practical feasibility and effectiveness in achieving a baseline cybersecurity posture under constrained resources.

The following conclusions can be drawn from this research: 1) existing information security frameworks exhibit a systemic gap with the actual needs of SMBs, making their full implementation impractical under resource constraints; 2) the proposed framework provides a practically achievable path to baseline cybersecurity, bridging the gap between academic standards and the real capabilities of small businesses; 3) prioritizing organizational security measures over technical ones is the key principle of effective cybersecurity for SMBs; 4) a phased approach with a 30/90/180-day horizon enables enterprises to systematically build their security posture in accordance with available resources.

1. Verizon Data Breach Investigations Report 2024. Basking Ridge: Verizon, 2024. 100 p.
2. U.S. Small Business Administration. Small Business Facts. Washington: SBA, 2024.
3. NIST Cybersecurity Framework 2.0. National Institute of Standards and Technology. Gaithersburg: NIST, 2024. 32 p.
4. ISO/IEC 27001:2022. Information security management systems — Requirements. Geneva: ISO, 2022. 19 p.
5. CIS Controls Version 8. Center for Internet Security. East Greenbush: CIS, 2021. 114 p.

Аналіз векторів загроз корпоративній безпеці засобами автоматизованого інструмента OSINT

УДК 004.056

Владислав Загороднюк[1], Артем Соколов[2]

Національний університет «Одеська політехніка»,
[1]10252811@stud.op.edu.ua, [2]sokolov.a.v@op.edu.ua

Експоненційне зростання обсягів даних з відкритих джерел вимагає перегляду підходів до забезпечення корпоративної кібербезпеки [1]. Традиційні методи моніторингу демонструють низьку ефективність, оскільки фізично не здатні впоратися з потоками інформації та генерують багато хибних тривог. Автоматизація підготовки кібератак зловмисниками зумовлює потребу в симетричних рішеннях, що робить превентивну стратегію безпеки критично важливим фундаментом для бізнесу [2].

Метою роботи є розробка автоматизованого інструмента OSINT, який використовує передові архітектури штучного інтелекту, зокрема багатоагентні моделі та Retrieval-Augmented Generation (RAG), для виявлення та комплексного аналізу векторів загроз.

До ключових векторів загроз належать: 1) експлуатація зовнішньої поверхні атаки (тіньове IT); 2) глибоке ШІ-профілювання для атак соціальної інженерії; 3) масові витоки конфіденційних даних у публічних репозиторіях.

Наукова новизна дослідження полягає в інтеграції багатоагентної архітектури LangGraph із великою мовною моделлю Gemini 3.1, яка виступає як

центральне когнітивне ядро для оркестрації розвідувального циклу [3]. Запропоновано гібридну математичну модель кількісної оцінки кіберризику (CRQ), що поєднує детерміновані метрики з методами неконтрольованого та ансамблевого машинного навчання [4].

Застосунок реалізовано мовою Python (FastAPI, Celery, Redis). Конвеєр обробки даних включає три автономні ШІ-агенти: *розвідник* (збір даних про субдомени), *агент збагачення* (мапування вразливостей через API Shodan і Censys) та *агент оцінки* (підсумковий аналіз за парадигмою ReAct). Модуль RAG здійснює семантичний пошук у векторній базі FAISS, що містить звіти Threat Intelligence, унеможливлюючи алгоритмічні галюцинації моделі.

Математична модель обчислює загальний показник кіберризику R_i на основі комбінації задокументованих вразливостей, частоти спроб атак (TEF), базової оцінки втрат від компрометації активу, динамічного коефіцієнта критичності, а також коригувального фактора впливу алгоритмів машинного навчання F_{ML}. Для розрахунку фактора F_{ML} інтегровано алгоритм Gradient Boosted Decision Trees (GBDT) для класифікації активів та просторову кластеризацію DBSCAN для детектування аномалій тіньового ІТ.

На основі контрольної вибірки з понад 70 000 записів визначено вагові коефіцієнти моделі. Для забезпечення прозорості рішень (Explainable AI) побудовано графік важливості ознак алгоритму GBDT (рис. 1). Він дозволяє кількісно оцінити вплив конкретних технічних артефактів (вразливостей, відкритих портів) на формування коригувального фактора F_{ML} у загальній моделі оцінки кіберризику.

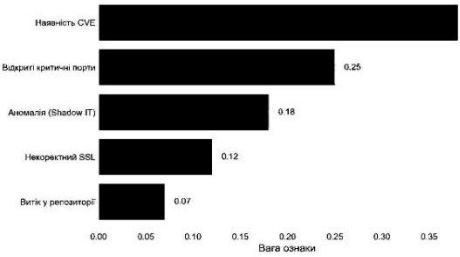

Рис.1. Графік важливості ознак

Аналіз графіка показує, що найбільш вагомим фактором ризику є наявність зафіксованих CVE (вага 0,38), тоді як відкриті критичні порти (0,25) та виявлені аномалії тіньового ІТ (0,18) посідають наступні за значущістю позиції. Для порівняння, лінійні моделі, такі як логістична регресія, продемонстрували значно гірші показники класифікації (F1-score на рівні 0,74) через нездатність ефективно фіксувати складні приховані зв'язки між технічними атрибутами мережевих активів [4]. Водночас алгоритм GBDT забезпечив мінімізацію хибних тривог завдяки вбудованим механізмам роботи з фрагментарними даними та інформаційним шумом.

Наскрізне тестування розробленого прототипу на прикладі реальної інфраструктури (домен op.edu.ua) підтвердило високу стабільність та

обчислювальну потужність архітектури, яка здатна безперебійно обробляти до 10 000 атомарних OSINT-запитів на годину. Завдяки синергії математичної моделі та інтелектуальних агентів, експериментальна точність ідентифікації загроз досягла 93,3%, а інтегральний показник F1-score склав 0,92. Крім того, автоматизація повного життєвого циклу розвідки дозволила скоротити час обробки 1 ГБ неструктурованих даних з 2-4 годин до 5-10 хвилин (приріст швидкодії у 12-48 разів).

Отже, такий підхід суттєво зменшує навантаження на аналітиків Security Operations Center (SOC) під час ручного сортування подій (на 58%) та допомагає автоматично формувати конкретні рекомендації щодо захисту периметра, забезпечуючи ефективний перехід компаній до проактивного управління корпоративними кіберризиками.

1. Ланде Д. В. OSINT у кібербезпеці : навч. посіб. Київ: ТОВ «Інжиніринг», 2024. 522 с.
2. Рибка Д. OSINT у забезпеченні національної безпеки. Науковий вісник Ужгородського національного університету. Серія: Право. 2023. Вип. 78. С. 344-348.
3. Фролов Д. І., Дягілєва М. С. Застосування технологій машинного навчання в кібербезпеці. Радіоелектроніка та молодь у XXI столітті. Харків : ХНУРЕ, 2025. №4. С. 97–99.
4. Чевардін В. Є., Юрченко О. В., Залужний О. В. Аналіз конкурентних атак на моделі машинного навчання систем кіберзахисту. Системи і технології зв'язку, інформатизації та кібербезпеки. 2023. №4. С. 9-15.

Метод шифрування на основі збільшення кількості модулів у системі залишкових класів

УДК 004.056.55

Віктор Залізняк[1], Павло Басістий[2], Михайло Касянчук[3]

[1, 3]Західноукраїнський національний університет,
[2]Тернопільський національний педагогічний університет
імені Володимира Гнатюка,
[1]viktor.zalizniak@gmail.com, [2]basi@ukr.net, [3]kasyanchuk@ukr.net

У сучасних криптографічних системах важливим завданням є підвищення стійкості алгоритмів шифрування без істотного зниження їхньої продуктивності [1]. Одним із перспективних напрямів розв’язання цієї задачі є використання системи залишкових класів (СЗК), яка дає змогу подавати числові дані у вигляді набору залишків за системою попарно взаємно простих модулів [2]. Такий підхід забезпечує незалежність обчислень за кожним модулем і створює передумови для побудови швидкодіючих криптографічних перетворень.

Класичне шифрування в СЗК ґрунтується на представленні відкритого тексту як набору залишків та подальшому відновленні відповідного десяткового числа за допомогою китайської теореми про залишки (КТЗ). У такій схемі модулі є ключами, а криптостійкість істотно залежить від складності їх