сумарне зниження енергоспоживання для типової навчальної лабораторії на 30 місць становить близько 50% [1]. Крім того, апаратна простота «тонких» клієнтів (відсутність вентиляторів та жорстких дисків) збільшує середній час напрацювання на відмову (MTBF) до 70 000 годин у порівнянні з 30 000 годин для класичних комп'ютерів [1].

У контексті навчання з кібербезпеки архітектура малопотужних клієнтів також вирішує ключову проблему надійної ізоляції та швидкого відновлення стендів. Оскільки «тонкі» клієнти обмежують взаємодію із зовнішніми носіями, несанкціоноване копіювання даних або зараження локальної машини шкідливим кодом стає технічно неможливим [1, 4]. Сама ж інфраструктура VDI дозволяє ефективно використовувати технології «золотого образу» (golden image) та зв'язаних клонів (linked clones) [1]. Завдяки цьому після завершення лабораторної роботи користувацька сесія миттєво відключається, а змінена чи навіть скомпрометована віртуальна машина за кілька секунд повністю автоматично відновлюється до еталонного «чистого» стану [1, 5].

Отже, впровадження малопотужних апаратних вузлів у віртуалізовані навчальні середовища є обґрунтованим кроком, що забезпечує суттєве зниження сукупної вартості володіння (TCO) інфраструктурою [1]. Перехід від «товстих» клієнтів до спеціалізованих «тонких» пристроїв гарантує радикальне зменшення енергоспоживання на кінцевих робочих місцях, забезпечуючи при цьому централізоване керування та максимальний рівень ізоляції операційного середовища, який є критично необхідним для безпечного дослідження сучасних кіберзагроз [3, 4].

1. Rot A., Chrobak P. Benefits, Limitations and Costs of IT Infrastructure Virtualization in the Academic Environment. Case Study using VDI Technology. In Proceedings of the 13th International Conference on Software Technologies (ICSOFT 2018), 2018. P. 704-711.
2. Pattinson C., Cross R., Kor A. L. Thin-client and Energy Efficiency. JISC Green IT Technical Report, 2011. 23 p.
3. Akintunde R. A. The Benefits of Thin Clients to Business Organizations in Developing Countries “A Case Study of Nigeria”. Master’s Thesis, University of Oulu, 2017. 83 p.
4. Смирнов О.А. Сучасні підходи до побудови захищених віртуалізованих IT-інфраструктур у закладах вищої освіти. Сучасний захист інформації. – 2024. – Т. 15, №1. – С. 45-52.
5. Mell P., Grance T. The NIST Definition of Cloud Computing. NIST Special Publication 800-145, 2011. 7 p.

Гібридна модель захисту вебзастосунків на основі OWASP Top 10 і штучного інтелекту

УДК 004.056:004.8:004.77

[1]Савчук Костянтин, [2]Нємкова Олена

Національний університет Львівська Політехніка,
[1]kostiantyn.v.savchuk @lpnu.ua, [2]olena.a.niemkova@lpnu.ua

Вебзастосунки сьогодні є частиною майже кожного цифрового сервісу: інтернет-магазинів, банків, навчальних систем і державних порталів. Через це вони часто стають ціллю атак. У дослідженні розглянуто SQL-ін'єкції, XSS, CSRF та DDoS. Традиційні засоби захисту, зокрема WAF, IDS, IPS, статичні правила і сигнатури, що добре працюють проти відомих атак. Але їм важко помічати нові або змінені атаки, особливо у хмарних системах, мікросервісах та API.

Метою дослідження є побудова гібридної моделі веббезпеки, яка поєднує чіткі правила OWASP Top 10:2025 і методи штучного інтелекту [1]. Модель має два шари. Перший шар, Foundation, відповідає за базовий захист за правилами OWASP. Другий шар, Amplifier, додає три методи ШІ: HTTP2vec, графові нейронні мережі та Kitsune. Для порівняння різних методів виявлення атак було проаналізовано наукові праці та галузеві звіти. Перший шар закриває базові ризики вебзастосунків. Параметризовані запити та підготовлені оператори відокремлюють дані користувача від SQL-коду і допомагають проти ін'єкцій. Політика Content Security Policy обмежує виконання небезпечних скриптів і зменшує шкоду від XSS. SameSite cookies і короткоживучі токени захищають сесії. Багатофакторна автентифікація зменшує користь викраденого пароля. Захищене налаштування прибирає типові помилки, наприклад стандартні паролі, зайві сервіси або відкриті сховища. Для ризиків ланцюга постачання пропонуються сканування залежностей, Software Bill of Materials та перевірка процесу збірки.

Другий шар шукає те, що правила можуть пропустити. HTTP2vec працює з HTTP-запитами як з текстом. Модель навчається на нормальному трафіку, перетворює запити у числові вектори і знаходить запити, які сильно відрізняються від звичайних. Це корисно для виявлення SQLi, XSS та command injection, але така модель має великий розмір і потребує значних обчислювальних ресурсів [2]. Графові нейронні мережі показують зв'язки між користувачами, пристроями, сесіями та IP-адресами. Так легше помітити захоплення акаунтів або скоординовані атаки, хоча графові дані не завжди просто підготувати [3]. Kitsune працює на мережевому шлюзі або edge-пристрої, використовує невеликі автоенкодери і швидко бачить DDoS, сканування та MitM-атаки [4].

У моделі обидва шари з'єднані через SIEM і SOAR. Сигнали від HTTP2vec, графових нейронних мереж, Kitsune, WAF та IDS надходять до SIEM. SIEM збирає ці сигнали, порівнює їх і визначає, які сповіщення важливіші. Якщо підозрілий запит одночасно бачить модель HTTP2vec і WAF, довіра до такого сповіщення стає вищою. SOAR може автоматично заблокувати IP-адресу, відкликати токен або ізолювати систему. Якщо впевненість середня, сповіщення отримує аналітик. Його рішення потім можна використати для поліпшення моделей.

Порівняння можливостей двох підходів показало, що гібридний підхід поєднує їх сильні сторони. Правила добре зупиняють відомі атаки, а ШІ допомагає знайти нові або скоординовані загрози. Така модель важча для обходу, бо зловмиснику потрібно обійти і правила, і ШІ. У дослідженні також наведено галузеві дані: після додавання ШІ до SIEM і SOAR кількість

помилкових сповіщень може зменшитися приблизно на 60%, а розслідування інцидентів може стати приблизно на 40% швидшим [5]. Але варто підкреслити, що ці числа треба сприймати обережно, бо вони взяті з вторинних джерел, а не з контрольованого експерименту.

Для оцінювання таких систем доцільно не обмежуватися ROC-AUC. У безпекових даних шкідливий трафік часто становить менше ніж 0,1% від усього трафіку, тому ROC-AUC може приховати велику кількість зайвих сповіщень. Криві Precision-Recall та показник Average Precision краще показують, скільки сповіщень справді є корисними [6]. Для систем реального часу пропонується Numenta Anomaly Benchmark, бо він враховує, наскільки рано система помітила аномалію [7].

Висновки. У дослідженні запропоновано гібридну модель захисту вебзастосунків з двома шарами. Foundation дає базовий і зрозумілий захист за OWASP Top 10:2025, а Amplifier підсилює його трьома методами ШІ: HTTP2vec, графовими нейронними мережами та Kitsune. Головна ідея моделі проста: ШІ не замінює традиційний захист, а робить його сильнішим. Подальша робота має включати перевірку моделі в контрольованому середовищі, створення кращих відкритих наборів даних, навчання моделей без передавання чутливого трафіку та тестування стійкості ШІ до навмисного обходу.

1. OWASP Foundation. OWASP Top 10:2025. 2025. URL: https://owasp.org/Top10/2025/
2. Gniewkowski M. et al. HTTP2vec: Embedding of HTTP requests for detection of anomalous traffic. arXiv, 2021.
3. Bilot T., Legay A., Rønne P. B. Graph neural networks for intrusion detection: A survey // IEEE Access. 2023. Vol. 11. P. 45589-45612.
4. Mirsky Y. et al. Kitsune: An ensemble of autoencoders for online network intrusion detection // Proc. NDSS 2018.
5. Dilmegani C. Top 13 AI cybersecurity use cases with real examples in 2025. AIMultiple Research. 2025.
6. Saito T., Rehmsmeier M. The Precision-Recall plot is more informative than the ROC plot // PLOS ONE. 2015. Vol. 10(3). e0118432.
7. Lavin A., Ahmad S. Evaluating real-time anomaly detection algorithms - the Numenta Anomaly Benchmark // IEEE ICMLA. 2015. P. 38-44.

Fast squaring of multiword numbers using Mersenne modules

UDK 519.67

Andrii Tereshchenko[1], Valeriy Zadiraka[2]

V.M. Glushkov Institute of Cybernetics, [1]teramidi@ukr.net, [2]zvk140@ukr.net

In the era of post-quantum computing, it is necessary to increase the length of keys to increase cryptographic strength, which affects the performance of hardware-software cryptographic complexes. The performance of such complexes depends to a greater extent on the performance of the square operation [1] by modulus.

The multiword operation of squaring by Mersenne modulus is considered, which is one of the steps of the algorithm for implementing the multiword operation of