні характери та виникати через низку причин, а саме: недостатньою увагою до безпеки під час розробки програмного забезпечення, використання застарілих технологій та вразливих бібліотек, відсутність ефективних механізмів автентифікації та контролю доступу та недостатній захист під час передавання даних між клієнтом та сервером.

Загрози на рівні додатків залишаються одним із найкритичніших векторів атак у корпоративних інформаційно-комунікаційних системах. До основних ризиків належать SQL-ін’єкції, XSS, CSRF, використання вразливих компонентів та неправильна реалізація контролю доступу [4-8].

Щоб перевірити безпеку програм та її проаналізувати, використовують спеціальні автоматичні інструменти, які аналізують програми на різних рівнях:

- Перший тип інструментів перевіряє код програми, не запускаючи її. Вони допомагають знайти потенційні проблеми до того, як програма почне працювати. (Наприклад, SonarQube, Checkmarx, Veracode).
- Другий тип інструментів перевіряє вже працюючу програму, імітуючи реальні атаки. Це допомагає виявити слабкі місця, які можуть використовувати зловмисники. (Наприклад, Burp Suite, Acunetix, OWASP ZAP).
- Третій тип інструментів поєднує в собі обидва попередні методи, що дозволяє виявляти складніші проблеми. (Наприклад, Contrast Security).
- Четвертий тип інструментів перевіряє, чи немає в програмі старих або вразливих компонентів, які можуть бути використані для атаки. (Наприклад, OWASP Dependency-Check, WhiteSource) [9-15].

Останнім часом активно розвивається концепція DevSecOps, яка передбачає інтеграцію заходів безпеки у всі етапи розробки додатків. Це дозволяє виявляти та виправляти потенційні уразливості ще на стадії написання коду, що значно знижує ризики для корпоративних інформаційних систем. Основні принципи DevSecOps включають:

- Автоматизацію процесів безпеки – інтеграція засобів перевірки безпеки в CI/CD-конвеєри.
- Впровадження інструментів безперервного моніторингу – використання рішень, що аналізують активність додатків у реальному часі.
- Залучення безпеки на всіх етапах розробки – розробники, тестувальники та спеціалісти з безпеки працюють разом для запобігання уразливостям на ранніх етапах.

Популярні інструменти для DevSecOps: GitHub Dependabot, GitLab Security, Jenkins Security Plugins. Впровадження DevSecOps сприяє створенню більш захищених додатків без значного впливу на швидкість розробки та випуску оновлень. Окрім запобіжних заходів, важливим елементом безпеки програм є система реагування на інциденти. Для цього використовують: SIEM-системи (Security Information and Event Management) – централізований збір та аналіз журналів подій для виявлення загроз (наприклад, Splunk, Wazuh, IBM QRadar); XDR (Extended Detection and Response) – інтегровані рішення для розширеного моніторингу загроз та автоматизованої реакції (наприклад, Microsoft Defender XDR, Palo Alto Cortex XDR); SOAR (Security Orchestration, Automation, and Response) – інструменти для автоматизації розслідувань та реагування на кіберзагрози (наприклад, Splunk Phantom, IBM Resilient). Завдяки цим технологіям організації можуть швидко виявляти атаки та мінімізувати їхній вплив на бізнес-процеси [16-22,26,27].

Однак впровадження автоматизованого тестування в Agile-процеси розроблення може бути складним через необхідність значних початкових витрат та ресурсів [11]. Інструменти автоматизованого тестування безпеки, такі як SAST та DAST, є важливими компонентами забезпечення безпеки додатків. Проте вони не завжди здатні виявляти всі можливі вразливості. Деякі складні логічні помилки або специфічні вразливості можуть залишатися непоміченими автоматичними засобами тестування, адже вони орієнтовані на пошук поширених загроз [12].

Тому, з метою практичної оцінки ефективності засобів безпеки, що впроваджуються та функціонують на рівні додатків, необхідне додаткове їх оцінювання в безпечному середовищі за критеріями: точність виявлення загроз, рівень хибнопозитивних спрацювань, інтеграція, продуктивність, зручність використання.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Метою створення тестового середовища є розробка ізольованої, контрольованої інфраструктури, максимально наближеної до умов функціонування корпоративної інформаційно-комунікаційної системи. Це дозволяє об’єктивно оцінити ефективність засобів захисту на рівні додатків (зокрема, Burp Suite, AppScan, ZAP, Wazuh, Splunk) без впливу на продуктивні сервіси та дані. Розгортання середовища виконується з урахуванням безпекових рекомендацій [22]. Тестове середовище побудовано на віртуалізації з використанням VMware Workstation Pro або Oracle VirtualBox. Такий підхід дозволяє швидко масштабувати інфраструктуру, створювати «snapshots», проводити ізольовані тести.

Таблиця 1

Основні компоненти середовища

№	Назва	Операційна система	Призначення
1	DC01	Windows Server 2019	Доменний контролер (Active Directory)
2	WebServer01	Ubuntu Server 22.04	Apache/Nginx + веб-додаток (вразливий додаток)
3	FileServer01	Windows Server 2019	SMB-сервер, імітація корпоративного сховища
4	Client01	Windows 10	Користувач AD, браузерні атаки, емуляція активності
5	KaliPentest	Kali Linux	Пентест: Burp Suite, Metasploit, sqlmap, ZAP
6	PfSense-FW	FreeBSD (pfSense)	Розмежування DMZ/внутрішньої мережі, firewall
7	SIEM-Node	Ubuntu Server 22.04	Splunk/Wazuh Server для збору та аналізу подій

Для імітації реального функціонування корпоративної інформаційної системи середовище поділене на три логічні зони. DMZ (демілітаризована зона):

- Web-сервер – імітація доступного ззовні додатку (наприклад, CMS, CRM тощо).
- SIEM-сервер – Splunk або Wazuh, для збору логів, подій, виявлення аномалій.

DMZ ізольована фаєрволом від внутрішньої мережі, що дозволяє імітувати зовнішні атаки без загрози внутрішнім ресурсам.

Внутрішня мережа:

- File-сервер – SMB/FTP-служба, симуляція обміну документами й робочих процесів.
- Клієнтська машина – звичайний користувач AD, який використовує браузер, email тощо.
- Доменний контролер (DC) – реалізує централізовану автентифікацію, керування політиками безпеки.

Це ядро корпоративної інфраструктури, яке не повинно бути безпосередньо доступне ззовні.

Інструментальна зона: Kali Linux – включає набір інструментів для моделювання атак: Nmap, Burp Suite, OWASP ZAP, sqlmap, Hydra, Metasploit Framework.

Інструментальна зона використовується для моделювання загроз та оцінки ефективності захисту.

Логічна мережева архітектура тестового середовища, що імітує корпоративну мережу з відокремленими зонами:

- DMZ – зона, що «оголена» до атак, де найчастіше знаходяться веб-додатки. Тут імітується вразливий Web-сервер.
- Внутрішня мережа – сегмент, доступ до якого ззовні має бути максимально обмежений. Тут знаходяться критичні дані.
- Інструментальна зона (Kali) – зона, з якої виконуються атаки на середовище. Вона не має прямого доступу до продуктивних систем.
- PfSense Firewall – виступає центральною точкою контролю, яка дозволяє моделювати правила доступу між зонами (відповідає Zero Trust-принципам).

Зв’язки: усі зони підключені до фаєрвола (PfSense), що дозволяє змінювати політику доступу між ними; інструментальні атаки з Kali направляються на Web-сервер та SIEM, а результати логуються. Це дає змогу імітувати атакувальні сценарії та одночасно перевіряти логування, реагування й пропускну здатність інструментів захисту [23].

Всі елементи розгорнуті у середовищі VMware Workstation Pro або Oracle VirtualBox. Налаштування кожної ВМ передбачає легко відновлювати початковий стан та повторювати експерименти з нуля.

Експериментальна частина включає реальні сценарії атак на рівні додатків.

Таблиця 2

Сценарії тестування

№	Сценарій	Інструменти	Мета тесту
1	SQL-ін'єкція (SQLi)	sqlmap, Burp Suite	Виявлення помилок в обробці запитів до БД
2	XSS (міжсайтовий скриптинг)	OWASP ZAP, Burp Suite	Виявлення необроблених HTML/JS-вставок
3	CSRF-атака	Burp Suite	Тест захисту форм від підміни запитів
4	Brute Force	Hydra	Оцінка захисту форм входу
5	SMB enumeration	Kali (enum4linux, smbclient)	Тест контролю доступу до файлів
6	Мережеве сканування	Nmap	Виявлення слабких сервісів, перевірка логування
7	Аналіз логів та подій	Splunk, Wazuh	Перевірка реєстрації подій, реакції системи

Ізоляція середовища – повна мережева ізоляція досягається за рахунок створення окремої мережі типу Host-only/Internal та розгортання віртуального фаєрвола pfSense, який чітко регулює доступ між DMZ, внутрішньою мережею та пентест-середовищем. Відсутність доступу до Інтернету гарантує безпечне тестування навіть небезпечних векторів атак (наприклад, DoS чи експлуатація вразливостей в CMS).

Відтворюваність експериментів – функціонал snapshots, наявність шаблонів віртуальних машин та автоматизовані скрипти (де це можливо) дозволяють легко повертатися до початкового стану системи. Це забезпечує точність повторних тестів, що є критично важливим для наукової достовірності.

Різноманітність ОС та ролей – середовище включає Windows Server, Windows 10, Ubuntu, Kali Linux, що дозволяє охопити всі ключові рівні: серверний, клієнтський, інструментальний. Наявність ролей DC, File-сервер, WebApp, SIEM, Client забезпечує повноцінну симуляцію корпоративної мережі.

Підтримка активного та пасивного тестування – інструменти типу Burp Suite, sqlmap, ZAP, Metasploit використовуються для активного впливу на середовище, а Splunk, Wazuh, syslog – для пасивного моніторингу та реагування. Це дозволяє комплексно оцінити стійкість системи до атак і якість логування.

Збір логів та аналітичних даних – система логування реалізована за допомогою агентів Wazuh, універсальних syslog-механізмів, а також централізованої консолі Splunk із кореляційними правилами. Це дозволяє не лише виявляти атаки, а й формувати статистичні висновки щодо ефективності захисту. Таким чином, тестове середовище є не лише технічно функціональним, а й методологічно обґрунтованим, що робить його придатним для наукового дослідження ефективності засобів захисту додатків у реаліях корпоративної мережі.

Побудоване тестове середовище узгоджується з загальновизнаними міжнародними стандартами у сфері кібербезпеки, зокрема ISO/IEC 27001 (розділи A.13 – контроль комунікацій, A.12 – операційне управління) та NIST SP 800-53 (сімейство контролів System and Communications Protection – SC). Застосування принципів сегментації мережі, контролю доступу, багаторівневого моніторингу, журналювання подій та ізоляції середовища відповідає вимогам до побудови захищених інформаційних систем [24].

Основна перевага запропонованого середовища – простота конфігурації, гнучкість у масштабуванні, відтворюваність експериментів, що дає змогу адаптувати його для

дослідницької та освітньої діяльності [25]. Схема, що зображена на рисунку 1, демонструє, як атаки з інструментальної зони (Kali) проходять через додатки, що тестуються, логуються та потрапляють на обробку в SIEM-системи. Це дозволяє простежити весь цикл: від загрози до виявлення й реагування.

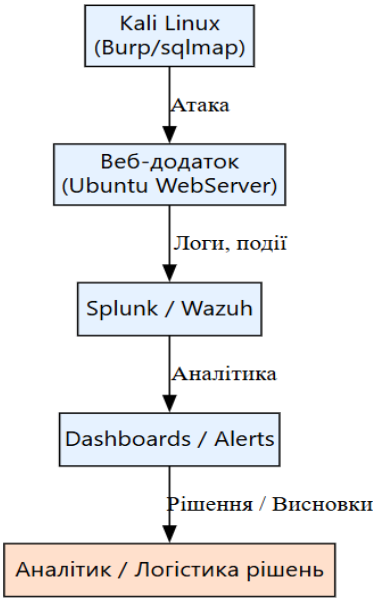

Рис. 1 – Схема потоку даних у тестовому середовищі

Для коректного дотримання умов ліцензування під час дослідження використовувалися такі моделі:

- Burp Suite Pro – версія з академічною ліцензією або trial-ліцензія (30 днів);
- OWASP ZAP, Wazuh – повністю безкоштовні open-source рішення;
- Splunk Free Edition – підтримка до 500 МБ логів на добу, що достатньо для тестування;
- AppScan (IBM) – доступ до демо-версії згідно з умовами науково-дослідного використання.

Це забезпечило повну легальність, доступність і функціональну достатність обраних засобів для проведення дослідження. Загалом, побудоване середовище охоплює всі ключові компоненти сучасної корпоративної мережі: автентифікація, веб-доступ, зберігання даних, реагування на події та аналіз загроз. Його модульна архітектура, повна ізоляція, а також підтримка як активного, так і пасивного тестування створюють надійну, валідну основу для експериментальної перевірки ефективності методів захисту даних. У наступних підпунктах будуть описані результати реалізації захисних заходів та аналітичні висновки щодо їх впливу на безпеку та продуктивність.

Завдяки чіткому зонуванню, використанню сучасних інструментів (Burp Suite, ZAP, Splunk, Wazuh тощо), підтримці журналів та аналітики, середовище дозволяє моделювати реальні сценарії атак та оцінювати ефективність методів захисту на рівні додатків.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Застосування тестового середовища для перевірки ефективності впроваджених

заходів безпеки на рівні додатків полягає у проведенні всебічного аналізу ефективності сучасних методів захисту корпоративних додатків. Дозволяє порівняти їх з традиційними підходами, оцінити реальну ефективність механізмів захисту з урахуванням їхнього впливу на продуктивність системи, створення моделі реальних загроз та визначенню оптимальних заходів безпеки для захисту даних на рівні додатків у корпоративних мережах.

Налаштовані механізми охоплюють: глибоке виявлення вразливостей; контроль цілісності системних компонентів; моніторинг у режимі реального часу; автоматизоване реагування на інциденти; формування журналів, звітів та візуалізацій для подальшого аудиту.

Реалізація обраних інструментів захисту в тестовому середовищі підтвердила можливість створення інтегрованої системи безпеки на рівні додатків, яка відповідає сучасним вимогам до захищеності корпоративних IT-інфраструктур. Використання Burp Suite Pro, OWASP ZAP, IBM AppScan і Acunetix забезпечило покриття ключових категорій вразливостей, зокрема відповідно до класифікації OWASP

Реалізація тестового середовища демонструє успішне поєднання класичних інструментів аналізу безпеки, автоматизованих засобів реагування та стратегічного управління ризиками, що робить запропонований підхід ефективним, масштабованим і таким, що може бути адаптований до реальних корпоративних середовищ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication systems security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
2. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
3. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). Enterprise information and cyber security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
4. Netwave. (n.d.). *Zakhyst korporatyvnykh merezh vid zahroz: zasoby ta metody* [Protection of corporate networks from threats: tools and methods]. Retrieved from https://netwave.ua/zahist-korporativnih-merezh-vid-zagroz-zasobi-ta-metodi/
5. Pidruchnyky dlia vuziv onlain. (n.d.). *Bezpeka informatsiinykh system* [Information systems security]. Retrieved from https://pidru4niki.com/74227/informatika/bezpeka_informatsiynih_sistem
6. OWASP. (2024). *OWASP Top Ten Security Risks*. Retrieved from https://owasp.org/www-project-top-ten/
7. The MITRE Corporation. (2024). *CWE – Common Weakness Enumeration*. Retrieved from https://cwe.mitre.org/
8. National Institute of Standards and Technology (NIST). (2024). *National Vulnerability Database (NVD)*. Retrieved from https://nvd.nist.gov
9. SANS Institute. (2024). *Application security risks*. Retrieved from https://www.sans.org/top25-software-errors
10. Microsoft. (2024). *Microsoft Security Development Lifecycle (SDL)*. Retrieved from https://www.microsoft.com/security/blog/security-development-lifecycle/
11. OWASP. (2024). *Input validation in web applications*. Retrieved from https://owasp.org/www-project-input-validation/
12. NIST. (2024). *Digital identity guidelines (SP 800-63-3)*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-63/3/final
13. SSL Labs. (2024). *TLS and encryption in web applications*. Retrieved from https://www.ssllabs.com/ssltest/
14. NIST. (2024). *Vulnerability management and software updates*. Retrieved from https://nvd.nist.gov/
15. Cisco Systems. (2024). *Intrusion Detection and Prevention Systems (IDS/IPS)*. Retrieved from https://www.cisco.com/c/en/us/products/security/ids-ips/

16. SANS Institute. (2024). *DevSecOps: Integrating security into development*. Retrieved from https://www.sans.org/cyber-security-courses/devsecops/
17. OWASP. (2024). *Application Security Verification Standard (ASVS)*. Retrieved from https://owasp.org/www-project-application-security-verification-standard/
18. Splunk Inc. (2024). *SIEM and XDR for application protection*. Retrieved from https://www.splunk.com/en_us/products/enterprise-security.html
19. NIST. (2024). *Recommendation for key management (SP 800-57)*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-57/
20. VirusTotal. (2024). *Antivirus software vulnerabilities*. Retrieved from https://www.virustotal.com/gui/home/
21. SANS Institute. (2024). *Challenges of implementing DevSecOps in modern companies*. Retrieved from https://www.sans.org/cyber-security-courses/devsecops/
22. Microsoft Security. (2024). *Issues of multi-factor authentication (MFA)*. Retrieved from https://www.microsoft.com/security/blog/
23. NIST. (2024). *Software update and vulnerability management*. Retrieved from https://nvd.nist.gov/
24. OWASP. (2024). *Limitations of automated application security testing*. Retrieved from https://owasp.org/www-project-application-security-verification-standard/
25. Cisco Systems. (2024). *Intrusion detection and prevention systems: Limitations and challenges*. Retrieved from https://www.cisco.com/c/en/us/products/security/ids-ips/
26. Kostiuk, Y., Skladannyi, P., Rzaeva , S., Mazur , N., Cherevyk, V., & Anosov, A. (2025). Features of Network Attack Implementation ThrougH TCP/IP Protocols. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *1*(29), 571–597. https://doi.org/10.28925/2663-4023.2025.29.915
27. Tsekhmeister, R., Platonenko, A., Vorokhob , M., Cherevyk, V., & Semeniaka, S. (2025). Research of Information Security Provision Methods in a Virtual Environment. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *3*(27), 63–71. https://doi.org/10.28925/2663-4023.2025.27.703

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue

Yevhenii Skuratovskyi
student of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-2973-6033
yoskuratovskyi.fitm24m@kubg.edu.ua

Andriy Anosov
PhD, Associate Professor,
Associate Professor of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-2973-6033
a.anosov@kubg.edu.ua

Valerii Kozachok
PhD, Associate Professor,
Associate Professor of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0003-0072-2567
v.kozachok@kubg.edu.ua

Zoreslava Brzhevska
PhD, Associate Professor,
Associate Professor of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-7029-9525
z.brzhevska@kubg.edu.ua

DEVELOPMENT OF A TEST ENVIRONMENT FOR EVALUATING THE EFFECTIVENESS OF IMPLEMENTED APPLICATION-LEVEL SECURITY MEASURES

Abstract: The article addresses the problem of ensuring cybersecurity of corporate information and communication systems at the application level, which remains the main vector of modern cyberattacks. The limitations of traditional tools such as firewalls and antivirus software in countering vulnerabilities of web applications, APIs, and microservice architectures are emphasized. To overcome these challenges, the authors propose the development of a test environment enabling comprehensive assessment of implemented security measures, including access control, encryption, user activity monitoring, vulnerability detection and prevention, and real-time incident response. The proposed virtualized environment, built on VMware Workstation Pro and Oracle VirtualBox, is divided into three logical zones (DMZ, internal network, and instrumental zone) and integrates tools such as Burp Suite, OWASP ZAP, sqlmap, Splunk, Wazuh, and Metasploit. It allows the simulation of typical attack scenarios (SQL injection, XSS, CSRF, brute force, network scanning) to evaluate detection accuracy, false-positive rates, performance, and integration of different security components. The environment is aligned with international standards ISO/IEC 27001 and NIST SP 800-53, while its flexibility, scalability, and reproducibility make it suitable for both research and educational purposes. Results confirm the relevance of integrating the DevSecOps approach with SIEM, XDR, and SOAR technologies to strengthen application-level protection. The proposed solution provides a reliable foundation for evaluating and improving cybersecurity measures in real corporate environments.

Keywords: security methods, web application, API interface, microservice architecture, access control mechanisms, user activity monitoring, test environment, application level, effectiveness of security measures.

REFERENCES

1. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication systems security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
2. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
3. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). Enterprise information and cyber security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
4. Netwave. (n.d.). *Zakhyst korporatyvnykh merezh vid zahroz: zasoby ta metody* [Protection of corporate networks from threats: tools and methods]. Retrieved from https://netwave.ua/zahist-korporativnih-merezh-vid-zagroz-zasobi-ta-metodi/
5. Pidruchnyky dlia vuziv onlain. (n.d.). *Bezpeka informatsiinykh system* [Information systems security]. Retrieved from https://pidru4niki.com/74227/informatika/bezpeka_informatsiynih_sistem
6. OWASP. (2024). *OWASP Top Ten Security Risks*. Retrieved from https://owasp.org/www-project-top-ten/
7. The MITRE Corporation. (2024). *CWE – Common Weakness Enumeration*. Retrieved from https://cwe.mitre.org/
8. National Institute of Standards and Technology (NIST). (2024). *National Vulnerability Database (NVD)*. Retrieved from https://nvd.nist.gov
9. SANS Institute. (2024). *Application security risks*. Retrieved from https://www.sans.org/top25-software-errors
10. Microsoft. (2024). *Microsoft Security Development Lifecycle (SDL)*. Retrieved from https://www.microsoft.com/security/blog/security-development-lifecycle/
11. OWASP. (2024). *Input validation in web applications*. Retrieved from https://owasp.org/www-project-input-validation/
12. NIST. (2024). *Digital identity guidelines (SP 800-63-3)*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-63/3/final
13. SSL Labs. (2024). *TLS and encryption in web applications*. Retrieved from https://www.ssllabs.com/ssltest/
14. NIST. (2024). *Vulnerability management and software updates*. Retrieved from https://nvd.nist.gov/
15. Cisco Systems. (2024). *Intrusion Detection and Prevention Systems (IDS/IPS)*. Retrieved from https://www.cisco.com/c/en/us/products/security/ids-ips/
16. SANS Institute. (2024). *DevSecOps: Integrating security into development*. Retrieved from https://www.sans.org/cyber-security-courses/devsecops/
17. OWASP. (2024). *Application Security Verification Standard (ASVS)*. Retrieved from https://owasp.org/www-project-application-security-verification-standard/
18. Splunk Inc. (2024). *SIEM and XDR for application protection*. Retrieved from https://www.splunk.com/en_us/products/enterprise-security.html
19. NIST. (2024). *Recommendation for key management (SP 800-57)*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-57/
20. VirusTotal. (2024). *Antivirus software vulnerabilities*. Retrieved from https://www.virustotal.com/gui/home/
21. SANS Institute. (2024). *Challenges of implementing DevSecOps in modern companies*. Retrieved from https://www.sans.org/cyber-security-courses/devsecops/
22. Microsoft Security. (2024). *Issues of multi-factor authentication (MFA)*. Retrieved from https://www.microsoft.com/security/blog/
23. NIST. (2024). *Software update and vulnerability management*. Retrieved from https://nvd.nist.gov/
24. OWASP. (2024). *Limitations of automated application security testing*. Retrieved from https://owasp.org/www-project-application-security-verification-standard/
25. Cisco Systems. (2024). *Intrusion detection and prevention systems: Limitations and challenges*. Retrieved from https://www.cisco.com/c/en/us/products/security/ids-ips/
26. Kostiuk, Y., Skladannyi, P., Rzaeva, S., Mazur, N., Cherevyk, V., & Anosov, A. (2025). Features of Network Attack Implementation ThrougH TCP/IP Protocols. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *1*(29), 571–597. https://doi.org/10.28925/2663-4023.2025.29.915
27. Tsekhmeister, R., Platonenko, A., Vorokhob, M., Cherevyk, V., & Semeniaka, S. (2025). Research of Information Security Provision Methods in a Virtual Environment. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *3*(27), 63–71. https://doi.org/10.28925/2663-4023.2025.27.703