Future studies must benchmark SVG LSB against standard defensive tools. Because SVGs are processed as code by firewalls rather than images, research can empirically prove whether vector steganography can bypass mainstream pixel-based steganalysis engines.

LSB steganography must evolve alongside modern web standards. By embedding data into the XML architecture of SVG files, we can open up a lightweight and novel vector for secure data transmission.

1. Aditya, S., Ved, M., Shashikant, K., Samadhan, K., & Shilpa, M. A. (2024). Image steganography using least significant bit. International Journal of Research Publication and Reviews, 5(4), 2505–2508. https://doi.org/10.55248/gengpi.5.0424.0966
2. Madoš, B., Hurtuk, J., Čopjak, M., Hamaš, P., & Ennert, M. (2014). Steganographic algorithm for information hiding using scalable vector graphics images. Acta Electrotechnica et Informatica, 14(4), 42–45. https://doi.org/10.15546/aeei-2014-0040
3. Xu Z. Xu D. Li Z. Zheng X. & Zhang C. (2026). GVIS: Generative vector image steganography. In proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 9384–9393). https://openaccess.thecvf.com/content/CVPR2026/papers/Xu_GVIS_Generative_Vector_Image_Steganography_CVPR_2026_paper.pdf

Метод виявлення ботнет-активності в корпоративній мережі на основі багатокритеріальної оптимізації XGBoost

УДК 004.056:004.85

Владислав Самойленко[1], Сергій Гахов[2]

Державний університет інформаційно-комунікаційних технологій,
[1]v.samoylenko@duikt.edu.ua, [2]gakhovsa@gmail.com

Ботнет-активність залишається однією з найнебезпечніших загроз для корпоративних мереж, оскільки використовується для DDoS-атак, розсилання спаму, крадіжки даних та прихованого віддаленого керування зараженими вузлами. У дослідженні авторів [1] на наборі даних CSE-CIC-IDS2018 було порівняно Random Forest, XGBoost та SVM для виявлення ботнетів. Найкращим базовим рішенням стала XGBoost, яка досягла середнього значення F1-міри 0,99 за крос-валідацією при часу навчання близько 16 с. Це обґрунтувало перехід від простого вибору моделі до її оптимізації з урахуванням умов практичного мережевого моніторингу.

Метою роботи є розроблення методу виявлення ботнет-активності, який одночасно забезпечує високу якість класифікації, контроль рівня хибних спрацювань та достатню пропускну здатність для потокового моніторингу. Для уникнення витоку інформації дані Friday-02-03-2018 було поділено на раннє вікно S1 для навчання й оптимізації та пізніше вікно S2 для фінального тестування, а benign-підмножину Thursday-15-02-2018 використано як незалежний негативний день для калібрування порога рішення за обмеженням FPR ≤ 1 %. Основою експерименту слугував набір даних CSE-CIC-IDS2018 [2].

Наукова новизна дослідження полягає у формуванні відтворюваного протоколу вибору конфігурації XGBoost [3], у якому багатокритеріальна оптимізація поєднується з operationally-oriented перевіркою моделі. Оптимізація виконувалася за двома цілями: середньою Average Precision на часово-коректній forward-валідації та наскрізною пропускною здатністю інференсу. Пошук конфігурацій здійснювався з використанням Optuna [4]. На відміну від підходів, де оцінюється лише якість класифікації або лише час predict, у роботі враховано повний ланцюг інференсу, включаючи побудову DMatrix, а робочий поріг обирається без використання майбутнього тестового вікна S2.

За результатами багатокритеріального пошуку було відібрано три репрезентативні конфігурації Pareto-фронту: Light, Balanced і Heavy. Основні результати порівняння наведено в таблиці 1. Модель Balanced з 40 деревами забезпечила F1 = 0,9963 на майбутньому вікні S2 при FPR = 0,0098 на незалежній benign-підмножині Thursday та медіанній наскрізній пропускній здатності 1 583 532 потоків/с. Для порівняння, конфігурація Heavy з 90 деревами дала лише незначно вищу F1 = 0,9965, але зменшила пропускну здатність до 559 256 потоків/с.

Важливо, що використання часово-коректної схеми оцінювання «навчання на ранньому вікні — тестування на пізнішому» наближує експеримент до реальних умов функціонування засобів мережевого моніторингу. Такий підхід зменшує ризик отримання надто оптимістичних оцінок якості, які можуть виникати під час випадкового перемішування потоків. Додаткове калібрування порога на незалежному benign-дні підвищує надійність практичного використання моделі та дає змогу заздалегідь обмежити інтенсивність хибних спрацювань.

Таблиця 1

Порівняння репрезентативних конфігурацій XGBoost

Конфігурація	Дерев	F1 на S2	Пропускна здатність, потоків/с
Light	20	0,9845	1 901 519
Balanced	40	0,9963	1 583 532
Heavy	90	0,9965	559 256

Отримані результати показують, що для практичних систем виявлення ботнетів максимізація лише метрик якості є недостатньою. Раціональнішим є вибір конфігурації, що забезпечує баланс між точністю, контрольованим обсягом хибних спрацювань та швидкодією обробки трафіку. У цьому дослідженні такою конфігурацією є Balanced: вона зберігає майже ту саму якість, що й складніша Heavy-модель, але має приблизно у 2,8 раза вищу наскрізну пропускну здатність.

Перспективи подальших досліджень полягають у розширенні методу за рахунок локальної інтерпретації ознак, часової агрегації рішень для послідовностей потоків та перевірки стійкості моделі на нових фрагментах мережевого трафіку. Це дасть змогу підвищити пояснюваність результатів для аналітика безпеки та адаптивність системи до змін у поведінці ботнетів.

Практичне значення запропонованого методу полягає у можливості використання XGBoost у системах реального часу для виявлення ботнет-активності в корпоративних мережах без перевантаження аналітиків надмірною кількістю хибних тривог. У підсумку, запропонований підхід може бути використаний як основа для побудови масштабованих засобів мережевого моніторингу, у яких одночасно враховуються точність виявлення, контроль FPR та продуктивність обробки трафіку.

1. Samoilenko V., Gakhov S. Comparative Analysis of Machine Learning Methods for Detecting Botnet Activities in Corporate Networks. SSRN Electronic Journal. 2025. DOI: 10.2139/ssrn.5188775.
2. Sharafaldin I., Habibi Lashkari A., Ghorbani A. A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. ICISSP 2018. P. 108–116. DOI: 10.5220/0006639801080116.
3. Chen T., Guestrin C. XGBoost: A Scalable Tree Boosting System. Proc. of the 22nd ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining. 2016. P. 785–794. DOI: 10.1145/2939672.2939785.
4. Akiba T., Sano S., Yanase T., Ohta T., Koyama M. Optuna: A Next-generation Hyperparameter Optimization Framework. Proc. of the 25th ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining. 2019. P. 2623–2631. DOI: 10.1145/3292500.3330701.

Ключові контролі стандартів інформаційної безпеки для захисту критичної інфраструктури

УДК 004.056.5

Сведенюк Олексій [1], Курій Євгеній [2]

Національний університет "Львівська політехніка",
oleksii.svedeniuk.asp.2025@lpnu.ua [1], yevhenii.o.kurii@lpnu.ua [2]

Актуальність та постановка проблеми. Об'єкти критичної інфраструктури (ОКІ) України перебувають під постійним тиском цілеспрямованих кібератак (APT). Конвергенція IT- та OT-технологій створює нові вектори загроз, де компрометація одного сегмента загрожує катастрофічними наслідками для національної безпеки. Складність традиційних підходів до захисту заважає їх швидкому впровадженню, що зумовлює необхідність виокремлення пріоритетних заходів контролю [1].

Мета роботи — визначити та обґрунтувати набір критичних контролів на основі міжнародних стандартів (NIST CSF, CIS Controls v8, ISO/IEC 27001), адаптованих для захисту активів вітчизняної критичної інфраструктури.

Наукова новизна. У роботі запропоновано адаптивну модель ієрархізації засобів захисту, яка враховує специфіку функціонування АСУ ТП (SCADA) та забезпечує безперервність критичних бізнес-процесів навіть в умовах обмежених ресурсів.

Виклад основного матеріалу. Аналіз фреймворків дозволяє виділити «фундаментальні контролі», що захищають від 85% поширених атак. Для ОКІ критичними є: 1) інвентаризація апаратних і програмних активів; 2) управління