МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
УКРАЇНИ "КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ
ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"

НАВЧАЛЬНО-НАУКОВИЙ
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

THEORETICAL AND APPLIED CYBERSECURITY

**Матеріали другої Всеукраїнської
науково-практичної конференції**

Випуск 2

Київ – 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ "КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"

НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

THEORETICAL AND APPLIED CYBERSECURITY

Матеріали другої Всеукраїнської науково-практичної конференції

Випуск 2

Київ – 2024

Рекомендовано до друку Вченою радою
КПІ ім. Ігоря Сікорського
(протокол № 14 від 12 червня 2024 р.)

Theoretical and Applied Cybersecurity. Матеріали другої всеукраїнської науково-практичної конференції (TACS-2024). – Київ: Інжиніринг. – 190 с. ISBN 978-966-2344-98-1

До збірника увійшли матеріали доповідей, представлених на другій всеукраїнській науково-практичній конференції Theoretical and Applied Cybersecurity (TACS-2024, 30 травня 2024 року, м. Київ, Україна).

У збірнику представлені матеріали, присвячені питанням кібернетичної безпеки критичних інфраструктур, моделювання та протидії інформаційним операціям, технологій інформаційно-аналітичних досліджень на основі відкритих джерел інформації. Наведені матеріали з актуальних проблем інформаційної та кібернетичної безпеки, можливості застосування штучного інтелекту, системного аналізу при забезпеченні підтримки прийняття рішень, комп'ютерному моделюванні процесів і систем, актуальні завдання забезпечення інформаційної та кібербезпеки.

Для фахівців в області інформаційних технологій, інформаційної і кібернетичної безпеки, а також для аспірантів і студентів старших курсів вищої школи відповідних спеціальностей.

ISBN 978-966-2344-98-1

МЕТОД РЕАЛІЗАЦІЇ ВЕНТИЛЯ ТОФФОЛІ НА ОСНОВІ ВЕНТИЛЯ МАРГОЛУСА НА ЧОТИРЬОХ І БІЛЬШЕ КУБІТАХ

А.М. Терещенко, В.К. Задірака

Інститут кібернетики ім. В.М. Глушкова
НАН України,
teramidi@ukr.net, zvk140@ukr.net

У даній роботі розглядається метод покрокової компенсації поворотів фаз, який трансформує модифікацію вентиля Марголуса до схеми реалізації вентиля Тоффолі. Розглянутий метод дозволяє будувати схеми реалізації вентиля Тоффолі на чотирьох і більше кубітах.

Вступ

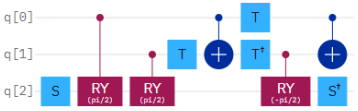
На даний час розроблено багато алгоритмів [1-2], які є ефективними для послідовної та паралельної моделі обчислень. Універсальним інструментом для задачі переносу класичних алгоритмів [3], включаючи реалізації операцій багаторозрядної арифметики, у квантову модель обчислень є вентиль Тоффолі. Комбінуючи різні модифікації вентиля Тоффолі, необхідно звертати увагу на поворот фази, який є основною відмінністю реалізацій квантових алгоритмів від класичних алгоритмів, та який має вплив на результат всієї схеми, що не є бажаним. У роботі розглянуто метод побудови вентиля Тоффолі на чотирьох і більше кубітах. Частиною цього методу є покроковий метод корегування повороту фази модифікації реалізації вентиля Марголуса.

Реалізація вентиля Тоффолі на трьох кубітах

Існує багато реалізацій вентиля Тоффолі з використанням різних базових вентилів. Авторами була досліджена схема реалізації, яка надана на рис. 1. З таблиці видно, що початкові стани кубітів $|0\rangle$ та $|1\rangle$ після обчислення схеми будуть також $|0\rangle$ та $|1\rangle$. Якщо у разі виконання реалізації схеми з'являються інші стани, наприклад, такі, як $|i\rangle$, $|-i\rangle$,

$|-1\rangle$ та інші, то це означає, що результат обчислення схеми має поворот фази для такого початкового стану.

Реалізація, яка побудована на основі п‘яти двокубітних вентилів, як, наприклад на Рис. 1, вважається оптимальною реалізацією. Вентилі S, S‘, T, T‘ використовуються для компенсації повороту фази результату обчислення схеми.



$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

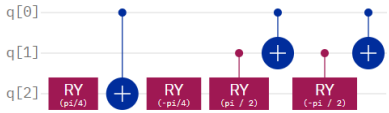
Рис. 1. Схема реалізації вентиля Тоффолі на основі венитлів CRY, CX, S, S‘, T, T‘ та представленням вентиля Тоффолі у матричному вигляді

Схема на рис. 1 не є зручною для побудови вентиля Тоффолі більшого порядку. Це пов‘язано з тим, що двокубітні вентилі CRY та CX поєднують різні пари кубітів (0-1 (CX), 0-2 (CRY), 1-2 (CRY)).

Реалізація на основі вентиля Марголуса

Зробимо заміну вентиля 0-2 (CRY) на рис. 1 вентилями $\mathrm{RY}(\pi/4)$, CX, $\mathrm{RY}(-\pi/4)$ та отримаємо модифікацію Марголуса [4], яка відрізняється від реалізації вентиля Тоффолі тим, що результат схеми обчислення початкової комбінації $|101\rangle$ має поворот фази на π (або $-\pi$). Повороту фази на π у матричному вигляді відповідає значення -1 на Рис. 2.

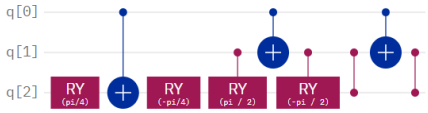
Лема 1. Компенсація повороту фази на π модифікації реалізації вентиля Марголуса на основі трьох пар вентилів CY, CRY, CX для початкового стану $|101\rangle$ може бути виконана за допомогою пари вентилів CZ, вентилів S та S‘, пари вентилів T (поворот фази на $\pi/4$), та одного вентиля T‘ (поворот фази на $-\pi/4$).



$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Рис. 2. Схема реалізації вентиля Марголуса на основі пар венитлів RY, CRY, CX та представленням вентиля Марголуса у матричному вигляді

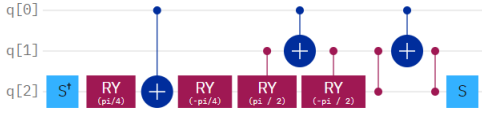
Доведення. Компенсацію повороту фази на π для початкового стану $|101\rangle$ (рис. 2) можна зробити за три кроки. На першому кроці додаймо вентилі CZ, як показано на Рис. 3, що дає змогу перенести поворот фази результату з початкового стану $|101\rangle$ до стану $|011\rangle$.



$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Рис. 3. Схема реалізації вентиля Марголуса з переносом повороту фази результату зі стану $|101\rangle$ до стану $|011\rangle$ та представленням у матричному вигляді

На другому кроці після додавання вентилів S та S‘ поворот фази “розподіляється” на станах $|011\rangle$ та $|111\rangle$ з поворотом фази на $3\pi/2$, що відповідає значенню $-i$ у матричному представленні на рис. 4.



$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -i \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -i & 0 & 0 & 0 & 0 \end{bmatrix}$$

Рис. 4. Схема реалізації вентиля Марголуса з переносом повороту фази результату до станів $|011\rangle$ та $|111\rangle$ та представленням у матричному вигляді

На третьому кроці відбувається остаточне корегування за рахунок додавання пари вентилів T та одного вентиля T‘. Отримуємо модифікацію на Рис. 5, в результаті якої відсутні повороти фаз для всіх початкових станів.

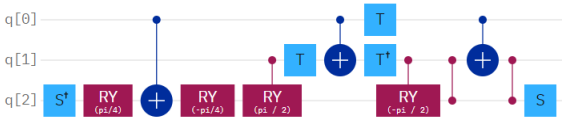


Рис. 5. Схеми реалізації вентиля Тоффолі на основі вентиля Марголуса

Лему доведено.

Реалізація вентиля Тоффолі на чотирьох кубітах

Зробимо заміну вентилів CX на рис. 2 вентилями CCX (вентилі Тоффолі) та отримаємо модифікацію реалізації вентиля Марголуса на чотирьох кубітах, для якої присутній поворот фази для початкового стану $|1011\rangle$.

Лема 2. Компенсація повороту фази на π модифікації реалізації вентиля Марголуса на основі трьох пар вентилів CY, CRY, CX для початкового стану $|1011\rangle$ може бути виконана за допомогою пари вентилів CZ, вентилів S та S‘, пари вентилів CX, вентилів T та T‘, пари вентилів P($\pi/8$) та вентиля P($-\pi/8$).

На Рис. 6 послідовне додавання вентилів виділене прямокутниками різного кольору для компенсації фази.

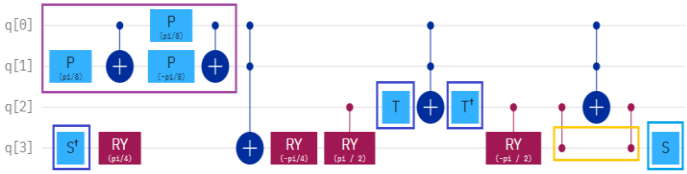


Рис. 6. Схеми реалізації вентиля Тоффолі на основі вентиля Марголуса на чотирьох кубітах

Порівнюючи Рис. 5 та Рис. 6 можна побачити, що один вентиль T замінено групою вентилів, які виділені прямо-

кутником у лівому верхньому куті на рис. 6. Компенсація повороту фази вже складається з чотирьох кроків. На першому кроці додаються вентилі CZ з поворотом фази на π, на другому кроці додаються вентилі S та S‘ з поворотом фази на $\pi/2$ та $-\pi/2$, на третьому кроці додаються вентилі T та T‘ з поворотом фази на $\pi/4$ та $-\pi/4$, на четвертому кроці додаються вентилі P з поворотом фази на $\pi/8$ та $-\pi/8$. Таким чином, можна описати загальний метод.

Метод побудови N-кубітної схеми реалізації вентиля Тоффолі на основі вентиля Марголуса

Вентиль Марголуса. Для отримання N-кубітної схеми вентиля Марголуса зробимо заміну вентилів CX на рис. 2 вентилями C…CX (N–1-кубітні схеми вентиля Тоффолі). Для такої модифікації присутній поворот фази тільки для початкового стану $|101\ldots1\rangle$, де три крапки позначають N–4 одиниці. Далі використовується наступний метод.

Метод компенсації повороту фази для початкового стану $|101\ldots1\rangle$. На кожному кроці додається пара вентилів з однаковими за значенням $\pi/2^{s-1}$ (де s – номер кроку, починаючи з одиниці), але протилежними за знаком значення повороту фази. Хоча на першому кроці додається пара вентилів CZ, можна вважати, що повороти на π та $-\pi$ є тотожними для вентиля CZ в такому сенсі. На остатньому кроці замість пари додається три вентиля, де два вентиля мають позитивне значення фази, а один – негативне. Загалом компенсація повороту фази потребує 2N+1 додаткових вентилів: CZ, S, S‘, T, …, $P(\pi/2^{N-1})$, $P(-\pi/2^{N-1})$, де CZ є двокубітними вентилями, а решта – однокубітні вентилі.

Зауваження. Для реалізація вентиля Тоффолі на чотирьох кубітах необхідна додаткова пара вентилів CX (рис. 6), а для реалізації на п‘ятьох кубітах окрім пари CX, необхідна пара CCX (рис. 7) і т.д. Якщо у реалізації схеми CCX (вентиль Тоффолі) присутні вентилі CX для такої ж самої пари кубітів, то ця частина схеми може бути оптимізована і не потребує додаткової пари вентилів CX. Аналогічним чином, якщо у реалізації схеми CCCX (вентиль Тоффолі на

4 кубітах) присутні вентилі CCX, то у цій частини схеми оптимізація може бути проведена таким чином, що не буде потребувати додаткової пари вентилів CCX. Але така оптимізації у рамках даної роботі не розглядається.

Використаємо метод для реалізації вентиля Тоффолі на п‘ятьох кубітах.

Реалізація вентиля Тоффолі на п‘ятьох кубітах

Для отримання 5-кубітної схеми реалізації вентиля Марголуса зробимо заміну вентилів CX на рис. 2 вентилями CCCX. Компенсація повороту фази буде складатися з п‘яти кроків, де на остатньому кроці будуть додаватися три вентилі з поворотом фази на $\pi/16$ та $-\pi/16$, як показано на Рис. 7.

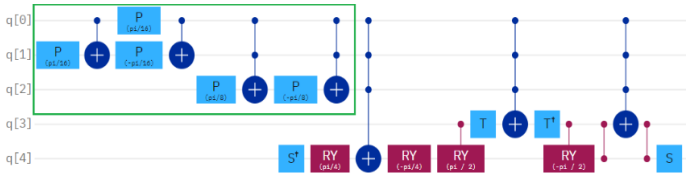


Рис. 7. Схеми реалізації вентиля Тоффолі на п‘ятьох кубітах

На рис. 7 зеленим прямокутником показано остатні два кроки компенсації повороту фази. Зауважимо, що у зеленому прямокутнику є пари вентилів CX та CCX.

Висновок

У даній роботі розглянуто метод побудови вентиля Тоффолі на основі вентиля Марголуса на чотирьох і більше кубітах. Запропоновано будувати вентиль Тоффолі на основі модифікації вентиля Марголуса, яка використовує три пари вентилів RY, CRY, CX. Вентилі більших порядків будуються заміною вентилів CX вентилями CCX для схеми на чотирьох кубітах, CCCX – для схеми на п‘яти кубітах і т.д. Розглянуто метод компенсації повороту фази результату обчислення початкового стану вигляду $|101 \ldots 1\rangle$, де три крапки позначають N–4 одиниць (N>3). Показано, що для ком-

пенсації повороту фази для реалізації вентиля на N кубітах необхідно 2N+1 додаткових вентилів, два з яких є двокубітними, та може бути виконана за N послідовних кроків, де на кожному кроці додаються вентилі з поворотами фаз $\pm\pi/2^{s-1}$, де s – номер кроку, починаючи з одиниці. Результати роботи протестовані за допомогою квантового сумилятора IBM [5].

Перелік використаних джерел

1. Zadiraka, V.K., Tereshchenko, A.M. Calculating the Sum of Multidigit Values in a Parallel Computational Model. Cybernetics and Systems Analysis. 2022. № 58. P. 473–480.

2. A. Tereshchenko, V. Zadiraka, “Algorithm for calculation the carry and borrow signs in multi-digit operations in the parallel computational model”, International Journal of Computing, 22(1), 21-28. (2023).

3. Draper, T. G. (2000). Addition on a quantum computer. arXiv preprint quant-ph/0008033.

4. Barenco, Adriano; Bennett, Charles H.; Cleve, Richard; DiVincenzo, David P.; Margolus, Norman; Shor, Peter; Sleator, Tycho; Smolin, John A.; Weinfurter, Harald (1995-11-01). "Elementary gates for quantum computation". Physical Review A. 52 (5). American Physical Society (APS): 3457–3467. arXiv:quant-ph/9503016.

5. https://quantum.ibm.com/composer

ВИЗНАЧЕННЯ КОЕФІЦІЄНТІВ ЛОГІКО-ЙМОВІРНІСНИХ МОДЕЛЕЙ КІБЕРБЕЗПЕКИ З ВИКОРИСТАННЯМ ВІРТУАЛЬНИХ ЕКСПЕРТІВ

Д.В. Ланде, О.М. Новіков, Л.Б. Алексейчук

Національний технічний університет України
«Київський політехнічний інститут ім. Ігоря Сікорського»,
Київ, Україна
d.lande@kpi.ua

У роботі розглянуто питання моделювання загроз та аналіз ризиків для об'єктів критичної інфраструктури, зокрема, логіко-ймовірнісний метод для моделювання небезпечних станів і оцінки ризиків. Зроблено акцент на коректному визначенні ймовірностей переходів у мережах за допомогою генеративного штучного інтелекту. Запропоновано дві стратегії оцінки параметрів мережі: Output-алгоритм і Input-алгоритм, результати яких було порівняно за допомогою міри Фробеніуса, що підтвердило високу кореляцію отриманих матриць та їх узгодженість.
Ключові слова: логіко-ймовірнісна модель, критична інфраструктура, оцінка ризиків, штучний інтелект.

Вступ

Ефективним напрямком досліджень у сфері кібербезпеки є моделювання загроз та аналіз ризиків. Зокрема, задачі моделювання загроз, аналізу кібербезпеки та інші аспекти безпеки об’єктів критичної інфраструктури було розглянуто в роботах [1, 2] та інших.

Одним з напрямків вирішення задач моделювання загроз та аналізу ризиків об’єктів критичної інфраструктури є логіко-ймовірнісній метод, вперше запропонований англійським вченим Дж. Булем [3]. Логіко-ймовірнісний метод полягає у розробці моделі функції небезпечного стану із застосуванням операцій булевої алгебри з подальшим використанням теорії ймовірності. У роботах [4, 5] у якості об’єкту розвитку небажаної події

розглядалась система кіберзахисту інформаційно-комунікаційної системи, яка перебуває під впливом кібератак.

Важливим у питанням розробці та застосуванні логіко-ймовірнісних моделей є коректне та точне визначення їх коефіцієнтів. В роботах з теорії логіко-ймовірнісного моделювання це питання, частіше за все, залишається поза розглядом. Разом з цим, для визначення коефіцієнтів логіко-ймовірнісних моделей ІКС можна використовувати статистичні методи, методи, які враховують структуру мережі, методи машинного навчання і методи експертного оцінювання.

Статистичні методи базуються на спостереженні за мережевим трафіком протягом певного періоду часу. На основі історичних даних підраховуються частоти переходів між серверами, що дозволяє визначити коефіцієнти.

Методи, які враховують структуру мережі можуть дати уявлення про те, які сервери, ймовірно, будуть зв'язані між собою. Зокрема, метод Монте-Карло використовується для оцінки ймовірностей переходів шляхом випадкового генерування великої кількості можливих шляхів і аналізу результатів.

Методи машинного навчання традиційно використовують для прогнозування трафіку в мережах, ймовірностей переходів на основі попередніх даних можуть застосовуватись нейронні мережі та LSTM. Ці методи можуть бути використані для прогнозування ймовірностей переходів на основі попередніх даних.

Методи експертного оцінювання можна використовувати для оцінки ймовірностей переходів у мережах серверів в умовах, коли доступні дані обмежені, неможливості врахувати трафік в реальній системі, коли історичні дані недостатні або не повністю відображають всі можливі стани і переходи в мережі, коли розглядаються системи з великою кількістю зв’язків різного рівня, де автоматичні методи можуть бути занадто складними. Серед відомих методів експертних оцінок можна назвати методи експертних опитувань, дельфійський метод, метод аналізу ієрархій, метод байєсовських мереж, тощо.

Мета дослідження. Метою роботи є представлення методології визначення ймовірностей переходів у мережах методів експертного опитування віртуальних експертів з використанням генеративного штучного інтелекту для визначення.

Опис методології. У цій роботі зупинимось саме на методі експертних опитувань, тобто залучення групи експертів для надання оцінок ймовірностей переходів на основі їхнього досвіду і знань. Для усереднення, досягнення консенсусу між експертами будемо застосовувати дельфійський підхід, в рамках якого група експертів незалежно оцінює ймовірності, а потім переглядає свої оцінки на основі узагальнених результатів. Будемо розглядати так званих «віртуальних експертів», які моделюються засобами генеративного штучного інтелекту [6].

Для оцінювання параметрів мережі пропонується застосування різних моделей генеративного штучного інтелекту, які реалізують «віртуальних експертів» [6]. На базі їх відповідей на спеціальні запити (промпти), що стосуються суті мережевих зв'язків, оцінюються ймовірності переходів за цими зв'язками.

Задача ставиться таким чином: нехай існує мережа з направленими зв'язками, вузли якої відповідають деяким серверам мережі. Відповідно до призначення вузлів і напрямків зв'язку необхідно надати експертні оцінки значень ймовірностей переходів.

Для оцінки цих ймовірностей і подальшого усереднення їх результатів можливо дві стратегії.

Перша стратегія полягає в оцінці зв'язків, що виходять із вузлів мережі. Для цього перебираються всі вузли мережі і запитуються ймовірності переходу від них по всім наявним вихідним зв'язкам. Такий підхід назвемо **Output**-алгоритмом.

Інший, протилежний підхід полягає у розгляданні всіх зв'язків, що входять в кожний вузол мережі і оцінювання ймовірностей входження за кожним із цих зв'язків. Такий підхід назвемо **Input**-алгоритмом.

Для розглянутих прикладів оцінюється міра взаємної близькості матриць зв'язків (*Output* та *Input*), що відповідають мережі, за Фробеніусом, показується що ця міра менше ніж близькість з випадковою матрицею, з матрицею суміжності.

Після отримання оцінок всіх ймовірностей за цими двома алгоритмами отримуються дві матриці, відповідні значення яких можна усереднити і надати як загальний результат експертної оцінки (у відповідності узгодженості цих матриць).

Для опису логічної структури інформаційно-комунікаційної системи використаємо орієнтований граф $G(V,E)$, де $v_i \in V$ - множина об'єктів/інформаційних ресурсів/сервісів системи, $E = (e_1,...,e_L)$, $e_k = (v_i, v_j)$ - наявність чи відсутність зав'язків між ними, $E \subseteq V \times V$ та $e_i \in E$.

Якщо на одному фізичному сервері розміщується декілька сервісів, що можуть бути об'єктами, джерелами загроз або через них можуть проходити сценарії атак, то будемо виділяти їх в окремі об'єкти - v_i. Отриманий граф $G(V,E)$ будемо представляти у вигляді матриці суміжності, яку називають матрицею доступності об'єктів. Граф буде орієнтованим тому що з деяких об'єктів можна ініціювати з'єднання тільки в односторонньому порядку.

Логіко-ймовірніснісну модель такої системи було запропоновано:

$$J(A) = P(G, A, O, P),$$

Де $J(A)$ - критерій ймовірності успішності сценарію атаки,

$G(V,E)$ - відома та фіксована топологія мережі,

$V = \{v_1,...,v_N\}$ – множина об'єктів/ресурсів/сервісів у ІКС,

$A = \{a_1,...,a_K\} \subset V$ - множина джерел загроз,

$O = \{o_1,...,o_M\} \subset V$ - множина критичних об'єктів для атак,

$P = \{P_1, \ldots, P_N\}$ - ймовірності захоплення об'єктів ІКС.

Саме для оцінки значень пропонується підхід оцінки перехідних ймовірностей за допомогою множини віртуальних експертів».

Розглянемо мережу з вузлами (Рис. 1):

Firewall - S1, Mail Server - S2, Web Server - S3, AWP Administrator – S4, AWP Clients - S5, Application Server - S6, DB Server – S7.

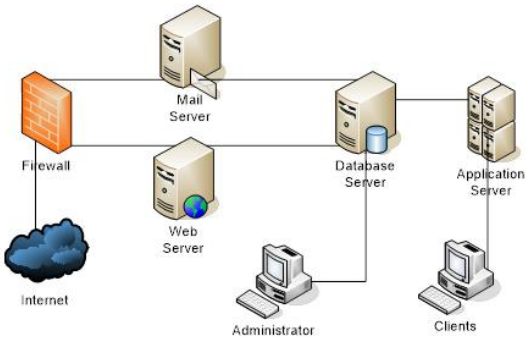


Рисунок 1 – Приклад мережі [5]

Ці вузли зв'язані між собою спрямованим зв'язками, яким відповідає матриця суміжності, елементами якої можуть бути 0 і 1 (Таблиця 1).

Таблиця 1 - комунікації (Links)

	S1	S2	S3	S4	S5	S6	S7
Firewall (S1)	0	1	1	0	0	0	0
Mail Server (S2)	1	0	0	0	0	0	1
Web Server (S3)	1	0	0	0	0	0	1
AWP Administrator (S4)	1	1	1	0	1	1	1
AWP Clients (S5)	0	0	0	0	0	1	0
Application Server (S6)	0	0	0	0	1	0	1
DB Server (S7)	0	0	0	0	0	1	0

При застосуванні методології «віртуальних експертів» здійснюється звернення до сервісів генеративного штучного інтелекту ChatGPT https://chat.openai.com/, Gemini (https://gemini.google.com/), Groq (https://groq.com/). Надалі для оцінки значень параметрів системи багатократно надаються запити (промпти), які після цього усереднюються.

Оцінка параметрів на основі алгоритму Output

Послідовно для всіх вузлів мережі, з яких виходять зв'язки, виконуються промпти, результати виконання яких усереднюються:

Промпт 1 (p12=P(S1->S2), p13=P(S1->S3)):

Нехай відбулось проникнення у корпоративну мережу через фейрвол, зловмисники хочуть досягти сервера баз даних. Кількісно оцініть умовну ймовірність того, що вони пройшли від фейрволу до поштового сервера – p12, до веб-сервера – p13. Надайте експертні чисельні значення умовних ймовірностей p12, p13.

Аналогічним чином формуються промпти 2 – 5.

В результаті отримання результатів виконання промптів від систем штучного інтелекту отримані параметри мережі, якій відповідає така таблиця умовних ймовірностей (матриця Output):

	S1	S2	S3	S4	S5	S6	S7
Firewall (S1)	0	0.4	0.5	0	0	0	0
Mail Server S2)	0.28	0	0	0	0	0	0.78
Web Server (S3)	0.27	0	0	0	0	0	0.75
AWP Administrator (S4)	0.55	0.55	0.55	0	0.55	0.23	0.65
AWP Clients (S5)	0	0	0	0	0	1	0
Application Server (S6)	0	0	0	0	0.29	0	0.66
DB Server (S7)	0	0	0	0	0	1	0

Оцінка параметрів на основі алгоритму Input:

Послідовно для всіх вузлів мережі, у які входять зв'язки, виконуються промпти, результати виконання яких усереднюються:

Промпт 1 (p21=P(S2->S1), p31=P(S3->S1),

p41=P(S4->S1)):

Нехай відбулось проникнення у корпоративну мережу, зловмисники хочуть досягти сервера баз даних. Відомо, що йде звернення до фейрволу із внутрішнього сегменту. Кількісно оцініть умовну ймовірність того, звернення до фейрволу йде від поштового сервера (p21), від веб-сервера (p31), від сервера адміністратора (p41). Надайте експертні чисельні значення умовних ймовірностей p21, p31, p41.

Аналогічним чином формуються промпти 2 – 6.

Таблиця умовних ймовірностей (Input):

	S1	S2	S3	S4	S5	S6	S7
Firewall (S1)	0	0.34	0.3	0	0	0	0
Mail Server (S2)	0.28	0	0	0	0	0	0.25
Web Server (S3)	0.38	0	0	0	0	0	0.3
AWP Administrator (S4)	0.4	0.36	0.35	0	0.44	0.35	0.65
AWP Clients (S5)	0	0	0	0	0	0.4	0
Application Server (S6)	0	0	0	0	0.59	0	0.5
DB Server (S7)	0	0	0	0	0	0.38	0

Оцінка близькості отриманих матриць

Оцінка міри близькості дозволяє нам побачити, наскільки отримані матриці корельовано між собою, і наскільки вони відрізняються від випадкової матриці і матриці комунікацій. Для проведення розрахунків отримані матриці нормуються (їх значення будуть варіюватись від 0 до 1) шляхом ділення всіх елементів на найбільший. У

даному випадку застосовується норма Фробеніуса $\|\cdot\|_F$, що дорівнює кореню квадратному із суми квадратів різниць всіх елементів відповідних матриць:

$$\|A, B\|_F = \sqrt{\sum_{i,j}(a_{ij} - b_{ij})^2}.$$

В процесі попарного порівняння застосовувались такі матриці:

Output – таблиця умовних ймовірностей, отримана за алгоритмом Output;

Input – таблиця умовних ймовірностей, отримана за алгоритмом Input;

Links – таблиця комунікацій;

Random – випадкова матриця.

У результаті розрахунків (Таблиця 2) виявилося, що матриці Output та Input зв'язані між собою сильніше всього, що свідчить про їх узгодженість, тобто коректності застосування методу.

Таблиця 2 – результати взаємного порівняння матриць.

Матриця 1	Матриця 2	Норма Фробеніуса, різниці матриць
Output	*Input*	0,167
Output	*Links*	0,248
Intput	*Links*	0,286
$\frac{Output + Input}{2}$	*Links*	0,211
Output	*Random*	0,407
Input	*Random*	0,520

Наведена таблиця, отримана у результаті нормування відповідних матриць і розрахунку міри Фробеніуса, свідчить щодо високої кореляції отриманих матриць Output та Input, а також можливості використання їх середніх значень, які дають результати найбільш корельовано з вихідною комунікаційною матрицею.

Висновки

Логіко-ймовірнісний метод є ефективним інструментом для моделювання загроз і аналізу ризиків, що дозволяє створювати моделі, які враховують ймовірності розвитку небажаних подій внаслідок зовнішніх впливів. Проте коректне визначення коефіцієнтів для таких моделей залишалось проблемним питанням.

Запропонований підхід із залученням множини віртуальних експертів, створених засобами генеративного штучного інтелекту, показав свою ефективність. Віртуальні експерти дозволяють оперативно та надійно оцінити ймовірності переходів у мережах навіть за відсутності повних історичних даних.

Два алгоритми оцінки ймовірностей переходів – Output та Input – показали узгодженість результатів, що підтверджує коректність методу. Попарне порівняння матриць, отриманих за цими алгоритмами, з матрицею комунікацій та випадковою матрицею виявило високий рівень їх подібності, що свідчить про надійність запропонованого підходу.

Таким чином, запропоновані методи експертного оцінювання за участі віртуальних експертів відкривають нові можливості для оперативного аналізу ризиків.

Перелік використаних джерел

1. Dinesh Kumar Saini. Cyber Defense: Mathematical Modeling and Simulation. International Journal of Applied Physics and Mathematics, Vol. 2, No. 5, September 2012, pp. 312-315. DOI: http://dx.doi.org/10.7763/IJAPM.2012.V2.121

2. Juan Fernando Balarezo, Song Wang, Karina Gomez Chavez, Akram Al-Hourani, Sithamparanathan Kandeepan A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. Engineering Science and Technology, an International Journal, Vol. 31, July 2022, 15 p. DOI: http://dx.doi.org/10.1016/j.jestch.2021.09.011

3. Boole George. An investigation of the laws of thought, on which founded the mathematical theories of logic and

probabilities. London, 1854. - 343 p. Режим доступу: https://www.gutenberg.org/ebooks/15114

4. L. Alekseichuk, O. Novikov, A. Rodionov, D. Yakobchuk Cyber Security Logical and Probabilistic Model of a Critical Infrastructure Facility in the Electric Energy Industry // Theoretical And Applied Cybersecurity - Vol.5 No. 1, 2023, pp. 61-66. DOI: https://doi.org/10.20535/tacs.2664-29132023.1.287365L

5. L. Alekseichuk, O. Novikov, A. Rodionov, D.Yakobchuk The Best Scenario of Cyber Attack Selecting on the Information and Communication System Based on the Logical and Probabilistic Method // Theoretical And Applied Cybersecurity. - Vol.5 No. 2, 2023, pp. 81-88. DOI: https://doi.org/10.20535/tacs.2664-29132023.2.288973

6. Dmytro Lande, Leonard Strashnoy. GPT Semantic Networking: A Dream of the Semantic Web - The Time is Now. - Kyiv: Engineering, 2023. - 168 p. ISBN 978-966-2344-94-3

ОСОБЛИВОСТІ ТРАНСФОРМАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ В УМОВАХ ВІЙНИ

Даник Ю.Г.[1], Валерій Шестаков В.І.[2]

[1]Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", м. Київ, Україна, zhvinau@ukr.net
[2]Національна академія Служби безпеки України, м. Київ, Україна, shvi_zt@ukr.net

У доповіді запропоновано результати диференційного аналізу державної політики у сфері кібербезпеки країн Європейського Союзу, НАТО, Китаю. Проаналізовано окремі нормативно-правові акти вітчизняного та закордонного законодавства, які визначають політику України, закордонних держав та їх союзів з кібербезпеки, регламентують діяльність суб'єктів системи забезпечення кібербезпеки. Окреслено пріоритетні напрями трансформації державної політики України у сфері кібербезпеки і кібероборони в умовах воєнних конфліктів з врахуванням досвіду відбиття широкомасштабної агресії рф проти України. Показано, що синергія кібердій відбувається у разі їх комплексної реалізації за єдиним замислом і планом, узгодженими за цілями, задачами, місцем та часом.

Ключові слова: кіберпростір, кібербезпека, кібероборона, кіберзагроза, кіберінцидент, державна політика кібербезпеки, національна система кібербезпеки.

Вступ

Розвиток інформаційних, телекомунікаційних, комп'ютерних технологій та їх конвергенція з технологіями штучного інтелекту приводить до зростання різноманітності форм та видів кіберзагроз. Одночасно зростають можливості, ефективність і ризики їх реалізації в інтересах деструктивних впливів на противника або в

злочинних цілях. Це, в свою чергу, вимагає розбудови та розвитку національних систем кібербезпеки і кібероборони та наддержавних структур реагування на кіберінцеденти.

Крім того, стійкою світовою тенденцією є перенесення протиборства в кіберпростір. Кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій. В провідних країнах світу набирає сили тенденція зі створення кіберкомандувань і кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі [1]. При цьому, виникає протиріччя між випереджаючим технологічним розвитком, який спричиняє появу нових та ускладнення існуючих кіберзагроз, веде до синергії різноманітних інформаційних та кібердій та рефлексивним виробленням важливих для суспільства рішень щодо формування та виконання завдань з кібербезпеки, пошуку шляхів адекватного реагування на кіберзагрози та зниження ризиків їх реалізації.

Особливості трансформації державної політики провідних країн у сфері кібербезпеки

З розширенням цифрового ландшафту та ускладненням кіберзагроз Європейський Союз (ЄС) поставив кібербезпеку на чільне місце у своєму політичному порядку денному. Спираючись на [2, 3], можна стверджувати, що ЄС досяг значних успіхів у розробці всеосяжної системи управління кібербезпекою, що охоплює правові, регуляторні та стратегічні аспекти. Політика ЄС спрямована на: створення добровільної схеми сертифікації кібербезпеки для хмарних сервісів [4]; посилення співпраці між країнами-членами ЄС у разі великих кібератак [5].

Незважаючи на відмінності в сутності, структурах і повноваженнях ЄС та НАТО, обидві організації розробили надійну політику кібербезпеки, щоб захистити цифрову інфраструктуру, критично важливі служби та підвищити стійкість до кіберзагроз.

У доповіді показано досвід із забезпечення кібербезпеки Естонії, яка прийняла цифровізацію, як основну

національну стратегію. Показано проблемні питання США щодо забезпечення безпеки свого кіберпростору. Акцентовано увагу, що політика кібербезпеки США прагне збалансувати потребу в безпеці із захистом громадянських свобод, наприклад, таких, як свобода слова та приватне життя. Стратегія Китаю в сфері кібербезпеки відображає складну взаємодію різних структур у вирішенні проблем національної безпеки, економічних амбіцій і еволюції соціальних норм у цифровій сфері. Китай наголошує на концепції суверенітету в Інтернеті, який надає уряду значний контроль над ресурсами мережі у межах своїх кордонів, регулювання онлайн-контенту, зокрема обмеження соціальних мереж.

Особливості трансформації державної політики України у сфері кібербезпеки в умовах повномасштабного вторгнення рф

Україна з 2014 року активно працює над забезпеченням кібербезпеки в умовах гібридної, а з 24.02.2022 повномасштабної агресії рф. Правову основу забезпечення кібербезпеки визначено в [6]. Один із ключових кроків щодо розбудови національної системи кібербезпеки було введення в дію Стратегії кібербезпеки України (Стратегія). Зокрема, в рамках Стратегії передбачено: уніфікацію підходів, методів і засобів забезпечення кібербезпеки з практиками ЄС та інших країн; розробку та впровадження Плану реалізації Стратегії кібербезпеки; наукове супроводження реалізації Стратегії.

У доповіді розглядається трансформація окремих із стратегічних цілей Стратегії, яка пов’язана з повномасштабним вторгнення рф. Акцентується увага на тому, що рф здійснює нанесення гібридних атак, які поєднують кіберскладову та ракетні удари. Із високою ймовірністю до гібридних атак віднесено кібератаку на компанію «Київстар» [7].

На основі [7] зазначається, що основними об’єктами кібератак є: провайдери телекомунікаційних та інтернет-послуг; інформаційні ресурси організацій сектору безпеки і

оборони; ресурси об'єктів кретичної інфраструктури; окремі комп'ютери та гаджети працівників/службовців таких структур. Однак, як зазначив Віце-прем'єр-міністр України з інновацій, розвитку освіти, науки та технологій — Міністр цифрової трансформації України Михайло Федоров: "Попри велику кількість атак, ворогу не вдалося вплинути на обороноздатність держави та позбавити населення життєво важливих послуг" [8].

Показано, що на сьогодення в інтересах кібероборони здійснюють діяльність спеціалізовані структури сил безпеки і оборони, бізнес-структури, громадські організації тощо. Із самого початку повномасштабного вторгнення рф почалися процеси самоорганізації волонтерів та інтернет-спільнот України в спільноти протидії агресії в / і через кіберпростір. У зв'язку із можливою загрозою переростання окремих груп Інтернет-спільнот, що набули певний досвід дій в кіберпросторі, в злочинні угрупування, залучення громадянського суспільства повинно координуватись та контролюватись суб'єктами системи кібербезпеки.

Висновки

За результатами досліджень можна стверджувати, що беззаперечним пріоритетом державної політики у сфері забезпечення кібербезпеки є і має бути подальша інтеграція в ЄС і НАТО. Для підвищення рівня кіберстійкості необхідно: посилювати співпрацю між усіма суб'єктами кібербезпеки, активно залучати до виконання завдань кібероборони громадянське суспільство, забезпечити координацію різних суб'єктів, що проводять кібердії на рівні Ставки Верховного Головнокомандувача Збройних Сил України; оновлювати законодавство відповідно до кращих світових стандартів; активізувати наукові дослідження питань з обґрунтування організаційно-правових засад забезпечення кібербезпеки, ведення кібероборони; постійно удосконалювати систему підготовки військових та цивільних фахівців з кібербезпеки і кібероборони.

Вирішення складних проблем кібербезпеки вимагає всебічного удосконалення та необхідних трансформацій державної політики у сфері забезпечення кібербезпеки, щодо розширення та поглиблення постійної співпраці і взаємодії Уряду України та всіх суб'єктів системи кібербезпеки між собою на міжвідомчому і загальнодержавному рівнях, на міждержавному та міжнародному рівнях, а також з представниками освіти, науки, промисловості та іншими зацікавленими стейкхолдерами сектору безпеки і оборони, економіки держави, громадянського суспільства тощо, при забезпеченні достатнього рівня необхідних інвестицій.

Список літератури

1. Стратегія кібербезпеки України. Затверджено Указом Президента України від 26 серпня 2021 року № 447/2021.
2. The EU Cybersecurity Act. Shaping Europe's digital future. URL: https://digital-strategy.ec.europa.eu/en/policies/cyberse curity-act (дата звернення: 22.05.2024).
3. Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555 (дата звернення: 22.05.2024).
4. EU Cyber Resilience Act. Shaping Europe's digital future. URL: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act (дата звернення: 22.05.2024).
5. Commission welcomes political agreement on Cyber Solidarity Act. European Commission - European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1332 (дата звернення: 22.05.2024).
6. Закон України "Про основні засади забезпечення кібербезпеки України"
7. Російські кібероперації аналітика за II півріччя 2023 року. https://cip.gov.ua/services/cm/api/attachment/download?id=64621&embedded=true&a=bi. (дата звернення: 22.05.2024).
8. Зараз триває перша у світі кібервійна. https://www.kmu.gov.ua/news/zaraz-tryvaie-persha-u-sviti-kiberviina-mykhailo-fedorov-na-mizhnarodnomu-forumi-z-kiberbezpeky (дата звернення: 22.05.2024).

ТЕХНОЛОГІЯ ІДЕНТИФІКАЦІЇ ПОЛІТИЧНОЇ СПРЯМОВАНОСТІ ДЖЕРЕЛ ІНФОРМАЦІЇ НА БАЗІ МАШИННОГО НАВЧАННЯ

Пучков О.О., Субач І.Ю., Рибак О.О.

Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна rybak.oleksandr01@gmail.com

Запропоновано інформаційну технологію для аналізу та визначення політичної спрямованості джерел інформації в Інтернеті та соціальних мережах. Використовуючи бібліотеку машинного навчання fastText, створюється модель для класифікації тексту. Інформаційна технологія містить модулі сканування, екстрагування сутностей (ключові слова, персони, локації, організації).

Ключові слова: соціальні медіа, машинне навчання, моніторинг, інформаційна технологія, штучний інтелект.

Вступ

Політична спрямованість джерела інформації впливає на спосіб подання контенту. Відкриті джерела, зокрема соціальні мережі, відіграють важливу роль у формуванні суспільної думки. Інформація з таких джерел може містити багато "сміття", але навіть на перший погляд нейтральний контент може містити прихований підтекст, сенс або ідею, яку прагне нав'язати певна сторона. Почута думка може вплинути на свідомість людини, змінюючи її ставлення до тієї чи іншої сторони. Отже, окремі джерела відкритої інформації можуть завдати різного ступеня шкоди.

Тому врахування інформації з соціальних медіа є важливим для забезпечення інформаційної безпеки особи, суспільства та держави.

Компоненти технології

1. Здійснюється збір інформації (сканування) з відкритих джерел, таких як месенджери, соціальні мережі та інші. Підсистема сканування реалізовується за допомогою мови програмування Python та її модулів, таких як Requests, Selenium та BeautifulSoup4 для зручного отримання інформації з вебсторінок.

2. Друга складова реалізує функції навчання моделі для автоматичного визначення політичної спрямованості каналів соціальних мереж. Для цього використовується бібліотека fastText[1], [2]., створена Лабораторією досліджень штучного інтелекту Facebook's AI Research lab [3][4]. fastText дозволяє створювати моделі та алгоритми машинного навчання для отримання векторних представлень слів, використовуючи нейронні мережі для представлення слів. Однак робота з бібліотекою fastText у випадку соціальних медіа, де публікації часто відбуваються двома мовами (українською та російською), не завжди дає точні результати. Тому для отримання більш точного визначення політичної направленості джерел здійснюється окреме навчання моделей для української та російської мов. Навчання моделей відбувається шляхом створення чотирьох словників: "проукраїнські", "антиукраїнські", "проросійські" та "антиросійські". За допомогою скрипту на Python перевіряється кожне повідомлення на кількість "позитивних" і "негативних" слів, розділяючи їх за пороговим значенням 90%. Повідомлення, які не досягають цього порогу, маркуються як нейтральні. Отримані дані використовуються для навчання двох моделей fastText: одна для української, інша для російської мови.

3. Визначення політичної направленості джерела інформації здійснюється шляхом аналізу маркованих повідомлень, що містяться у ньому. Для цього задається порогове значення класифікаційного правила. Наприклад, якщо кількість негативних повідомлень перевищує 70%, то джерело вважається негативним, тобто підтримуючим країну-агресора у нашому випадку. Джерела, спрямування яких важко визначити, маркуються як нейтральні. Після

визначення відсотку повідомлень з певним спрямуванням розраховується рейтинг джерел, від класифікацій найбільш негативних (які активно підтримують агресора та війну) до найменш негативних. Завдяки постійному моніторингу джерел і маркуванню їх повідомлень рейтинг можна розраховувати з більшою точністю.

Висновки

До цього часу у відкритому доступі не існувало засобів для автоматизованого визначення політичної спрямованості інформаційних ресурсів. У цій роботі розглянуто проблематику цього питання та запропоновано систему автоматичного визначення політичної спрямованості відкритих джерел інформації.

Розроблено методологію та інструментальні засоби, які включають комплекс програмних модулів для навчання моделей за допомогою бібліотеки fastText. Ці засоби дозволяють визначати політичне спрямування відкритих джерел інформації на основі сучасних нейромережевих технологій.

Перелік використаних джерел

1. P. Bojanowski, E. Grave, A. Joulin, T. Mikolov “Bag of Tricks for Efficient Text Classification”, 9 August 2016. [Online]. https://arxiv.org/abs/1607.01759

2. N. Badri, F. Kboubi, A. Chaibi, “Combining FastText and Glove Word Embedding for Offensive and Hate speech Text Detection”, 2022. [Online]. https://www.sciencedirect.com/science/article/pii/S1877050922010134

3. K. Ryan. “Facebook's New Open Source Software Can Learn 1 Billion Words in 10 Minutes”. August 19, 2016. [Online]. https://www.inc.com/kevin-j-ryan/facebook-open-source-fasttext-learns-1-billion-words-in-10-minutes.html

4. C. Low. “Facebook is open-sourcing its AI bot-building research”. August 18, 2016. [Online]. https://www.engadget.com/2016-08-18-facebook-open-sourcing-fasttext.html

ДИФЕРЕНЦІАЛЬНА АТАКА НА ШИФР IDEA НА ОСНОВІ ВЛАСТИВОСТЕЙ ЙОГО КЛЮЧОВОГО СУМАТОРА

Паршин О.Ю., Яковлєв С.В.

Навчально-науковий Фізико-технічний інститут,
КПІ ім. Ігоря Сікорського, Київ, Україна
parshin_o@ukr.net, yasv@rl.kiev.ua

У цій роботі пропонується нова, теоретична диференціальна атака на шифр IDEA. Одержано оцінки стійкості даного шифру до атак наведеного типу, а також запропоновано зміну в дизайні ключового суматора, яка дозволяє підвищити стійкість IDEA.

Ключові слова: блоковий шифр, схема Лая-Мессі, IDEA; диференціальний криптоаналіз

Вступ

Шифр IDEA є блоковим шифром, запропонованим С. Лаєм та Дж. Мессі у 1991 році [1]. Головною особливістю даного шифру є відсутність S-блоків; натомість, надійність забезпечується використанням складної раундової функції із спеціально підібраними різними алгебраїчними операціями [2]. У даній роботі розглядається побудова диференціальної атаки на класичний шифр IDEA, а також запропоновано зміну в дизайні ключового суматора, яка може покращити його стійкість до атак подібного типу.

Структура шифру IDEA

Шифр IDEA використовує три алгебраїчні операції, які традиційно позначаються як $\oplus$, $\boxplus$, $\odot$ – побітове додавання, додавання за модулем 2^{16} та множення за модулем $(2^{16}+1)$ (для останньої операції вважається, що число 0 відповідає значенню 2^{16}).

Шифр IDEA оперує 64-бітними блоками повідомлень та 128-бітним ключем шифрування. Один раунд шифрування має такий вид:

$$X^{(i)} = \left(X_1^{(i)}, X_2^{(i)}, X_3^{(i)}, X_4^{(i)}\right),$$
$$Y^{(i)} = \left(X_1^{(i)} \odot Z_1^{(i)}, X_2^{(i)} \boxplus Z_2^{(i)}, X_3^{(i)} \boxplus Z_3^{(i)}, X_4^{(i)} \odot Z_4^{(i)}\right), \textbf{(1)}$$

$$(n_i, q_i) = \left(Y_1^{(i)} \oplus Y_3^{(i)}, Y_2^{(i)} \oplus Y_4^{(i)}\right),$$
$$(r_i, s_i) = \left(s_i \boxplus \left(Z_5^{(i)} \odot n_i\right), \left(\left(Z_5^{(i)} \odot n_i\right) \boxplus q_i\right) \odot Z_6^{(i)}\right),$$
$$W^{(i)} = \left(Y_1^{(i)} \oplus s_i, Y_2^{(i)} \oplus r_i, Y_3^{(i)} \oplus s_i, Y_4^{(i)} \oplus r_i\right),$$
$$X^{(i+1)} = \left(W_1^{(i)} \oplus s_i, W_3^{(i)} \oplus s_i, W_2^{(i)} \oplus r_i, W_4^{(i)} \oplus r_i\right);$$

тут $Z_j^{(i)}$ – 16-бітові раундові ключі.

На останньому, восьмому раунді шифрування вихідне перетворення обчислюється як

$$X^{(9)} = \left(W_1^{(8)} \oplus s_8, W_2^{(8)} \oplus r_8, W_3^{(8)} \oplus s_8, W_4^{(8)} \oplus r_8\right),$$

і остаточно шифротекст одержується як

$$C = \left(X_1^{(9)} \odot Z_1^{(9)}, X_2^{(9)} \boxplus Z_2^{(9)}, X_3^{(9)} \boxplus Z_3^{(9)}, X_4^{(9)} \odot Z_4^{(9)}\right).$$

Розглянемо два повідомлення, різниця яких за побітовим додаванням має форму $(\alpha, \alpha, \alpha, \alpha)$. Зі структури раундового перетворення видно, що якщо описана різниця пройде через ключовий суматор без змін, то вона збережеться впродовж всього раунду шифрування. Таким чином, можна розглядати лише ймовірність збереження різниці при проходженні через суматор (1) без змін:

$$P = \left(Pr_{x,y}\left((x \oplus \alpha) \boxplus y = (x \boxplus y) \oplus \alpha\right)\right)^2 \cdot$$
$$\cdot \left(Pr_{x,y}\left((x \oplus \alpha) \odot y = (x \odot y) \oplus \alpha\right)\right)^2 =$$
$$= \left(DP^{\boxplus}(\alpha, 0 \to \alpha)\right)^2 \left(DP^{\odot}(\alpha, 0 \to \alpha)\right)^2 \textit{(2)}$$

Введена імовірність P характеризує складність диференціальної атаки розпізнавання на шифр IDEA.

Зміна в дизайні ключового суматора

Розглянемо операцію

$$x \otimes y = (x \boxplus 1) \odot (y \boxplus 1) \boxminus 1.$$

Для $x, y \in \{0,1,\dots,2^n-1\}$ результат цієї операції $x \otimes y \in \{0,1,\dots,2^n-1\}$, тому вона, на відміну від модульного множення в оригінальному шифрі IDEA, виконується для природного представлення чисел двійковими векторами без додаткових уточнень. З іншого боку, введена операція є складнішою з точки зору обчислення, оскільки вона є композицією декількох операцій одночасно, але таке ускладнення може бути застосоване для збільшення стійкості шифру.

Розглянемо два модифікованих ключових суматора шифру IDEA:

$$Y'^{(i)} = \left(X_1^{(i)} \otimes Z_1^{(i)}, X_2^{(i)} \boxplus Z_2^{(i)}, X_3^{(i)} \boxplus Z_3^{(i)}, X_4^{(i)} \otimes Z_4^{(i)}\right) \quad \textbf{(3)}$$

$$Y''^{(i)} = \left(X_1^{(i)} \odot Z_1^{(i)}, X_2^{(i)} \otimes Z_2^{(i)}, X_3^{(i)} \otimes Z_3^{(i)}, X_4^{(i)} \odot Z_4^{(i)}\right) \quad \textbf{(4)}$$

Для оригінального шифру IDEA та для шифрів з даними суматорами було знайдено різниці α, які визначають найбільші можливі значення імовірності P. Одержані результати наведено у таблиці 1.

Відповідно до таблиці 1, описана диференціальна атака може бути використана для побудови розпізнавача для одного раунду шифрування шифру IDEA з ймовірністю $\approx 2^{-31}$.

Структурна зміна **(3)** призвела до незначного зменшення стійкості шифру, в той час як **(4),** навпаки, значно посилила її для атаки, описаної вище. Виграш в стійкості між **(3)** та **(4)** є в середньому майже квадратичним:

$$P\left(Y'^{(i)}\right) \approx \left(P\left(Y''^{(i)}\right)\right)^{1.94}.$$

Таблиця 1. Порівняльна таблиця ймовірностей *P*

α_{hex}	$log_2\left(P\left(Y^{(i)}\right)\right)$	$log_2\left(P\left(Y'^{(i)}\right)\right)$	$log_2\left(P\left(Y''^{(i)}\right)\right)$
0001	-34.05	-31.95	-62.0
0002	-34.05	-31.95	-62.0
0004	-34.05	-31.95	-62.0
0008	-34.05	-31.95	-62.0
8000	-32.05	-29.95	-62.0
8001	-32.58	-31.15	-59.72
8002	-32.94	-31.15	-60.09
8004	-32.69	-31.15	-59.84
8008	-32.58	-31.15	-59.72
8080	-30.88	-30.0	-56.88

Висновки

У даній роботі було описано нову диференціальну атаку на шифр IDEA, яка носить теоретично-демонстративний характер, та побудовано оцінки стійкості від неї. Запропоновано алгебраїчну операцію на основі модульного множення, яка адаптована під природне представлення чисел двійковими векторами. Із використанням даної операції запропоновано модифікації ключового суматора шифру IDEA, які дозволяють суттєво посилити стійкість даного шифру до диференціального криптоаналізу.

Перелік використаних джерел

1. Xuejia Lai. On the design and security of block ciphers. (1995). DOI:10.3929/ETHZ-A-000646711

2. Jorge Nakahara Jr. Lai-Massey Cipher Designs. History, Design Criteria and Cryptanalysis. Англ. 2018, 44 с.

ОСОБЛИВОСТІ АТАК З ВИКОРИСТАННЯМ СОЦІАЛЬНОГО ГРАФУ ТА ПІДХОДИ ДО ЗАХИСТУ

Драгунцов Р.І., Зубок В.Ю.

ІПМЕ ім. Г.Є. Пухова, Київ, Україна,
vitaly.zubok@gmail.com

Проблема компрометації технічно грамотних і досвідчених співробітників, що оперують в інформаційній інфраструктурі агентом загрози полягає у високому рівні їх обізнаності та вмінням захистити власні ІТ-активи. Найчастіше їхні близькі соціальні контакти можуть не мати такого рівня власного кіберзахисту, використовують менш захищені домашні мережі, представляють простішу ціль для кіберзлочинців. Розглянуто особливості несфокусованих атак, що здійснюються через соціальний граф та використовують слабкості в «ланцюгу довіри», а також сформовані основні принципи захисту.
Ключові слова: соціальний граф, кібератака, графова модель загроз

Актуальність та особливості атак з використанням соціального графу

Високопривілейований персонал ІТ-систем найчастіше є складною ціллю для атаки агентом кіберзагрози. Компрометація пристрою одного з членів родини такого співробітника тим чи іншим способом може надати зловмиснику можливість атакувати безпосередньо важливу ціль в умовах високого рівня довіри та, часто, відсутності корпоративних систем захисту [1]. Подібні атаки використовують соціальний граф. Графові моделі атак часто застосовуються під час моделювання загроз кібербезпеки, зокрема для розбудови стратегії кіберзахисту, [2] однак питання впливу соціального графу на кібербезпеку в контексті несфокусованих атак вивчене недостатньо [3]. Важливі особливості даного класу атаки описані в Табл. 1 [4].

Таблиця 1. Особливості атак через соціальний граф

Характеристика	**Вплив**
Невизначеність початку вектору атаки	Зловмисник, використовуючи соціальний граф, може розпочати атаку в невизначеній точці, з якої досягти невизначеної точки входу в IT інфраструктуру.
Тривалість та комплексність атаки	Виконання атаки агентом загрози є ускладненим внаслідок необхідності вкладення більших ресурсів на розвиток атаки та вищої складності в уникненні виявлення на одному з етапів
Розмиття поверхні атаки	Ускладнення визначення потенційних точок компрометації та визначення рівня ризику для співробітників компанії.
Високий рівень довіри до точки компрометації	За умови успішної компрометації точка компрометації в інфраструктурі – скомпрометований співробітник або його активи – має відносно високий рівень довіри в інфраструктурі.
Низький рівень захисту точки компрометації	Компрометація співробітника або його активів здійснюється в умовах відсутності захисту того рівня, що забезпечується всередині корпоративної інфраструктури.
Обмеженість спостережності інформації	Компрометація технічних активів співробітника здійснюється в домашній мережі, що ускладнює або унеможливлює збір та аналіз журнальної інформації.
Складність проактивної ідентифікації	Значна довжина шляху компрометації та варіативність потенційних шляхів компрометації унеможливлюють або суттєво ускладнюють проактивну ідентифікацію атаки.

Модель атаки

Даний процес можна математично описати як задачу проходження в графі з використанням декількох структурних і динамічних концептів. Розглянемо мережу як спрямований граф $G=(V,E)$, де V представляє собою вузли (особи та елементи IT-інфраструктури), а E - орієнтовані ребра, що символізують взаємодії або можливість доступу між особами або особою і елементом IT-інфраструктури. Ініціація загрози - агент загрози вибирає початковий вузол $v0 \in V$ (компрометація першої особи) та використовує її цифрову ідентичність для поширення загрози. Пропагація загрози розглядається як динамічний розвиток на графі, де кожен наступний вузол активується, якщо його можна досягти від попередньо активованого вузла через спрямоване ребро (E). Це означає, що агент загрози поширює вплив від однієї особи до її оточення. Умова зупинки визначається наступним чином: Процес продовжується до тих пір, поки не буде досягнутий вузол $v*$, який має достатній рівень привілеїв у IT-інфраструктурі, що дозволяє агенту загрози обійти захищений периметр. З кінцевим результатом можна візуалізувати шлях загрози як послідовність ребер і вузлів від $v0$ до $v*$, що показує, як загроза минає захисні механізми і використовує соціальну інженерію для досягнення своєї мети.

Використання моделі та прийняття рішення щодо захисту

Оцінка шляхів в рамках наданої вище моделі може допомогти визначити ключові вузли для посилення захисту та застосувати ряд принципів протидії:

- Підхід Zero Trust – до відповідних атак вразливими можуть бути абсолютно усі користувачі без залежності до рівня обізнаності. Рівень довіри в рамках розподілу доступу всередині інфраструктури має бути нульовий однаково для усіх груп.

- Відмова від BYOD (Bring Your Own Device) – використання корпоративних пристроїв у домашніх мережах користувачів або використання власних пристроїв всередині корпоративної інфраструктури істотно підвищує відповідні ризики – дана практика розглядається як небезпечна [5].
- Впровадження рішень MDM (Mobile Device Management) – системи, що дозволяють контролювати корпоративні робочі станції поза корпоративним периметром можуть забезпечити виконання політик безпеки та достатній рівень прозорості, що дозволить ефективно протидіяти атакам наведеним вище.

Перелік використаних джерел

1. Chin, K. (2023, травень). The Impact of Social Media on Cybersecurity. UpGuard. https://www.upguard.com/blog/the-impact-of-social-media-on-cybersecurity
2. Bilar, D. J. (б. д.). Oscillation through Co-evolution: A Manifestation of Moving Target Defense. У CSIIRW 8.
3. Du, H., & J. Yang, S. (2011). Discovering Collaborative Cyber Attack Patterns Using Social Network Analysis. У Social Computing, Behavioral-Cultural Modeling and Prediction - 4th International Conference.
4. How cyber attacks work. (2015, 14 жовтня). NCSC. https://www.ncsc.gov.uk/information/how-cyber-attacks-work
5. J. Ferdousi, B. (2022). Cyber security risks of bring your own device (byod) practice in workplace and strategies to address the risks. International Journal of Science Academic Research, 3(10).

ОПТИМАЛЬНЕ РОЗПОДІЛЕННЯ РЕСУРСІВ ЗАХИСТУ ПРИ БАГАТОПОЗИЦІЙНИХ КІБЕРАТАКАХ

Смирнов С. А., Лугінін Б.А.

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря
Сікорського», Київ, Україна
s.smirnov@kpi.ua

Запропонована процедура оптимального реагування на багатопозиційні кібератаки на основі дослідження ймовірнісної моделі гри полковника Блотто. Точні рішення гри (для рівноваги за Нешем) відомі лише при суттєвих обмеженнях симетричності та однорідності моделі. Підхід що пропонується дозволяє побудувати найкращу протидію гравця за даними про розподіл ресурсів атакуючої сторони, без обмежень на вигляд моделі.

Ключові слова: розподіл ресурсів, багатопозиційні кібератаки, гра полковника Блотто, ймовірнісна модель виграшів.

Вступ

В сучасних кіберсистемах безпека як самої системи так її можливість протистояти загрозам часто визначається ресурсними обмеженнями сторони захисту. Саме тому оптимальний розподіл ресурсу є завжди актуальною проблемою. Гра полковника Блотто (ГПБ) як модель конкурентної боротьби двох осіб на декількох майданчиках вперше вона була поставлена Борелем [1] ще в 1921 році, проте і надалі залишалася актуальною та привертала увагу дослідників [2-5]. Як модель конкурентної боротьби двох сторін вона застосовується у воєнній, соціальній, економічній сфері тощо. Вважаємо доцільним використати її також для побудови ефективних систем кіберзахисту, де в якості розподільного ресурсу сторони захисту можуть розглядатися як обчислювальна потужність застосованих комп'ютерних засобів, так і робочий час команд фахівців.

Математична модель ГПБ

Дві конфліктуючі сторони розподіляють свої (неперервно подільні) ресурси x_i та y_i, i=$\overline{1,n}$, по n майданчиках, де безпосередньо відбуваються «бої». Запаси ресурсів гравців обмежені $\sum_{i=1}^{n} x_i \le R_x$, $\sum_{i=1}^{n} y_i \le R_y$. Ймовірності перемоги $p_i^x(x_i,y_i)$ $p_i^y(x_i,y_i)$ гравців на i-му майданчику задається наступним чином:

$$p_i^x(x_i,y_i) = \frac{\alpha_i x_i^{r_i}}{\alpha_i x_i^{r_i} + \beta_i y_i^{r_i}},\ p_i^y(x_i,y_i) = \frac{\beta_i y_i^{r_i}}{\alpha_i x_i^{r_i} + \beta_i y_i^{r_i}}.$$

де $r_i \in$ - показники, що характеризують еластичність дії вкладеного ресурсу на породжений їм вплив або «силу», а $\alpha_i > 0$, $\beta_i > 0$ - коефіцієнти ефективності використання цього впливу на відповідних майданчиках для першого та другого гравців. Очікувано функції очікуваних виграшів будуть мати наступний вигляд:

$$F_x(x,y) = \sum_{i=1}^{n} X_i p_i^x(x_i,y_i),$$
$$F_y(x,y) = \sum_{i=1}^{n} Y_i p_i^y(x_i,y_i),$$

де X_i, Y_i - цінність перемоги на i-му майданчику для кожного з двох гравців. Тобто кожен гравець намагається максимізувати математичне очікування цінності своїх перемог по всіх майданчиках.

Асиметрична гра, при $R_x \neq R_y$, з параметрами $r_i = 1$, $\alpha_i = 1$, $i \in N$ досліджена в роботі [3] в умовах X_i=Y_i=const. В роботі [4] знайдено рівновагу в чистих стратегіях для випадку X_i=Y_i=V_i, вже при довільних $r_i \in$, $\alpha_i > 0$, $i \in N$. Ми розглянемо ситуацію $X_i \neq Y_i$, але при умові $r_i = 1$ (класична трактовка лінійної оцінки ефективності впливу вкладеного ресурсу на результат).

Спрощення моделі та оптимізація

Головна ідея роботи полягає в наступному: пошук рівноваги у ГПВ складна задача, але навіть знання відповідних стратегій (які звісно забезпечують гарантований результат) може виявитись менш ефективним при протидії відомої, але не рівноважної стратегії нападу, оскільки знання цінностей противника завжди можуть виявитися неповними, а його дії неочікуваними. Тому

потрібно забезпечити оптимальне реагування на атаки виходячи із знання вкладеного їм ресурсу і чіткого розуміння власних цінностей та інтересів.

Для пошуку розв'язку поставленої оптимізаційної задачі запишемо функцію Лагранжа для сторони захисту: $L=F_x+\lambda(R_x-\sum_{i=1}^{n}x_i)$. Далі отримуємо систему рівнянь наслідком якої буде $\lambda=X_i\frac{\alpha_i\beta_i y_i}{(\alpha_i x_i+\beta_i y_i)^2}$, $R_x=\sum_{i-1}^{n}x_i$. З першого рівняння отримаємо точний вираз x_i через λ, підставив який в друге рівняння знайдемо точне значення λ як залежність від y_i та параметрів α_i , β_i . Далі отримаємо відповідні шукані x_i у вигляді:

$$x_i=(R_x+\sum_{i=1}^{n}y_i\,\beta_i\alpha_i)\frac{\sqrt{X_i y_i\beta_i\alpha_i}}{\sum_{i=1}^{n}\sqrt{X_i y_i\beta_i\alpha_i}}-y_i\beta_i\alpha_i$$

Отриманий вираз забезпечує оптимальний розподіл $\{x_i\}$ ресурсу захисту відповідно «розвідданих» щодо розподілу $\{y_i\}$ ресурсів атаки. Результат очікувано залежить не окремо від значень коєфіцієнтів ефективності, а саме від їх відношення, внаслідок того, що ймовірність перемоги так само визначається за їх відношенням.

Висновки

Знайдено розв'язок задачі оптимального розподілу ресурсів захисту у моделі гри полковника Блотто за відомим розподілом ресурсів атакуючої сторони. Розглянуто випадок ймовірнісної моделі виграшу для двох гравців без обмежень по значеннях цінності перемог і ефективності вкладання ресурсів.

Показано, що відхід від концепції пошуку рівноваги у грі дозволяє розширити сферу використання моделі разом зі спрощенням математичної задачі, яку вдалося розв'язати в аналітичному вигляді, що також спрощує застосування розв'язку.

Надалі планується дослідження оптимальних рішень для довільних значень показника еластичності та в умовах неповної інформації, тобто для ситуацій, коли розподіл ресурсу атакуючої сторони не є точно відомим.

Перелік використаних джерел

1. Borel E. La théorie du jeu les équations intégrales á noyau symétrique // Comptes Rendus de l'Académie. 1921. Vol. 173. P. 1304 – 1308. Comptes Rendus de l'Académie. 1921. Vol. 173. P. 1304 – 1308

2. Enric Boix-Adserà, Benjamin L. Edelman, Siddhartha Jayanti. The Multiplayer Colonel Blotto Game // https://arxiv.org/abs/2002.05240v3

3. Friedman L. Game-theory Models in the Allocation of Advertising Expenditure // Operations Research. 1958. Vol. 6. P. 699 – 709.

4. Robson R.W. Multi-Item Contest / Australian National University. Working Paper № 446, 2005. – 27 p. https://www.researchgate.net/publication/4980074_Multi-Item_Contests

5. Roberson B. The Colonel Blotto Game // Economic Theory. 2006. Vol. 29. P. 1 – 24.

ЗАСТОСУВАННЯ SAT-РОЗВ'ЯЗУВАЧІВ ДЛЯ ПОШУКУ N-ОК ШУРА

А.Ю. Васалатій, В.В. Бичок,
О.В. Циганкова, М.О. Хмельницький

Навчально-науковий Фізико-технічний інститут, НТУУ «КПІ ім. Ігоря Сікорського», м. Київ, Україна

В даній роботі розглядається можливості застосування SAT-розв'язувачів для розробки алгоритмів розбиття множини на підмножини, в яких відсутні n-ки Шура, с подальшим використанням в розв'язанні різноманітних задач у різних галузях захисту інформації, таких як, наприклад, криптографія та теорія кодування. SAT-розв'язувачі відомі своєю здатністю швидко знаходити рішення булевих задач, але їх потенціал у сфері розбиття множини на підмножини ще не був повністю досліджений. N-ки Шура використовуються в абстрактній алгебрі як розширення циклічних груп. Основна ідея роботи полягає в тому, щоб перетворити задачу розбиття множини на підмножини у задачу виконання булевої формули, де кожна змінна відповідає присутності або відсутності кожного елемента у підмножині.

Ключові слова: n-ки Шура, SAT-задача, SAT-розв'язувач, алгоритм розбиття, множина, підмножина, циклічні групи, розширення циклічних груп

Вступ

N-ки та числа Шура, однойменна теорема і множини, які не можливо розбити на 2 підмножини без *n*-ок Шура, стали ключовою темою багатьох досліджень, зокрема деякі з них відображені в наступних статтях: The Minimal Number Of Monochromatic Schur Tuples In a Cyclic Group[1] , Vishal Balaji, Andrew Lott, Alex Rice. Schur's Theorem In Integer Lattices[2].

Крім того, нещодавно, саме з використанням SAT-розв'язувача було знайдено вирішення столітньої задачі з цієї галузі: яке є найбільше натуральне число n таке, що

існує п’яти-кольорове розфарбування додатних чисел до n без монохроматичного рішення виду a + b = c, що наведене у статті Marijn J. H. Heule: Schur Number Five[3].

Щодо галузі кібербезпеки, то трійки Шура використовуються для дослідження властивостей випадково збурених множих - Schur Properties Of Randomly Perturbed Sets[4], які в свою чергу мають застосування в криптографії.

Розбиття множин на підмножини, з урахуванням наявності або відсутності n-ок Шура, нині є актуальною темою в сучасній теорії графів, криптографії та теорії інформації і кодування, зокрема будучи корисним для аналізу властивостей комбінаторних структур.

Мета дослідження полягає розробка алгоритму знаходження довільного розбиття множини на підмножини, які не містять жодної n-ки Шура з використанням SAT-розв'язувача.

Потрібно побудувати скрипт алгоритми для розбиття будь-якої множини з застосуванням SAT-розв'язувача на підмножини, які не містять жодної n-ки Шура.

Фундаментальні поняття

У статті будуть використані наведені нижче скорочення:

КНФ - кон’юнктивна нормальна форма.

ДНФ - диз’юнктивна нормальна форма.

DIMACS - текстовий формат для SAT-розв'язувача.

SAT-задача (Boolean Satisfiability Problem) - це завдання, що полягає у перевірці чи існує для заданої формули така інтерпретація, на якій вона набуває істинного значення. SAT-розв’язник - комп'ютерна програма, здатна вирішити SAT-задачу.

Для досліджень, як джерело математичного апарату, було використано Symbolic logic and mechanical theorem proving [5]

Будемо називати n-ками Шура таку послідовність цілих (натуральних) чисел:

$x_1, x_2, \ldots, x_n$, такі, що $x_1 + x_2 + \ldots + x_{n-1} = x_n$ де $x_1 < x_2 < \ldots < x_n$.

Створення алгоритму застосування SAT-розв'язувачів для пошуку розбиттів на дві множини без n-ок Шура

Застосування SAT-розв'язувачів для пошуку розбиттів на дві множини

Нехай множина S має вигляд S = {1, 2, …, p}. Задача полягає у тому аби перевірити чи існує таке довільне розбиття на дві її підмножини S_1 та S_2, що жодна з них не містимети жодної n-ки Шура, заданої розмірності.

Для ілюстрації методу розв'язку, оберемо множину S(10) і n-ку Шура розмірності 4. Подамо задачу у вигляді КНФ. Оскільки потрібно перевірити чи існує розбиття на дві підмножини без четвірок Шура, то очевидно, що лише в такому випадку дана КНФ буде виконуваною. Відповідно репрезентуємо приналежність числа з множини S підмножині як атом виду P_i, де $1 \leq i \leq 10$. Інтерпретація, на якій атом P_i набуває істинного значення в практичній площині, означатиме, що число i належить першій підмножині S_1, хибного значення - підмножині S_2. Якщо розглядати випадкову четвірку на заданій множині Шура, наприклад - {1,2,3,6}, то достатньою умовою, що вона не належатиме жодній підмножині повністю, буде належність хоча б одного її елементу першій підмножині і одного - другій. Подамо це у вигляді КНФ $(P_1 \vee P_2 \vee P_3 \vee P_6) \wedge (\neg P_1 \vee \neg P_2 \vee \neg P_3 \vee \neg P_6)$. Проте даної формули не достатньо, адже вона є лише частиною загальної, а перевірка відбувається для однієї четвірки, в повному ж вигляді для S(10) маємо:

$$(P_1 \vee P_2 \vee P_3 \vee P_6) \wedge (\neg P_1 \vee \neg P_2 \vee \neg P_3 \vee \neg P_6)$$
$$(P_1 \vee P_2 \vee P_4 \vee P_7) \wedge (\neg P_1 \vee \neg P_2 \vee \neg P_4 \vee \neg P_7)$$
$$(P_1 \vee P_2 \vee P_5 \vee P_8) \wedge (\neg P_1 \vee \neg P_2 \vee \neg P_5 \vee \neg P_8)$$
$$(P_1 \vee P_2 \vee P_6 \vee P_9) \wedge (\neg P_1 \vee \neg P_2 \vee \neg P_6 \vee \neg P_9)$$
$$(P_1 \vee P_2 \vee P_7 \vee P_{10}) \wedge (\neg P_1 \vee \neg P_2 \vee \neg P_7 \vee \neg P_{10})$$
$$(P_1 \vee P_3 \vee P_4 \vee P_8) \wedge (\neg P_1 \vee \neg P_2 \vee \neg P_4 \vee \neg P_8)$$
$$(P_1 \vee P_3 \vee P_5 \vee P_9) \wedge (\neg P_1 \vee \neg P_3 \vee \neg P_5 \vee \neg P_9)$$
$$(P_1 \vee P_3 \vee P_6 \vee P_{10}) \wedge (\neg P_1 \vee \neg P_3 \vee \neg P_6 \vee \neg P_{10})$$
$$(P_1 \vee P_4 \vee P_5 \vee P_{10}) \wedge (\neg P_1 \vee \neg P_4 \vee \neg P_5 \vee \neg P_{10})$$

$$(P_2 \vee P_3 \vee P_4 \vee P_9) \wedge (\neg P_2 \vee \neg P_3 \vee \neg P_4 \vee \neg P_9)$$
$$(P_2 \vee P_3 \vee P_5 \vee P_{10}) \wedge (\neg P_2 \vee \neg P_3 \vee \neg P_5 \vee \neg P_{10})$$

Застосувавши наш скрипт, роботу якого буде описано нижче, отримуємо від SAT-розв'язувача наступні інтерпретації:

Таблиця 1

P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}
F	F	T	T	F	T	T	T	F	F
F	F	T	T	F	F	T	T	T	T

Якщо врахувати, що істинні і хибні значення позначають приналежність до підмножин, то маємо наступні розбиття:

1) $S_1 = \{3, 4, 6, 7, 8\}$ і $S_2 = \{1,2, 5,9, 10\}$
2) $S_1 = \{3, 4, 7, 8, 9, 10\}$ і $S_2 = \{1,2, 5,6\}$

Очевидно, що при збільшенні потужності множини S, буде збільшуватися кількість заданих на даній множині четвірок і до формули потрібно буде дописати нові кон'юнкції диз'юнктів вигляду $(P_2 \vee P_3 \vee P_5 \vee P_{10}) \wedge (\neg P_2 \vee \neg P_3 \vee \neg P_5 \vee \neg P_{10})$ для нових комбінацій.

При збільшенні розмірності n-ки Шура, потрібно буде розширювати кожну пару диз'юнктів про приналежність хоча б одного елементу до підмножин для 5-ти елементів вони набувають вигляду:

$(P_2 \vee P_3 \vee P_4 \vee P_5 \vee P_{14}) \wedge (\neg P_2 \vee \neg P_3 \vee \neg P_4 \vee \neg P_5 \vee \neg P_{14})$.

Для пошуку розбиття множини S={k…n}, S={-k…-n} або ж S={-k…n}, де k, n є N, сукупність дій буде аналогічна: приналежність числа до певної підмножини також буде визначатися окремим атомом, де інтерпретація, на якій він набуває істинного значення, вказуватиме на приналежність числа до підмножини S_1, хибного - S_2. Для чисел 3..10 будуть відповідно:

P_1,P_2,P_3,P_4,P_5,P_6,P_7,P_8.

В нумерації атомів, з яких складатиметься формула, в даному випадку, зробимо зсув індексу на 2, в порівнянні зі значенням числа, що він репрезентує, щоб вона починалася з 1 - більшість SAT-розв'язувачів саме так індексують атоми. В іншому ж - все однаково, наприклад, трійка (3,4,7) в загальній формулі буде виглядати наступним чином:

$(P_1 \vee P_2 \vee P_5) \wedge (\neg P_1 \vee \neg P_2 \vee \neg P_5)$.

При опрацюванні результату SAT-розв'язувача потрібно врахувати, який саме атом відповідав певному числу з нашої множини.

На основі цього можемо сформулювати загальний алгоритм вирішення даної проблеми з використанням SAT-розв'язувача.

Алгоритм застосування SAT-розв'язувачів для пошуку розбиттів на дві множини без n-ок Шура

1. Обрати досліджувану множину і розмірність n-ки Шура;
2. Знайти всі можливі n-ки Шура на заданій множині;
3. Утворити для кожної n-ки КНФ вигляду $(P_1 \vee P_2 \vee \ldots \vee P_n) \wedge (\neg P_1 \vee \neg P_2 \ldots \vee \neg P_n)$, з яких сформувати загальну формулу, де $(P_1 \vee P_2 \vee \ldots \vee P_n)$ - означає, що хоча б 1 елемент n-ки належить першій підмножині, а $(\neg P_1 \vee \neg P_2 \ldots \vee \neg P_n)$ - другій;
4. Обрати SAT-розв'язувач, який буде використаний для пошуку інтерпретацій;
5. За необхідності перетворити формулу в прийнятний для SAT-розв'язувача формат, наприклад DIMACS;
6. На основі отриманих інтерпретацій побудувати можливі розбиття.

Висновки

У роботі досліджено способи розбиття множини на підмножини, в яких відсутні n-ки Шура з використанням SAT-розв'язувачів. За результатами досліджень було створено алгоритм застосування SAT-розв'язувачів для пошуку розбиттів на дві множини без n-ок Шура, для якого

розроблено програмні імплементації на мові Python з використанням бібліотеки надбудови **pycosat**[7] над SAT-розв'язувачем **PicoSAT**. Розроблений алгоритм знаходить усі можливі розбиття заданої множини на підмножини, використовуючи вхідні параметри потужності множини і розмірність n-ки Шура. Алгоритм можна використовувати в алгоритмах верифікації, в аналізу програмного забезпечення, вирішенні обмежень, в автоматизації електронного проєктування та дослідженні операцій, при створенні математичних алгоритмів моделювання процесів та штучному інтелекті тощо.

Перелік використаних джерел

1. Katarzyna Taczała. The Minimal Number Of Monochromatic Schur Tuples In a Cyclic Group. Functiones et Approximatio 58.1 (2018), p. 131–143 URL: https://projecteuclid.org/journalArticle/Download%3Furlid%3D10.7169%252Ffacm%252F1724&ved=2ahUKEwjTstSdz6OGAxV_XvEDHRSeBTEQFnoECBYQAQ&usg=AOvVaw2wx6yFrHLklweiChK2NOx_

2. Vishal Balaji, Andrew Lott, Alex Rice. Schur's Theorem In Integer Lattices. INTEGERS 22 (2022) w62. URL: https://math.colgate.edu/~integers/w62/w62.pdf.

3. Marijn J. H. Heule. Schur Number Five. Computer Science Department The University of Texas at Austin 2317 Speedway, M/S D9500 Austin, Texas 78712-0233 URL: https://ojs.aaai.org/index.php/AAAI/article/view/12209/12068.

4. Shagnik Das, Charlotte Knierim, Katrick Morris. Schur Properties Of Randomly Perturbed Sets. European journal of Combinatorics. May 2022 URL: https://arxiv.org/pdf/2205.01456.

5. Chin-Liang Chang, Richard Char-Tung Lee. Symbolic logic and mechanical theorem proving. 1973

6. Armin Biere. PicoSAT. URL: https://fmv.jku.at/picosat/.

7. Ilan Schnell. Pycosat. URL: https://pypi.org/project/pycosat/.

ESTIMATING THE PROBABILITY OF ATTACKS ON KEY OBJECTS OF THE SUPPLY CHAIN OF CRITICAL INFRASTRUCTURE OBJECTS

Mykola Ilin, Oleksandr Rybak, Iryna Stopochkina

Educational and Scientific Physical and Technical Institute
Ukraine
m.ilin@kpi.ua , semperfi@ukr.net , i.stopochkina@kpi.ua

The features of the supply chain of critical infrastructure objects of the industrial type have been analyzed. Types of cyber attacks on the supply chain of critical infrastructure are considered. The nature of resource relations is analyzed and a form of representation of the supply chain in the form of an oriented graph, with a division into levels, is proposed. An approach to taking into account the probabilities of object attacks, on which the functioning of some final object of the chain depends, is proposed, based on dynamic programming. The computational complexity of the proposed approach was evaluated, and conclusions were drawn about its operability for a real situation.

Introduction

The problems of cyberattacks on the supply chain are an actual area of research. Existing research is mainly aimed at maintaining the security of supply chain links and strengthening protection measures, and qualitative risk assessment [1].

The apparatus of graphs has proven itself well for the study of resource relations of industrial objects [2]. Much less attention is paid to issues of quantitative assessment of risks and calculation of probabilities of occurrence of undesirable events. This work contributes to the methods that will allow to calculate the probability of the occurrence of undesirable events due to damage to the supply chain for selected key objects.

Proposed solutions

A supply chain is an interconnected infrastructure of relationships and processes between organizations and their personnel in the development, distribution, and sale of products, services, or resources. We rely on the concept of the automation pyramid, which can contain 5 different levels: ERP, MES, SCADA, PLC and intelligent devices of the Internet of Things, the physical level [3]. Accordingly, each of these layers consumes some resources that can be exposed to cyber attacks. Let the resource connections in the supply chain be represented in the form of a directed graph, the vertices of which are the resource-source objects, and the arcs of which are the directions of the supply of resources to the following objects. The graph does not contain cycles in its structure. Each vertex of the graph v_i is related to a certain probability p_i of successful cyber attack on the critical infrastructure facility.

Assumptions:

1)If there is no edge that comes to vertex v_i, then it can be successfully attacked with p_i probability.

2) If v_i has included connections, that is, the object is depended on others in the supply chain, and can be successfully attacked with p_i probability with condition of successful attack of at least one from the objects, which influence v_i. Other way, we consider that v_i object is not under attack.

Let's calculate the probability of attack for object v_k , having data about resource relations for object supply and appropriate probabilities of attacks on different parts (vertices) of supply chain. For convenience, we will consider the vertex v_k as the end-point vertex, that means it has not outgoing edges.

Concept of solution. Let's divide the graph into "levels". We will assume that from level the edges can go only to the level $s + 1$. If it's not so – then introduce intermediate vertices with a probability of successful attack p_i=1 (fig. 1). We consider a graph as one that does not contain directed cycles.

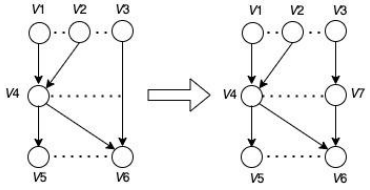


Fig. 1. Splitting the graph into levels

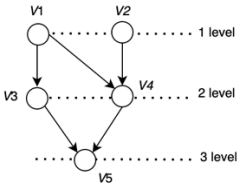


Fig. 2. Graph of the supply chain

According to the theorem about topological sorting, such a graph can always be divided into levels in such a way that the direction of the arcs is directed strictly according to the growth of the level.

We will perform dynamic programming by levels from top to bottom (from the first). For each level, we calculate the probability that this particular subset of vertices will be successfully attacked.

Example. Let this graph be of the type shown in Fig. 2.

Then, the attack probabilities for the levels will be:

$\{v_1, v_2\}: p_1p_2; \{v_1\}: p_1(1-p_2); \{v_2\}: p_2(1-p_1);$
$\emptyset: (1-p_1)(1-p_2); \quad \{v_3, v_4\}: p_3p_4, \quad \{v_3\}: p_3(1-p_4);$
$\{v_4\}: p_4(1-p_3); \emptyset: (1-p_3)(1-p_4).$
$p(\{v_3; v_4\}) = \big(p_1p_2 + p_1(1-p_2)\big)p_3p_4 = p_1p_3p_4;$
$p(\{v_3\}) = \big(p_1p_2 + p_1(1-p_2)\big)p_3(1-p_4) = p_1p_3(1-p_4);$
$p(\{v_4\}) = \big(p_1p_2 + p_1(1-p_2)\big)(1-p_3)p_4 + (1-p_1)p_2p_4 =$
$= p_1(1-p_3)p_4 + (1-p_1)p_2p_4;$
$p(\{\emptyset\}) = \big(p_1p_2 + p_1(1-p_2)\big)(1-p_3)(1-p_4) + (1-$
$p_1)p_2(1-p_4) + (1-p_1)(1-p_2)\cdot 1 =$
$= p_1(1-p_3)(1-p_4) + (1-p_1)p_2(1-p_4) + (1-p_1)(1-$
$p_2).$
$p(\{v_5\}) = p_5(p(\{v_3; v_4\}) + p(\{v_3\}) + p(\{v_4\})) =$
$= p_5(p_1p_3 + p_1(1-p_3)p_4 + (1-p_1)p_2p_4)\,.$

All cases can be presented in a table, the cells of which show the probability that a subset of level n will be attacked, given an attack on a specified subset of level m. The empty set

corresponds to the case when none of the object vertices has been successfully attacked. Building such a table allows you to algorithmize the process.

Conclusions

The approach proposed in the paper leads to an NP-complete class of algorithms. However, in specific cases, the supply chain graph has a relatively small number of vertices: for example, if the number of vertices does not exceed 10, recalculating the probabilities using the specified approach is a computationally feasible task. In addition, most often we need to examine only a part of the entire graph of connections, that is, that part of the chain that affects exactly the specified object (end vertex).

Literature

1.Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry. URL: https://www.cisa.gov/sites/default/files/2023-01/eo14017-supply-chain-fact-sheet.pdf .

2. Why supply chain management and graph technology are a perfect match. URL: https://linkurious.com/blog/supply-chain-graph/

3. Chen-Ching Liu,

Cyber Security of SCADA, Substations, and Distribution Systems. URL:

https://mpr-production-assets.s3.amazonaws.com/media/documents/Presentation1_CCLiu_Cyber_Physical_System_Security_of_a_Power_Grid.pdf

ВИВЕДЕННЯ ТА АНАЛІЗ НАРАТИВІВ У ІНФОРМАЦІЙНИХ ПОТОКАХ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

О.О. Гуменюк, А.В. Комар, І.М. Свобода, Д.В. Ланде

Навчально-науковий Фізико-технічний інститут, НТУУ «КПІ ім. Ігоря Сікорського», м.Київ, Україна
olehhumeniukba@gmail.com

Це дослідження пропонує інноваційний підхід до виведення та аналізу наративів у великих інформаційних потоках за допомогою штучного інтелекту. Використання алгоритмів машинного навчання та обробки природної мови (NLP) дозволяє автоматизувати процеси токенізації, екстракції подій та наративів. Інструменти штучного інтелекту дозволяють виявляти приховані зв'язки та структури в текстових даних, значно підвищуючи ефективність та точність аналізу. Результати дослідження демонструють потенціал ШІ у покращенні розуміння та управління інформаційними потоками в різних сферах життя.

Ключові слова: штучний інтелект, GenAI, обробка природної мови, машинне навчання, токенізація, подія, наратив, мережі подій, кластеризація, аналіз наративів, інформаційні потоки.

Вступ

Аналіз наративів в інформаційних потоках стає все більш актуальним в сучасному світі, де обсяги даних постійно зростають. Наративи, як форма представлення інформації, допомагають структурувати та інтерпретувати події, що відбуваються навколо нас [1, с.15]. Штучний інтелект (ШІ) відіграє ключову роль в обробці великих обсягів текстових даних та виявленні наративів, автоматизуючи процеси аналізу та дозволяючи виявляти приховані структури в текстах [2, с.34]. Застосування алгоритмів машинного навчання та NLP) відкриває нові

можливості для ефективного і точного аналізу наративів [3, с.50].

Мета цієї роботи – дослідити методи аналізу наративів у великих інформаційних потоках за допомогою ШІ. Основна увага зосереджена на створенні мереж подій і кластеризації для розуміння структури наративів та їх впливу на інформаційний контекст.[4, с.75]

Токенізація тексту

Токенізація — це основний етап обробки тексту, коли він розбивається на елементи, такі як слова, фрази або символи, для подальшої структуризації інформації. Вибір інструментів для токенізації, таких як бібліотеки NLTK та SpaCy, залежить від завдань аналізу. [1, с. 15].

$$F_{tokenize\_weighted}(t_i, w_i) = \{(t_i, w_i)\},$$

де t_i є токенами в тексті $T, w_i = f(t_i, T)$, w_i є вагою токена, яка може бути визначена через частоту, TF-IDF, або іншу метрику, що визначає важливість слова в контексті тексту.

Визначення понять і подій

Після токенізації текст аналізується на поняття та події, що включає використання методів машинного навчання та GenAI. Цей процес допомагає виявити ключові елементи, які формують основу наративів. [2, с. 34].

$$F_{concepts\_events\_context}(T, Context) = \{(e_j, C_j)\},$$

де e_j - події у тексті $T, C_j = g(e_j, Context)$, C_j представляє контекст події, що може включати залежності від інших подій, історичний контекст, або реляційні зв’язки.

Створення мережі подій

Методика побудови мережі подій полягає у з'єднанні подій, понять, слів та токенів для створення структур, які дозволяють візуалізувати та аналізувати взаємозв’язки між елементами тексту. Для цього був використаний інструмент Gephi. [4, с. 75].

$$F_{event\_netwok\_extended}(E) = \{(N, s(e_k, C_l))\}$$

де N є мережею $s(e_k, C_l)$ є силою звязку між e_k та e_l, $s(e_k, C_l)$ може визначатися через кількість спільних контекстів, спільних згадок, або інші відносини.

Для отримання наративів застосовувався GPT-4. Було проаналізовано новину «Контроль над IT-інфраструктурою допомагає США реалізувати кольорові революції в країнах – Радбез». З новини отримано 20 наративів, 20 подій та 20 концептів для кожного з них. Використовуючи ChatGPT-4, встановлено можливі причинно-наслідкові зв'язки між наративами та подіями.

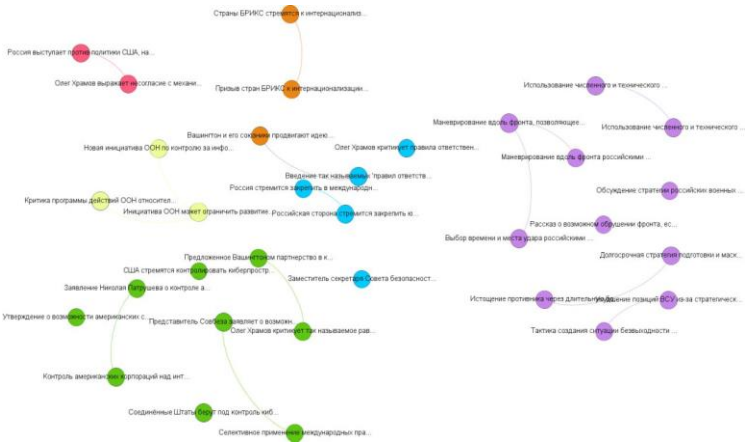


Рисунок 1 - Візуалізація кластеризованої мережі наративів і подій

Висновки

Дослідження підтвердило, що методи аналізу наративів на основі ШІ є потужним інструментом для обробки великих обсягів текстових даних. Це може бути корисним для наукової спільноти та практичного застосування у різних галузях, таких як журналістика, соціологія, політика та інші. Методологічний підхід, запропонований у цьому

дослідженні, відкриває нові перспективи для автоматизації та вдосконалення процесів аналізу інформаційних потоків, сприяючи кращому розумінню та управлінню наративами у сучасному світі.

Перелік використаних джерел

1. Salgado A., Zeng J., Abnar S. A Survey on Event-based News Narrative Extraction. — 2023-07-17. — P. 15.
2. Smith R., Doe J., Lee K. A Survey on Narrative Extraction from Textual Data. — 2023-01-06. — P. 34, 60.
3. Williams B., Chen Y., Patel R. Testing the Quantitative Spacetime Hypothesis using Artificial Narrative Comprehension. — 2020-09-23. — P. 50.
4. Martin J., Brown T., Doe P. Using Narrative Function to Extract Qualitative Information. — 2020-12-28. — P. 75.

ФОРМУВАННЯ СТРАТЕГІЙ КІБЕРБЕЗПЕКИ ЗА ДОПОМОГОЮ МЕТОДУ АНАЛІЗУ ІЄРАРХІЙ ТА ШТУЧНОГО ІНТЕЛЕКТУ

І.М. Свобода

Навчально-науковий Фізико-технічний інститут, НТУУ «КПІ ім. Ігоря Сікорського», м.Київ, Україна
i.svoboda@kpi.ua

Це дослідження пропонує інноваційний підхід до формування стратегій кібербезпеки, який поєднує метод аналізу ієрархій (MAI) та моделі штучного інтелекту GPT-4. Моделі GPT-4 генерують матриці парних порівнянь для MAI, що дозволяє автоматизувати та спростити процес прийняття стратегічних рішень у сфері кібербезпеки. Результати демонструють потенціал великих мовних моделей (LLM) у формуванні ефективних та масштабованих стратегій кібербезпеки.

Ключові слова: *GPT-4, MAI, великі мовні моделі, генеративний ШІ, метод аналізу ієрархій, стратегії кібербезпеки, прийняття рішень.*

Вступ

Метод аналізу ієрархій (MAI), розроблений Томасом Л. Сааті, пропонує структурований підхід до прийняття рішень у складних ситуаціях, враховуючи якісні та кількісні фактори [1][2]. Поява великих мовних моделей (LLM), таких як серія Generative Pre-trained Transformer (GPT) [3], відкриває нові можливості для автоматизації процесів прийняття рішень за допомогою штучного інтелекту [4]. Однак, незважаючи на широке застосування MAI та значну роль LLM, досліджень, які безпосередньо інтегрують ці підходи для формування стратегій кібербезпеки, практично немає. Тому мета цієї роботи – дослідити інтеграцію MAI з LLM для створення системи підтримки прийняття рішень на основі штучного інтелекту у сфері кібербезпеки, зосереджуючись на використанні

LLM для імітації експертних суджень та автоматизації створення матриць парних порівнянь в рамках MAI.

Віртуальні експерти для стратегій кібербезпеки

Для формування стратегій кібербезпеки з використанням MAI ми розробили сім віртуальних експертів на основі GPT-4 з персоналізованими характеристиками. "Консультант з MAI" визначив оптимальну структуру дерева MAI для мети "Формування стратегії захисту критичної інфраструктури від кібератак". Віртуальні експерти згенерували та узгодили шість критеріїв верхнього рівня, адаптованих до поставленої мети.

Віртуальні експерти виконали попарні порівняння в рамках MAI, створюючи матриці на основі своєї експертизи. Ми агрегували індивідуальні матриці за допомогою методу геометричного середнього (1):

$$A_{agg}(i,j) = \left(\prod_{k=1}^{E} A_k(i,j)\right)^{\frac{1}{E}}$$

де $A_{agg}(i,j)$ позначає агреговане значення попарних порівнянь між елементами i та j у зведеній матриці, $A_k(i,j)$ - значення попарного порівняння між елементами i та j, надане віртуальним експертом k, а E - загальна кількість віртуальних експертів (у нашому випадку 7).

Автоматизація MAI через штучний інтелект

Інтеграція методу аналізу ієрархій (MAI) з великими мовними моделями (LLM) дозволило автоматизувати та вдосконалити процес формування стратегій кібербезпеки. Віртуальні експерти на основі GPT-4 згенерували узгоджені й раціональні матриці попарних порівнянь, спрощуючи прийняття рішень та підвищуючи ефективність, особливо при роботі зі складними ієрархіями критеріїв та альтернатив.

Для обчислення векторів пріоритетів використовується формула (2):

$$w_i = \left(\frac{1}{n}\right)\sum_{j=1}^{n} a_{ij}^{norm}$$

де w_i - пріоритетна вага i-го критерію (або альтернативи), а n - загальна кількість критеріїв (або альтернатив).

Застосування методу автоматизації MAI через штучний інтелект дозволило успішно сформувати стратегії кібербезпеки для захисту критичної інфраструктури від кібератак. Аналіз виявив, що оптимальною альтернативою є "Впровадження Zero Trust архітектури" з вектором пріоритету 0,3542. Віртуальні експерти надали детальні обґрунтування своїх суджень, підкресливши важливість комплексного підходу до забезпечення кібербезпеки критичної інфраструктури.

Висновки

Результати дослідження демонструють значний потенціал інтеграції MAI з LLM для автоматизації прийняття рішень у сфері кібербезпеки, дозволяючи швидко та обґрунтовано формувати стратегії з урахуванням множини критеріїв та альтернатив. Однак, необхідно враховувати і певні обмеження методу, такі як залежність ефективності віртуальних експертів від якості та актуальності даних [5], а також можливі обмеження пам'яті при роботі з особливо складними ієрархіями MAI [6]. Попри це, запропонований метод відкриває нові перспективи для автоматизації та вдосконалення процесу формування стратегій кібербезпеки, що може суттєво сприяти підвищенню рівня захисту критичної інфраструктури від кібератак.

Перелік використаних джерел

1. M. Köksalan, J. Wallenius, and S. Zionts, Multiple Criteria Decision Making: From Early History to the 21st Century. World Scientific, 2011. https://doi.org/10.1142/8042

2. T. L. Saaty, "How to make a decision: The analytic hierarchy process," European Journal of Operational Research,

vol. 48, no. 1, pp. 9-26, 1990 https://doi.org/10.1016/0377-2217(90)90057-I

3. A. Radford, K. Narasimhan, T. Salimans, and I. Sutskever, "Improving Language Understanding by Generative Pre-Training," 2018. https://openai.com/research/improvinglanguage-understanding-by-generative-pre-training

4. M. Sallam, "ChatGPT Utility in Healthcare Education, Research, and Practice: Systematic Review on the Promising Perspectives and Valid Concerns," Healthcare (Switzerland), vol. 11, no. 6, Article 887, 2023. https://doi.org/10.3390/healthcare11060887

5. L. Tang et al., "Evaluating large language models on medical evidence summarization," npj Digital Medicine, vol. 6, no. 1, Article 158, 2023. https://doi.org/10.1038/s41746-023-00896-7

6. D. Lande, L. Strashnoy, and O. Driamov, "Analytic Hierarchy Process in the Field of Cybersecurity Using Generative AI," SSRN, Nov. 2, 2023. https://ssrn.com/abstract=4621732

АНАЛІЗ ШКІДЛИВОГО ТРАФІКУ НА КАНАЛЬНОМУ РІВНІ

Палагін В.В., Івченко О.В.

Черкаський державний техноголічний університет,
м. Черкаси, Україна
palahin@ukr.net, o.ivchenko@chdtu.edu.ua

Наведено типові загрози комп'ютерним мережам фізичного та канального рівнів моделі OSI та проведено аналіз особливостей виявлення таких загроз. Результати аналізу можуть бути використані для прийняття обґрунтованих рішень щодо вибору методів захисту для мереж різного призначення та з різними вимогами щодо захисту інформації.

Ключові слова: Аналіз трафіку, ARP spoofing, штучний інтелект, атаки на рівні L2, MAC-адреса

Вступ

Пристрої мережі, які працюють на другому рівні еталонної моделі OSI вважаються найслабшою ланкою в інфраструктурі безпеки [1-3, 6]. Розповсюджена IT-політика BYOD, використання віртуальних мереж і низки складних атак, збільшують вірогідність того, що мережі стають більш уразливими до проникнення саме на рівні L2. Протоколи рівня L2 дуже часто залишаються без належної уваги і здебільшого працюють зі стандартною конфігурацією. Слід пам'ятати, що порушення мережної безпеки на рівні L2 також впливатиме на всі рівні, розташовані вище. Таким чином, фахівцям з мережної безпеки потрібно також запобігати і вчасно нейтралізувати атаки на інфраструктуру LAN рівня L2.

Підробка ARP запиту/відповіді

Атака ARP spoofing, також відома як «отруєння кешу» ARP, використовується в атаці типу «людина посередині» [5, 6]. Під час атаки ARP spoofing зловмисник діє наступним чином: надсилає небажане, підроблене

повідомлення відповіді ARP, яке містить підроблену MAC адресу зловмисника для всіх хостів у локальній мережі. Після отримання відповіді ARP усі пристрої в локальній мережі оновлять свої ARP або таблиці MAC-адрес із неправильною MAC-адресою. Це ефективно «отруює кеш» на кінцевих пристроях. Якщо таблиці ARP «отруєні», це дозволить зловмиснику видати себе за інший хост, щоб отримати доступ до конфіденційної інформації. Таким чином трафік спрямовується не на фактичний хост, а на хост із підробленою MAC-адресою.

Зазвичай при проведенні атаки, націленої на отруєння кешу ARP, суб'єкт загрози може надсилати іншим хостам у підмережі самочинні ARP-відповіді, які містять MAC-адресу зловмисника і IP-адресу шлюзу за замовчуванням.

Приклад трафіку, який можна спостерігати при атаці отруєння кешу ARP показано на рисунку 1. З наведеного прикладу видно, що хост зловмисника направляє одноадресний запит і одноадресну відповідь, в яких видає себе за шлюз з IP-адресою 172.16.0.1

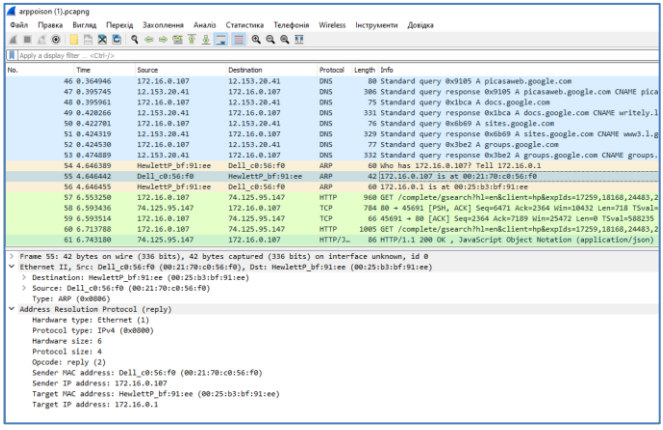


Рисунок 1 - Трафік при атаці отруєння кешу ARP

Шторм ARP

Зловмисник може самовільно надсилати комутатору ARP-повідомлення із підробленою MAC-адресою, в

результаті чого комутатор оновлюватиме свою MAC-таблицю. Оскільки всі MAC-таблиці мають обмежений розмір, комутатор може вичерпати ресурси для зберігання MAC-адрес. Атаки з переповнення таблиць MAC-адрес (MAC-флуд), користуючись цим обмеженням, бомбардують комутатор кадрами з підробленими MAC-адресами джерела, допоки таблиця MAC-адрес комутатора не заповниться.

Шторм ARP заповнює таблицю CAM комутатора і переповнює її тисячами фіктивних записів.

У цей момент комутатор просто діє як концентратор і надсилає дані на всі порти.

Наслідки такої атаки:

- У зловмисника з'являється можливість перехоплення всього трафіку з можливим наступним розкриттям конфіденційних даних.
- Через велику кількість широкомовних запитів знижується пропускна здатність мережі.

Захист від ARP-атак

Виявлення трафіку, який спричинений атакою ARP spoofing, є досить складною операцією, так як потребує аналізу і виявлення шкідливого трафіку при активізації атаки ARP spoofing (початковий етап «отруєння ARP кешу») і аналізу і виявлення самого факту, що трафік переадресовується через вузол зловмисника. Щоб виявити цю загрозу використовують [5,6]:

Системи виявлення/запобігання вторгненням (IDS/IPS): налаштування пристроїв для відстеження аномальної активності ARP, наприклад штормів ARP, які зазвичай мають специфічні сигнатури. Пристрій має надіслати сповіщення, якщо буде виявлено небажані відповіді.

Статичні записи ARP: жорстке відображення адрес для запобігання спуфінгу. Незважаючи на те, що це варіант, це не найкращий метод, оскільки він погано масштабується у великих мережах.

Брандмауери: використовуйте лише список контролю доступу з фільтрацією пакетів авторизований трафік знаходиться в сегменті мережі.

Програмне забезпечення для захисту від ARP: це програмне забезпечення відстежує спуфінг, який може представлятися як дві IP-адреси з однаковою MAC-адресою, а також інші методи для виявлення зловмисної поведінки ARP.

Висновки

В роботі проведений аналіз атак, які базуються на маніпулюванні протоколом ARP. Наведено приклади трафіку, який утворюється при активізації атаки з використанням протоколу ARP. Результати аналізу можуть бути використані для прийняття обґрунтованих рішень щодо вибору методів захисту для мереж різного призначення та з різними вимогами щодо захисту інформації.

Список використаних джерел

1. Wendell Odom. CCNA 200-301 Official Cert Guide. Volume 1-2 Cisco Press, 2019. — 1095 p.
2. Chris Carthern, William Wilson, Richard Bedwell, Noel Rivera Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA. Apress Media, 2015. — 839 p.
3. Omar Santos, John Stuppi CCNA Security 210-260 Official Cert Guide. Apress Media, 2016. — 608 p.
4. Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. — Львів: «Магнолія 2006», 2013. — 256 с.
5. Chris Sanders, Practical packet analysis. Using wireshark to solve real-world network problems. 3-d Edition, 2019.- 448 pages.
6. Lisa Bock, Learn Wireshark: A definitive guide to expertly analyzing protocols and troubleshooting networks using Wireshark, 2nd Edition, 2022. - 606 pages.

ІСНУЮЧІ ВРАЗЛИВОСТІ TOR-МЕРЕЖ

Живило Є.О., Сімонькін А.А.

Національний університет «Полтавська політехніка імені Юрія Кондратюка», м. Полтава, Україна
zhivilka@i.ua, andreysima6@gmail.com

Розробка дієвої стратегії захисту будь-якої системи електронних комунікацій та системи управління технологічними процесами є доволі серйозним і відповідальним завданням. Сьогодні широке коло осіб знаходяться в пошуку сучасних технічних проєктів щодо організації анонімних мережевих з'єднань, захищених від прослуховування в умовах застосування механізмів аналізу трафіку. Враховуючи те, що на сьогодні ні одна система не є повністю безпечною, в даній роботі опрацьовано практичні результати аудиту браузера Tor Browser і інструментів OONI Probe, rdsys, BridgeDB і Conjure.
Ключові слова: кібербезпека, захист інформації, архітектура, TOR-мережа.

Вступ

Одним із консолідованих рішень будь-якої установи щодо створення та розгортання анонімної мережі є архітектура побудована на основі Socks-протоколу, де дані багаторазово шифруються і пересилаються через мережеві вузли (nodes). Отже результатом проектування зазначених рішень є The Onion Router – мережі. Так пакети всередині мережі використовують випадкові маршрути, а вузли знають тільки, від якого сервера вони отримують дані і якому серверу передають. В цих умовах повний маршрут проходження пакетів залишається невідомим.

Постановка проблеми

Аудит безпеки будь-якого програмного чи апаратно-програмного комплексу є важливою необхідністю всього його життєвого циклу. Тестування безпеки дозволяє виявити "сліпі плями", усунути ймовірні недоліки і

показати способи поліпшення загального стану безпеки [1]. За результатами аудиту стану безпеки Tor Project було виявлено ряд вразливостей, дві з яких віднесено до категорії небезпечних, одній присвоєно середній рівень небезпеки, а шість віднесено до проблем із незначним рівнем небезпеки. Також у кодовій базі було знайдено десять проблем, віднесених до категорії не пов'язаних із безпекою недоробок. Загалом код проєкту Tor відзначено як такий, що відповідає практикам безпечного програмування.

Отже, вбачається за необхідне детально розглянути існуючі потенційні вразливості TOR-мережі.

Виклад основного матеріалу

Основними проблематиками які були виявлені стали:

– *вразливість у бекенді* rdsys, який використовується для доставки різних ресурсів користувачам, зокрема списків проксі та посилань для завантаження. Проблематика за цією вразливістю полягала у відсутності аутентифікації під час звернення до реєстраційного обробника ресурсів. В подальшому зазначене дозволило зловмиснику зареєструватися і надати шкідливий ресурс користувачеві. Постексплуатація здійснюється за надсиланням HTTP-запиту до обробника rdsys;

– *вразливість у* Tor Browser. Проблема пов'язана з відсутністю перевірки цифрового підпису під час завантаження списку мостів через rdsys і BridgeDB. Оскільки цей список завантажується до підключення до анонімної мережі Tor, можлива підміна вмісту списку атакуючим, наприклад, через перехоплення з'єднання. Постексплуатація дозволяє користувачам підключатись через скомпрометовані мостові вузли, контрольовані зловмисником;

– *вразливість в підсистемі* rdsys, дала змогу атакуючому підвищити свої привілеї з рівня користувача nobody до користувача rdsys, за наявності доступу до сервера і можливості запису в каталог із тимчасовими файлами. Постексплуатація зводиться до заміни виконуваного файлу, що розміщується в каталозі /tmp.

Отримання прав користувача rdsys дає змогу атакуючому внести зміни в виконувані файли, що запускаються через rdsys [2].

– *вразливості низького ступеня небезпеки.* Більшість із них були пов'язані з використанням застарілих бібліотек, що містять відомі вразливості, або з можливістю здійснення відмови в обслуговуванні. У Tor Browser, наприклад, була можливість обійти заборону виконання JavaScript під час виставлення вищого рівня захисту, відсутність обмежень щодо завантаження файлів і потенційний витік інформації через призначену для користувача домашню сторінку, що дає змогу відстежувати користувачів між перезапусками.

Отже, відомо, що на поточний момент усі відомі слабкі місця які було виявлено – виправлено. Крім того, впроваджено додаткові заходи безпеки, включно з аутентифікацією для всіх компонентів rdsys і перевіркою цифрових підписів під час завантаження списків у Tor Browser.

При цьому, під час проведення пентестінгу існує доволі велика впевненість що в TOR-мережах можуть бути присутні декілька потенційних вразливостей, а саме:

1. Вихідні вузли Tor є кінцевими точками маршруту, через які виходять дані з мережі Tor у звичайний інтернет. Оскільки дані на цьому етапі вже не зашифровані, адміністратор вихідного вузла може переглядати і навіть змінювати трафік.

2. Аналіз трафіку. Зловмисники можуть проводити аналіз трафіку для ідентифікації користувачів. Використання кореляційного аналізу, коли трафік на вхідних та вихідних вузлах співставляється за часом і об'ємом, може дозволити визначити початкове та кінцеве місце призначення трафіку.

3. Зловмисні вузли. Здійснюється контроль великої кількості вузлів у мережі Tor, що спонукає реалізацію атаки типу "man-in-the-middle" або аналіз трафіку [3]. Також є можливість запустити зловмисні сервери, які спеціально надають послуги з видачею невірної інформації або підробляють відповіді.

4. Sybil-атаки. Передбачається створення великої кількості псевдонімних вузлів, які виглядають як різні, але насправді контролюються однією особою чи групою. Це може зменшити ефективність розподілу маршрутів та підвищити ймовірність перехоплення трафіку.

5. Експлуатація програмних уразливостей. Можлива наявність уразливостей для зламу системи користувача та деанонімізації його дій.

6. Атаки на приховані сервіси. Приховані сервіси Tor (наприклад, .onion сайти) також можуть бути вразливими до атак, як і будь-які інші веб-сайти. Можливе використання DDoS атак, SQL-ін'єкцій або інших методів, щоб вивести сервіс з ладу або отримати несанкціонований доступ до даних [4].

7. Уразливості фізичних мереж. Можливість проведення атак фізичної мережі, через які проходить трафік Tor. Наприклад, атаки на рівні інтернет-провайдерів або надавачів послуг хостингу, де розміщені вузли Tor.

8. Відстеження через інші засоби. Можливе здійснення аналізу активності в соціальних мережах, фішинг, експлуатація слабких паролів або використання інших уразливих сервісів [5].

Висновки

Отже, Tor надає потужний інструмент для збереження приватності користувачам. Але при цьому Tor-мережі не є повністю безпечними, мають доволі великий перелік уразливостей, що можуть бути використані для деанонімізації користувачів, призвести до викрадення цінної інформації чи витоку персональних даних. За цих умов необхідно додержуватись деяких рекомендацій щодо підвищення безпеки при використовуванні Tor-мереж, а саме, використовувати: останні версії програмного забезпечення Tor, VPN перед підключенням до Tor, регулярно оновлювати і перевіряти систему на уразливості. Необхідно пам'ятати, що ні одна система не є повністю захищеною, тож потрібно проводити аудит безпеки щоб покращити стан захищеності системи.

Перелік посилань

1. Живило, Є.О. Тестування на проникнення [навч. посіб.] . Ч. 2. / Є.О. Живило; за ред. Є.О. Живило.- Полтава : Нац. ун-т ім. Ю. Кондратюка, 2024.- 239 с.

2. Живило, Є.О. Захист інформації та кібербезпека в електронних комунікаційних мережах : навч. посіб. / Є.О. Живило.- Полтава : Нац. ун-т ім. Ю. Кондратюка, 2023.- 188 с.

3. Живило, Є.О. Оцінка кіберризиків на об'єктах критичної інформаційної інфраструктури організаційно-технічних моделей кіберзахисту / Міжнародна науково-практична конференція «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку», Харків, Національна академія Національної гвардії України, 14 березня 2024 р. – С. 98–101.

4. Про Tor [Електронний ресурс]. – Режим доступу: https://support.torproject.org/uk/about/.

5. Використання Tor для анонімного доступу в інтернет: Плюси та мінуси [Електронний ресурс]. – Режим доступу: https://mindscope.biz.ua/vykorystannya-tor-dlya-anonimnogo-dostupu-v-internet-plyusy-ta-minusy/.

CLOUD STORAGE RISK ANALYSIS METHOD BASED ON Q-ANALYSIS OF THREATS AND VULNERABILITIES

Polutsyganova V.I., Smirnov S.A.
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
Kyiv, Ukraine
medvika@ukr.net

The procedure for risk assessment is described, taking into account the complexity of the relationship between threats and vulnerabilities. The developed method is applied to the selected cloud storage and the defined formula provides a refined risk assessment. This approach allows, using expert assessments and the profile of attacks on the system, to take into account the impact of threats and to apply more effective methods of countering attacks in the future.

Key words: risk assessment, Q-analysis, expert assessments, cloud storage, threats, vulnerabilities, cyber systems.

Introduction

In modern cyber systems, a major role is played by the security of both the system itself and its ability to resist threats and reduce the impact of vulnerabilities present in it [1]. Cloud storage is an integral part of cyber systems and has complex interrelated vulnerabilities and threats, the implementation of which results in losses of various levels. To reduce the consequences of attacks, most users of cloud storage and not only them try to assess the risks of implementing attacks on the system. This paper describes a method of risk assessment based on a structural analysis of the threat/vulnerability system, which leads to the refinement of risk assessment and subsequent effective decision-making to counter attacks on the system.

Risk assessment method based on the structure of vulnerabilities and threats

It is presented in the work, estimates of the corresponding probabilities and losses were refined. The classic formula of

average losses takes into account the compatibility and dependence of adverse events, but, usually, the assessment of the probabilities of the realization of threats is simplified for the situation of individual incompatible events [2].

In reality, compatible implementations of vulnerabilities/threats may occur, which complicates probability estimates due to the occurrence of compatible and conditional probabilities. Clarification of the risk assessment also occurs due to the modification of the assessment of the amount of losses in the event of such events. Summarizing [3-6] approaches, below we present a complete method for calculating risk assessment for systems with a complex structure. We will present all the stages of the obtained generalized method.

I stage. Collection of data on the structure of system vulnerabilities and threats.

II stage. Synthesis of sympletial complex.

III stage. Use of Q-analysis methods to identify structural features of the simplicial complex.

IV stage. Classification of threats/vulnerabilities in the complex based on Q-analysis.

V stage. Determination of probability distribution and loss level.

VI stage. Calculation of risk estimates for the cyber system.

Based on the profile of attacks on the cyber system, a distribution of probabilities for threats is formed. With the help of expert methods, estimates of losses from vulnerabilities and threats are determined depending on their combination.

Using local maps and a structural tree, we build a formula for calculating the total risk of the system:

- for each leaf of the tree at any level of connectivity, the risks for the corresponding simplex are calculated (each risk is partial, but its calculation is not trivial);

- when moving along the structural tree, it leads to the fact that individual simplexes are connected into chains, that is, there is a "gluing" of simplexes with different degrees of q-bonding.

Application of the method risk assessment refinement on the example of cloud storage

In the course of the work, a general formula for risk assessment for cloud storage was obtained. Data for determining the structure of interdependence between vulnerabilities and threats was used from [7]. A Q-analysis was performed and the main metrics such as local maps, structure tree, structure graphs and defined. Based on the obtained data, threat classification was carried out and risks were calculated for each level of q-connectivity. A formula for calculating the total risk was obtained, which can be used in the future for modeling attack profiles and obtaining risk estimates:

$$R_{\text{загал.}} = \sum_{i=1}^{12} R_{T_i} - R_{\{T_1,T_7\}} - R_{\{T_4,T_7\}} - R_{\{T_1,T_8\}} - R_{\{T_1,T_2\}} - R_{\{T_1,T_6\}} - R_{\{T_4,T_8\}} - R_{\{T_4,T_9\}} - R_{\{T_1,T_3\}} - R_{\{T_1,T_5\}} - R_{\{T_1,T_{10}\}}$$

where T_1 is the corresponding threat against which the risk is assessed, $R_{\{T_i,T_j\}}$ is the "glue" between the simplexes generated by threats i and j and corresponds to a certain "sum" of the risk of compatible vulnerabilities affecting both threats. The amount at the beginning of the formula corresponds to the Bayesian risk assessment formula. 12 threats and 7 vulnerabilities were identified for this cloud storage [7].

Conclusions

The paper presents a risk assessment method for a complex system of threats and vulnerabilities. The developed method is used to assess cloud storage threats. The method provides a refined risk assessment due to taking into account the connections between threats and vulnerabilities. Taking into account the connections between threats and vulnerabilities gives a reduction in the risk assessment in the general case, the exact assessment is determined by the profile of attacks on the system and expert assessments of losses from their implementation.

References

1. Kachynskyi A. B. Security of complex systems / under the editorship. Corresponding member of the National Academy of Sciences of Ukraine Dovhoy S.O. — K.: Euston, 2017. - 498 p.
2. Vyshnyakov Y. D., Radaev N. N. General theory of risks. – 2 ed. – M.: Academy, 2008—368 p.
3. Beaumont J.R., Gatrell A.C. “An introduction to Q-analysis” Catmog 34, 1982. URL: https://alexsingleton.files.wordpress.com/2014/09/34-an-introduction-to-q-analysis.pdf.
4. Polutsyhanova V. I. Vulnerability classification using Q-analysis. Theoretical and applied cybersecurity. 2023. Vol. 5, no. 2. P. 56–61. URL: https://doi.org/10.20535/tacs.2664-29132023.2.285431.
5. Полуциганова В. І., Смирнов С. А. Методологія побудови основних метрик q-аналізу та їх застосування. Системні дослідження та інформаційні технології. 2019. № 3. С. 76–88. URL: https://doi.org/10.20535/srit.2308-8893.2019.3.07.
6. Le N. T., Hoang D. B. A Threat Computation Model using a Markov Chain and Common Vulnerability Scoring System and its Application to Cloud Security. Journal of Telecommunications and the Digital Economy. 2019. Vol. 7, no. 1. P. 37–56. URL: https://doi.org/10.18080/jtde.v7n1.181.

ФОРМУВАННЯ СЕМАНТИЧНОЇ МЕРЕЖІ КІБЕРЗАГРОЗ ШЛЯХОМ ОБРОБКИ ПРИРОДНОМОВНИХ ТЕКСТІВ

Анатолій Фегер, Дмитро Ланде

КПІ ім. Ігоря Сікорського, Київ, Україна

Ефективна аналітика кіберзагроз є важливою складовою сучасного кіберзахисту, зосередившись на використанні новітніх технологій штучного інтелекту, можна полегшити дослідження великих текстових масивів за допомогою контекстно-мережевого підходу. Це відкриває прискорені можливості для виділення загальних зв'язків і прихованих закономірностей між вилученими лінгвістичними сутностями. Запропоновано методологію забезпечення точності та повноти обробки NER з великого масиву новинних вирізок про кібератаки на Україну та висвітлено аналітичні можливості семантично-мережевого підходу.
Ключові слова: Cyber attacks, Semantic networks, Linguistics, GPT, NER

Вступ

У сфері кібербезпеки здатність швидко і точно ідентифікувати критичні елементи в неструктурованому тексті, такі як кіберзагрози і вразливості, має першорядне значення. Розпізнавання іменованих об'єктів, Named-Entity Recognition (NER) виділяється як важливий інструмент в обробці природної мови, Natural Language Processing (NLP), який полегшує вилучення структурованої інформації з текстів.

Це дослідження присвячене застосуванню методів NER, зокрема, використанню можливостей генеративного Штучного Інтелекту (ШІ) для обробки україномовних та російськомовних новинних статей про кібератаки проти України. Такий підхід дає змогу всебічно проаналізувати текстові корпуси, виокремити семантичні зв'язки та виявити релевантні об'єкти в контексті кожної новини.

На основі опрацьованих даних пропонується побудувати контекстну семантичну мережу, яка прояснює зв'язки та основні закономірності між об'єктами в текстовому просторі. Для підвищення точності та релевантності виокремлених об'єктів запропоновано додаткові процедурні рівні для підвищення точності та забезпечення повноти вихідних даних.

Методологія

Досліджуваний масив даних складається з новинних вирізок і статей, отриманих з відкритих джерел, що відображають кібератаки, пов'язані з Україною, за ключовими параметрами на україномовних та російськомовних ресурсах. Набір даних складається з 500 новинних вирізок, кожна з яких в середньому містить 976 слів, підготовлених як тестові документи для подальшого аналізу.

Для обробки було вилучено несуттєвий контекст, такий як дати, автори та посилання, а контент було розділено на 10 частин для зручності обробки. Кожна частина містила 50 вирізок, оброблених окремо ШІ з окремими запитами для забезпечення об'єктивності, без збереження попередньої історії запитів.

Дослідження використовує методи обробки природної мови для семантичного пошуку та вилучення зв'язків між сутностями [1]. Генеративний ШІ визначає еквіваленти в тексті, присвоює токенам мітки типів сутностей і визначає рівні зв'язків. Він також ітеративно заповнює контекстуальні прогалини. Для візуалізації семантичні пари сутностей нормалізуються та уніфікуються, щоб зменшити дискретність і фрагментарність даних.

Екстракція семантичних сутностей

Було використано описані техніки NER, як ключовий метод обробки природної мови - для ідентифікації та категоризації ключових елементів у просторі текстів та вилучення структурованої інформації з новинних вирізок. Обрано модель роду Generative Pre-trained Transformer

(GPT-4), оскільки вона продемонструвала більшу точність та ефективність при обробці україномовних новинних вирізок, в порівнянні з іншими моделями [2]. GPT-4 налаштовано на стандартній температурі 0,7 і використовує внутрішні алгоритми токенізації текстів, який вирішує проблему рідкісних слів, розбиваючи їх на підслова, які потім перетворюються на вектори високої розмірності, де фіксують як семантичні, так і синтаксичні деталі [3]. Архітектура GPT розширює його можливості, вбудовуючи лексеми контекстуально, враховуючи взаємозалежності між сусідніми лексемами.

Для підвищення ефективності NER було введено додатковий аналітичний рівень для вимірювання сили семантичних зв'язків між парами ідентифікованих сутностей. Цей рівень вимагає додаткового запиту в моделях GPT для оцінки якісних аспектів лінгвістичних зв'язків між сутностями в контексті новинної статті. Оцінка цих зв'язків включає низку внутрішніх методів GPT, від простих детермінованих підходів, таких як аналіз повторюваності слів, до більш складних методів, таких як оцінка косинусної схожості між векторами об'єктів для формування результату за запитом [4]. Ці методи інтегровані в подальшу мультимодальну стратегію яка відображає різноманітний характер запитів, промптів застосованих до визначеного набору даних.

Модель використовує ці методи для прогнозування рівня кореляції між вихідними сутностями, виводячи результати у форматі прикладу «Приватбанк; російські хакери; 55\%», де відсоток відображає оцінений лінгвістичний зв'язок за шкалою від 0 до 100. Цей підхід не лише ідентифікує сутності, а й аналізує їхні взаємозв'язки, тим самим підвищуючи точність даних, за впровадженням у подальшому відповідної фільтрації пар понять за цією ознакою, які демонструють мінімальну реляційну значущість.

Агрегація та нормалізація лексем

При обробці тексту великі мовні моделі, такі як GPT, генерують відповіді на основі розподілу ймовірностей, які

можуть здаватися правильними, але можуть містити шум та галюцинації. Таким чином, такі відповіді краще розглядати як рекомендацію віртуального експерта [5].

Для підвищення надійності кожен запит на розпізнавання об'єктів за NER дублюється, таке ітеративне злиття підказок і текстових просторів забезпечує кількісні варіації від декількох віртуальних експертів, створюючи більш повний набір даних. Описаний ітеративний метод покращує аналіз новинної інформації, інтерфейс дозволяє задавати значення кількості повторень запитів, що полегшує ітеративну генерацію відповідей у GPT-моделях.

Для забезпечення якісних та кількісних характеристик, стикаючись з проблемами синонімізації, та лінгвістичної невизначеності в лексемах виділяється висока варіативність сформованих взаємопов'язаних пар. Таке лінгвістичне розмаїття сильно ускладнює візуалізацію мережі, перешкоджаючи визначенню її ключових вузлів, центральності та категоризації, що має вирішальне значення для забезпечення аналітичних завдань.

Наприклад, «кібербезпека України» та «українська кібербезпека» які створюють додаткову сплутаність в побудованій мережі, тому методи лексичної нормалізації стандартизують термінологію для покращення структури мережі. Передові лінгвістичні моделі, такі як GPT, мають покращене контекстуальне розуміння простору текстів, точно ідентифікуючи та асоціюючи слова, вони підтримують автоматичну нормалізацію коренів слів, покращуючи оновлення наборів даних для використання.

Результати та обговорення

На основі вирізок новин про кібератаки на Україну було побудовано спрямовану семантичну мережу з використанням методологічно обґрунтованого процесу візуалізації та аналізу основних семантичних зв'язків у наборі даних за допомогою генеративного ШІ. Результатом цього процесу стало 50 семантичних пар на кожну стрічку новин загальною ємністю 25,000, які були відфільтровані за ступенем їх взаємозв'язку, залишивши по 20 релевантних пар на кожну новину. В результаті було оброблено

семантичних пар 10,000, з яких після нормалізації було отримано 1576, що сформували остаточний набір даних для аналізу.

На основі описаного процесу ми побудували репрезентативну візуалізацію, показану на Рис. 1, яка ефективно відображає взаємодію різних об'єктів у мережі. Розмір кожного вузла визначався довжиною імені об'єкта, а зв'язок між вузлами зображувався за допомогою кольорової схеми - від зеленого (низький зв'язок) до червоного (високий зв'язок), що ілюструє важливість і частоту взаємодії кожного об'єкта в мережі.

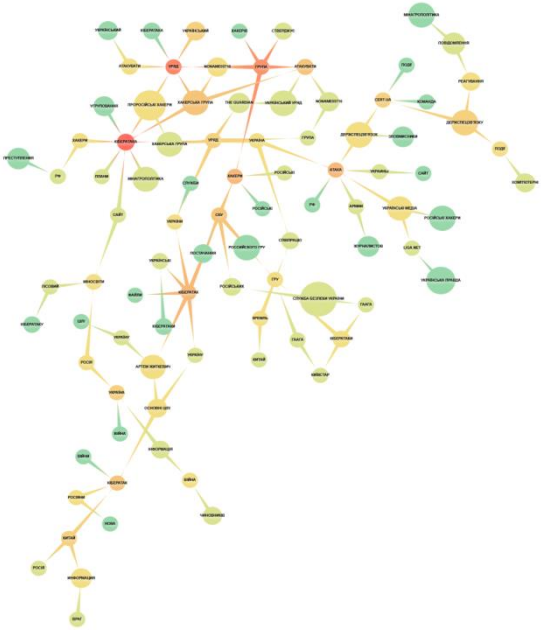


Рисунок 1 - Семантична мережа пар сутностей опрацьованих новинних видань

Подальший аналіз, включаючи оцінку центральності та ідентифікацію спільнот, дозволив глибше зрозуміти структуру мережі та ролі конкретних суб'єктів у ній. Аналіз

центральності визначив Україну, кібератаки та Міністерство освіти як центральні вузли, що мають вирішальне значення для підтримання узгодженості та потоків у мережі, як показано в Штаб. 1.

Близькість до центру продемонструвала, що такі організації, як Росія, Україна та Міністерство освіти, є не лише центральними, але й сильно впливають на інформацію в мережі, позиціонуючи їх як ключових акторів у реагуванні на інциденти, описані іншими вузлами. Крім того, використання методів виявлення спільнот ефективно ідентифікує групи в мережі, висвітлюючи різноманітні моделі взаємодії та зв'язки, починаючи від прямого впливу кібератак і закінчуючи ширшими геополітичними та освітніми впливами.

Таблиця 1. Значення типів центральності об’єктів в семантичній мережі

	Ступінь	Близькість
Україна	0.278	0.376
Росія	0.222	0.248
Кібератака	0.222	0.324
Мін-освіти	0.167	0.268
Китай	0.167	0.268

Висновки

Було використано передові методи обробки природної мови та генеративний ШІ для аналізу великого набору даних із вирізок новин про кібератаки, пов'язані з Україною. Використовуючи такі методи, як NER та побудова семантичних мереж, ми успішно виділили та проаналізували лінгвістичні зв'язки між текстовими об'єктами.

Описаний процес підвищує якість даних і розширює потенціал для виявлення ключових закономірностей і

зв'язків, які не є очевидними за допомогою традиційних методів.

Крім того, наша методологія демонструє ефективність мультимодальних підходів у дослідженнях кібербезпеки, де гнучкість і швидкість генеративного ШІ поглиблюють розуміння кіберзагроз та інформаційних війн.

Результати цієї роботи потенційно можуть бути використані для формування політики, посилення заходів безпеки та сприяти зміцненню глобальної кібербезпеки. Розширюючи межі аналізу тексту за допомогою штучного інтелекту, ця робота поглиблює наше розуміння кіберзагроз і створює основу для ефективної аналітики в галузі кібербезпеки та інших сферах.

Перелік використаних джерел

1. Dmytro Lande L. S. GPT Semantic Networking: A Dream of the Semantic Web - The Time is Now. — ISBN 978-966-2344-94-3. — 2023. — 168 p.
2. Koubaa A. GPT-4 vs. GPT-3.5: A Concise Showdown — 2023 — DOI: 10.20944/preprints2023 03.0422.v1.
3. Indurkhya N., Damerau F. J. Handbook of natural language processing. — CRC Press, 2010. — 2010. — 676 p.
4. Jianpeng Cheng L. D., Lapata M. Longshort-term memory-networks for machine reading // Conference on Empirical Methods in Natural LanguageProcess- ing. — 2016. — P. 551–561— DOI:10.48550/arXiv.1601.06733.
5. Dmitro Lande Anatolii Feher L. S. Cybersecurity in AI-Driven Casual Network Formation // Theoretical and Applied Cybersecurity. — 2023. — Vol. 5–Issue 2. — P. 105–113. — DOI:10.20535/tacs.2664-29132023.2.287139.

МЕТОД УПРАВЛІННЯ ДОСТУПОМ В МЕДИЧНІЙ СИСТЕМІ

В. М. Клиш, Ю. В. Баришев

Вінницький національний технічний університет, Вінниця, Україна
vklysh71@gmail.com, yuriy.baryshev@vntu.edu.ua

У роботі розглядається управління доступом до критичних інформаційних систем на прикладі медичних закладів. Визначено принципи, за якими працюють дозволи, і представлено стани дозволів. Для доведення концепції створено кілька ролей та обговорено правила визначення дозволів у випадку наявності декількох ролей у одного користувача.

Робота спрямована на створення системи управління доступом до медичних даних, використовуючи розмежування прав доступу, що сприяє покращеному захисту критичних систем від несанкціонованого доступу.

Ключові слова: кібербезпека, критична інфраструктура, медична таємниця, персональні дані, розмежування прав доступу, захист даних.

Вступ

Управління доступом до критичних інформаційних систем відіграє важливу роль для безпеки даних від несанкціонованого доступу. Тому надзвичайно важливо обмежити доступ до медичних даних лише для тих користувачів, які мають необхідні повноваження, оскільки несанкціонований доступ до такої інформації може призвести до серйозних наслідків, включаючи порушення приватності та конфіденційності, а також можливість втрати життя або погіршення стану здоров'я пацієнтів. Використання розмежування прав доступу в цьому контексті дозволяє точно визначати, які користувачі мають доступ до даних. Такий підхід сприяє підвищенню рівня захисту медичних даних та забезпечує їхню безпеку та цілісність.

Аналіз різних моделей розмежування прав доступу показав, що найдоцільнішою для управління доступом до

медичних систем є модель управління доступом на основі ролей (Role-Based Access Control, RBAC) [1, 2]. Основна перевага цієї моделі полягає у тому, що вона базується на ролях, тому адміністратору не потрібно вручну налаштовувати дозволи новим користувачам. Кожній ролі вже призначені відповідні дозволи, що робить процес управління доступом швидким та гнучким.

Метою роботи є покращення управління доступом до медичних даних.

Для досягнення цієї мети необхідно розв'язати низку завдань: визначити права, розробити ролі, надати ролі користувачам.

Обґрунтування станів дозволів та розробка ролей

Перед створенням ролей, спочатку треба визначити принципи за яким працюватимуть дозволи.

Кожному дозволу може бути надано один із трьох станів:

- дозволено (1) – право виконувати певну дію в системі;
- заборонено (0) – заборона на право виконувати певну дію в системі;
- невизначено (null) – відсутність специфікованого дозволу або заборони на виконання певної дії.

Після розгляду принципів специфікації прав доступу, наступним кроком є розробка ролей, які будуть використовуватися в медичній системі. Ролі визначають набір дозволів, які користувач отримує при призначенні відповідної ролі.

Для доведення концепції розроблено приклад набору ролей, наведений в Таблиці 1.

Роль «адміністратор» надає користувачеві повний доступ до управління системою, окрім доступу до даних пацієнтів. Ця роль призначається обмеженому колу осіб, щоб мінімізувати ризик неправильного використання повноважень.

Роль «сімейний лікар» надає користувачеві доступ до роботи з даними пацієнтів. Сімейні лікарі можуть змінювати свої дані, але не мають визначеного дозволу для редагування токенів чи ролей.

Таблиця 1 – Ролі та дозволи

Дія	Адміністратор	Сімейний лікар	Інтерн
Створення нового користувача	1	0	0
Зміна даних користувача	1	1	null
Видалення користувача	1	0	0
Створення токена	1	null	0
Видалення токена	1	null	0
Створення ролі	1	null	0
Видалення ролі	1	null	0
Редагування ролі	1	null	0
Доступ до системи	null	1	null

Роль «інтерн» не надає користувачеві жодного дозволу, лише два невизначених: змінювати свої дані та доступ до даних пацієнтів.

У випадку, коли користувач має дві ролі діє система, при якій визначення дозволів відбувається за наступними правилами:

- якщо хоча б один дозвіл має «-», тоді, дія заборонена;
- якщо дозволи мають «null», тоді дія заборонена;
- якщо дозволи мають «+» та «null», тоді дія дозволена.

Такі правила забезпечують чітке і безпечне управління доступом, оскільки унеможливлюють виконання дій, які можуть бути потенційно небезпечними або несанкціонованими. Наприклад, якщо користувач одночасно є інтерном і сімейним лікарем, він отримає доступ лише до тих дій, які явно дозволені обома ролями або однією з них при умові, що інша не забороняє ці дії.

Висновки

Запровадження системи управління доступом на основі ролей (RBAC) у медичних інформаційних системах є

критично важливим для забезпечення безпеки даних пацієнтів. Чітко визначені ролі та дозволи дозволяють керувати доступом до інформації, мінімізувати ризики несанкціонованого доступу та забезпечити безпеку персональним даним пацієнтів.

Перелік використаних джерел

1. Zhang, Y., Joshi, J.B. Role-Based Access Control. Encyclopedia of Database Systems. Springer, New York, 2018. P. 3252–3258 DOI: 10.1007/978-1-4614-8265-9_320 (date of access: 20.05.2024).

2. Liu Z., Gu W., Xia J. Review of access control model. Computers, materials & continua. 2019. Vol. 61, no. 3. P. 43–50. DOI: 10.32604/jcs.2019.06070 (date of access: 21.05.2024).

ВПЛИВ ФІШИНГОВИХ АТАК НА ПСИХОЛОГІЧНЕ БЛАГОПОЛУЧЧЯ

Вітомський Ю.Л.[1], Бондаренко С.Ю.[2]

[1]Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Київ, Україна
u.vitomskyi@gmail.com
[2]КТЗК ЦКБ ННІ ІБ СК НА СБ України, Київ, Україна
bondarenko.stephan@ukr.net

Фішингові атаки, поширена форма кіберзлочинності, використовують тактику соціальної інженерії, щоб обманом змусити людей розкрити конфіденційну інформацію. У цій науковій роботі досліджується глибокий вплив фішингових атак на психологічне благополуччя жертв. Завдяки огляду існуючої літератури, аналізу психологічних теорій та представленню емпіричних даних, ця робота має на меті з'ясувати наслідки фішингових атак для психічного здоров'я. Отримані дані свідчать про те, що ці атаки можуть призвести до значного психологічного дистресу, включаючи тривогу, депресію, а також всепроникне відчуття порушення та недовіри. Наприкінці авторами наведено рекомендації щодо пом'якшення цих наслідків та підвищення кіберстійкості.

Ключові слова: кіберпсихологія, фішингові атаки, соціальна інженерія, кібержертва.

Вступ

Фішингові атаки становлять значну загрозу в цифрову епоху, використовуючи обманні методи для маніпулювання людьми, щоб змусити їх розкрити особисту інформацію, таку як паролі, номери кредитних карток та інші конфіденційні дані. Ці атаки мають не лише фінансові наслідки, але й глибокий психологічний вплив на жертв. Розуміння психологічного впливу фішингових атак має вирішальне значення для розробки комплексних стратегій

кібербезпеки, які враховують не лише технічні, а й людські аспекти кіберстійкості.

Фішинг, за визначенням Робочої групи з боротьби з фішингом (APWG) – це кіберзлочин, який використовує замасковані електронні листи, веб-сайти або інші форми комунікації, щоб обманом змусити людей надати конфіденційну інформацію [1]. Незважаючи на розвиток технологій кібербезпеки, фішинг залишається постійною загрозою, що еволюціонує, оскільки зловмисники постійно вдосконалюють свої методи, щоб перехитрити системи захисту. Доведено, що кіберзлочинність, в тому числі фішинг, має значний психологічний вплив на жертв. Дослідження задокументували почуття безпорадності, гніву та страху серед жертв різних форм кіберзлочинності. Однак психологічний вплив саме фішингу залишається недостатньо вивченим порівняно з іншими формами кіберзлочинності.

Теорія когнітивної оцінки стверджує, що емоційна реакція на подію визначається оцінкою події людиною та її ресурсами подолання. Жертви фішингових атак можуть оцінювати подію як значну загрозу їхній особистій безпеці та відчувати, що вони не в змозі впоратися з нею, що призводить до підвищеної тривоги та стресу. Фішингові атаки можуть сприйматися як травматичні події, особливо якщо вони призводять до значних фінансових втрат або крадіжки особистих даних. Теорія травми припускає, що такий досвід може призвести до посттравматичного стресового розладу (ПТСР) та інших довгострокових психологічних проблем. Теорія соціального навчання підкреслює роль засвоєних моделей поведінки та соціального контексту у формуванні реакції людини на фішингові атаки. Жертви, які спостерігали або пережили попередні кіберзлочини, можуть мати підвищену чутливість і вразливість до нових атак.

Дослідження показують, що жертви фішингових атак часто відчувають цілий ряд психологічних наслідків, зокрема наступне [2]. Багато жертв повідомляють про високий рівень тривоги та стресу після атаки, викликаний занепокоєнням щодо особистої безпеки та фінансової

стабільності. Відчуття порушення та безпорадності може призвести до депресивних симптомів, особливо якщо напад призвів до значних фінансових втрат або втрати ідентичності. Фішингові атаки можуть підірвати довіру до онлайн-середовища, що робить жертв більш обережними у цифровій взаємодії та знижує загальну якість їхнього життя. Кількісні дані були зібрані за допомогою стандартизованих інструментів психологічної оцінки, включаючи шкалу генералізованого тривожного розладу з 7 пунктів (GAD-7), Опитувальник здоров'я пацієнта-9 (PHQ-9) для депресії та Контрольний список ПТСР для DSM-5 (PCL-5). Якісні дані були отримані за допомогою напівструктурованих інтерв'ю.

Кількісні дані були проаналізовані за допомогою статистичного програмного забезпечення для виявлення кореляцій між віктимізацією від фішингу та психологічним дистрессом. Якісні дані були проаналізовані за допомогою тематичного аналізу для виявлення спільних тем і стратегій подолання. кількісний аналіз виявив значний рівень психологічного стресу серед жертв фішингу. Основні висновки включають: 1) тривога: 62% учасників повідомили про помірні та сильні симптоми тривоги, а середній бал за шкалою GAD-7 склав 12,4; 2) депресія: 48% учасників мали депресивні симптоми від помірного до важкого ступеня, а середній бал за опитувальником PHQ-9 склав 15,7; 3) ПТСР: 35% учасників відповідали критеріям ПТСР, на що вказували бали за опитувальником PCL-5. Результати цього дослідження підкреслюють значний психологічний вплив фішингових атак. Висока поширеність тривоги, депресії та посттравматичного стресового розладу серед жертв підкреслює потребу в послугах психологічної підтримки на додаток до технічних рішень для боротьби з кіберзлочинністю. Ці результати свідчать про те, що комплексні стратегії кібербезпеки повинні включати психологічну підтримку та освіту, щоб допомогти жертвам оговтатися від атак і виробити стійкість до майбутніх загроз. Організаціям слід розглянути можливість впровадження програм підтримки та

інформаційних кампаній, спрямованих на емоційні та психологічні аспекти кіберзлочинності.

Висновки

Фішингові атаки мають глибокий вплив на психологічний стан жертв, призводячи до значної тривоги, депресії та посттравматичного стресового розладу. Подолання цих психологічних наслідків має вирішальне значення для розробки комплексних стратегій кібербезпеки. Майбутні дослідження повинні вивчати довгострокові психологічні наслідки фішингу та ефективність різних заходів підтримки.

Список використаних джерел

1. The psychological impact of phishing attacks on employees. Home of Cybersecurity News URL: https://cybermagazine.com/articles/the-psychological-impact-of-phishing-attacks-on-your-employe (дата звернення: 23.05.2024).
2. The Use Of Psychology In Phishing Attacks. Packetlabs. URL: https://www.packetlabs.net/posts/psychology-of-phishing-attacks/ (дата звернення: 23.05.2024).

СЦЕНАРІЇ АТАК НА ХОСТИНГ АУДІОКНИГ

Кіреєнко О.В.

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»,
м. Київ, Україна
kirealex12@gmail.com

В роботі представлено сценарії атак на інформаційну систему типу "хостинг аудіокниг". Розглядаються атаки здійснені зовнішніми порушниками та атаки з боку авторів контенту. окремо описані атаки на службові підсистеми та модулі хостингу, такі як синтезатор мови, рейтинг та класифікація контенту.

Ключові слова: Аудіокнига, порушник, цифровий підпис, watermark, хостинг, синтезатор мови

Вступ

Розробка моделі порушника є необхідним кроком при побудові захищеної інформаційної системи. Передбачення дій порушника дозволяє впроваджувати спеціалізовані засоби захисту, націлені на відповідні атаки. Найбільш ефективними є моделі, що розробляють під конкретну інформаційну систему. Трохи нижче за рівнем деталізації знаходяться моделі для деякого типу інформаційних систем. Саме така модель буде розглядатися в даній роботі.

Інформаційна система типу "хостинг аудіокниг" може на перший погляд здаватися нецікавою ціллю в порівнянні із соціальними мережами, системами онлайн банкінгу, відеоіграми, що містять платний контент, проте це не означає, що дані системи не потрібно захищати взагалі. Якщо порушник не може досягти успіху при атаці деякої пріоритетної цілі (наприклад онлайн банку), він може спробувати провести атаку на більш просту і можливо менш прибуткову систему. Сайт хостинг аудіокниг є такою другорядною ціллю.

Атаки на інфраструктуру

Більшість “класичних атак”. Особливу увагу приділити **несанкціонованому завантаженню об’єкту.**

Метою даної атаки є завантаження деякого файлу, необов’язково в аудіоформаті, для його зберігання системою. В цій атаці порушник використовує нашу систему як додатковий жорсткий диск. Файл може містити шкідливе ПЗ або заборонений контент, але конкретно в цій атаці ключовим є саме зберігання даної інформації. Доступ до неї інших користувачів порушника не цікавить, хоча і може стати опосередковано додатковим джерелом збитків для нашої системи

Атаки на інформацію в системі

Видалення аудіокниги

Порушник може використовувати вбудовані механізми пошуку та сортування контенту.

З**авантаження фрагменту аудіокниги, що перевищує дозволений обсяг для ознайомлення.**

Аудіофайл може бути “стиснутий” за допомогою програми audacity або іншого ПЗ.

Доступ до облікових даних користувачів.

Для отримання їх електронних адрес та розсилання спаму чи іншого шкідливого ПЗ.

Доступ до програми синтезатора мови.

Якщо оригінальний файл аудіокниги пошкоджено або втрачено, в нашій системі може бути передбачено можливість читання тексту вголос комп’ютерною програмою – синтезатором людського голосу. Порушник може бути зацікавлений у використанні даного модуля нашої системи, так як якісні програми синтезатори є платним ПЗ

Доступ до книги в текстовому вигляді

Система можу зберігати текстовий варіант книги для синтезатора мови.

Підміна аудіокниги

Порушення в механізмі замовлення паперового примірника

Атаки на модуль перекладу

Порушник може отримати доступ до модуля системи, що відповідає за переклад книг, і використати його у власних цілях.

Атаки на систему рейтингу

Порушник може впливати на оцінки наявних книг, що буде змінювати їх порядок в списку рекомендацій.

Атаки на систему класифікації книги

Порушник може вплинути на призначені книги теги стосовно жанру та інших параметрів, тим самим зробити пошук даної книги більш складним або неможливим

Видалення частини об'єкту

Користувач-жертва буде шукати пропущений матеріал на іншому сайті такого ж типу (недобросовісна конкуренція).

Атаки на рекламні матеріали на сайті

Підміна посилань або самого контенту

Перенесення об'єкту із категорії вільного доступу до категорії преміум доступу або навпаки.

Блокує або відкриває доступ до контенту для користувачів

Атаки на відмову в обслуговуванні приносять прибуток порушнику опосередковано.

Захист аудіоконтенту

В першу чергу потрібно розуміти, що на відміну від зображень та відео, ми не можемо використовувати водяний знак (watermark) без погіршення якості звуку. Якість водяного знаку обернено пропорційна кількості

шуму. Люди не хочуть слухати аудіокнигу із якимось шумом.

Аудіофайли займають менше місця ніж відео тієї ж довжини, але у випадку із аудіокнигами ці файли є досить довгими. Для великих файлів процедура цифрового підпису ускладнена. ЦП треба застосовувати не до самого файлу, а до його гешу.

Якщо файл розбити на декілька частин (окремі розділи книги) то підписувати потрібно кожен із них.

Аналіз аудіоконтенту є складною задачею. На відміну від тексту, який можна легко перевірити, виконавши пошук заборонених слів по файлу, аудіофайли потрібно прослуховувати. Це означає, що швидкість розгляду скарг від користувачів, які повідомляють нам про проблемний контент, є досить обмеженою і цим може скористатися порушник.

Висновки

Серед атак спрямованих на хостинг аудіокниг найбільш проблемними є атаки, що призначені для обходу обмежень на контент. Завантаження контенту із преміум доступом у вигляді відкритого для всіх контенту, а також завантаження у відкритий доступ більше ніж визначений обсяг матеріалу для ознайомлення, спричинятимуть матеріальні та репутаційні збитки. Використання службових підсистем та модулів системи можливе, хоча і менш імовірне.

Список літератури

1. Chin-Yung Lin, "Watermarking and digital signature techniques for multimedia authentication and copyright protection", PhDThesis, ColumbiaUniversity, 2001.

2. S. K. Dubey and V. Chandra, “Steganography, cryptography and watermarking: A review,” International Journal of Innovative Research in Science,Engineering and Technology, vol. 6, no. 2, pp. 2595–2599, 2017.

МЕТОД БАЙТ-ОРІЄНТОВАНОГО ШИФРУВАННЯ НА ОСНОВІ ОЗНАК ДАНИХ

В.А. Лужецький, Т. Г. Кирилащук, В.Ю. Дворський

Вінницький національний технічний університет,
Вінниця, Україна
lva.kzi2002@gmail.com

В роботі запропоновано метод байт-орієнтованого шифрування, особливість якого полягає у використанні набору байтових операцій додавання та віднімання, що визначається за ознаками секретного ключа і даних.

Ключові слова: зашифрування, розшифрування, секретний ключ, ознаки даних.

Вступ

Важливою особливістю сучасного етапу розвитку Інтернет-технологій є значне збільшення пристроїв, що мають доступ до Інтернет, зокрема RFID-міток і безконтактних смарт-карток. Ці пристрої характеризуються значними обмеженнями на апаратні ресурси та енергоспоживання. Створення таких пристроїв базується на використанні алгоритмів LW-криптографії. «Легковагові алгоритми» шифрування мають забезпечувати компроміс між вартістю апаратної реалізації, рівнем безпеки і продуктивністю, який залежить від вимог конкретного застосування.

Найменші апаратні витрати на реалізацію потребують потокові LW-шифри MICKEY [1], Trivium [2] і GRAIN [3]. Однак і вони не задовольняють вимогам деяких застосувань зокрема пасивним RFID-міткам. Тому потрібні шифри, що будуть повною мірою задовольняти всі вимоги.

Мета дослідження

Метою є зменшення апаратних витрат на реалізацію шифру для пристроїв, що характеризуються значними

обмеженнями на апаратні ресурси та енергоспоживання.

Метод байт-орієнтованого шифрування на основі ознак даних

Повідомлення, що підлягає шифруванню, подається як сукупність байтів:

$$M = m_1, m_2, m_3, \dots, m_L.$$

Секретний ключ довжини 64 біт також подається як сукупність байтів:

$$K = k_1, k_2, k_3, \dots, k_8.$$

Зашифрування повідомлення відбувається шляхом виконання такої послідовності дій.

1. Встановлення початкових значень.

$$k_1^* = k_1, k_2^* = k_2, k_3^* = k_3, \dots, k_8^* = k_8;\ m_1^* = m_1.$$

2. Обчислення значення ознаки q виконуваної операції.

$$A = (k_7^* + k_8^*) mod 256.\ A = a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0,$$

де a_i - символи двійкового коду числа A.

$$(a_2 a_1 a_0) + (a_5 a_4 a_3) = p\ s_2 s_1 s_0,$$

де $s_2 s_1 s_0$ - двійковий код суми; $p \in \{0; 1\}$ – перенесення.

$$q = ((a_7 a_6 p) + (s_2 s_1 s_0)) mod 8.$$

3. Зашифрування байту.

$$\mathrm{c}_i = \left(m_1^* + k_{q+1}^*\right) mod 256.$$

4. Оновлення k_j^*.

$k_j^* = k_{j-1}^*$ для j від 2 до 8, $k_1^* = m_1^*$.

5. Оновлення m_1^*.

$m_1^* = m_i$ для i від 2 до L.

Зашифроване подається як сукупність байтів:

$$\mathrm{C} = \mathrm{c}_1, \mathrm{c}_2, \mathrm{c}_3, \dots, \mathrm{c}_L.$$

Для розшифрування повідомлення потрібно виконати таку послідовність дій.

1. Встановлення початкових значень:

$$k_1^* = k_1, k_2^* = k_2, k_3^* = k_3, \dots, k_8^* = k_8;\ \mathrm{c}_1^* = \mathrm{c}_1.$$

2. Обчислення значення ознаки q виконуваної операції.

$$A = (k_7^* + k_8^*) mod 256.\ A = a_7a_6a_5a_4a_3a_2a_1a_0,$$

де a_i - символи двійкового коду числа A.

$$(a_2a_1a_0) + (a_5a_4a_3) = p\ s_2s_1s_0,$$

де $s_2s_1s_0$ - двійковий код суми; $p \in \{0; 1\}$ – перенесення.

$$q = ((a_7a_6p) + (s_2s_1s_0)) mod 8.$$

3. Розшифрування байту.

$$m_i = \left(c_1^* - k_{q+1}^*\right) mod 256.$$

4. Оновлення k_j^*.

5. $k_j^* = k_{j-1}^*$ для j від 2 до 8, $k_1^* = c_1^*$.

6. Оновлення c_1^*.

$c_1^* = c_i$ для i від 2 до L.

Схема пристрою для шифрування

Для реалізації описаного методу шифрування пропонується пристрій, схему якого наведено на рис.1. Тут регістр Рг0 призначений для зберігання чергового байту відкритого повідомлення m_i (чергового байту зашифрованого повідомлення c_i), регістри Рг1-Рг8 спочатку зберігають 8 байтів секретного ключа, а потім байти $m_i(c_i)$. Блок формування ознак БФО керує мультиплексором для вибору відповідного байту.

Апаратна складність такого пристрою 740 GE бібліотеки елементів UMCL18G212T3. Для порівняння, апаратна складність реалізації MICKEY -1210 GE, Grain – 1760 GE і Trivium – 2390 GE.

Висновки

Особливості запропонованого методу шифрування полягають в тому, що гама формується з використанням секретного ключа та байтів повідомлення, а накладанням гами керують ознаки байтів. Апаратна складність реалізації такого методу від 1,64 до 3,23 разів менша за складність відомих алгоритмів потокового шифрування LW-криптографії.

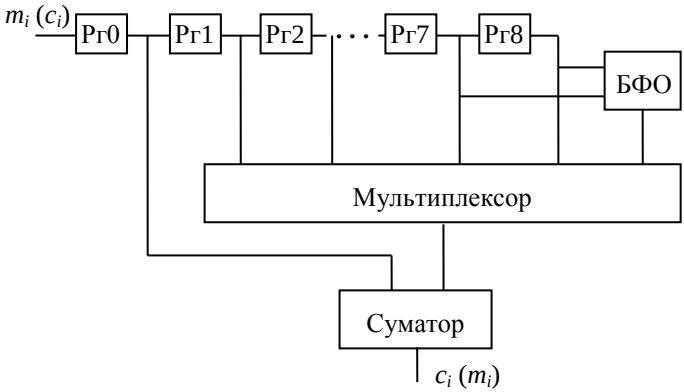


Рисунок 1. Схема пристрою для шифрування

Перелік використаних джерел

1. Babbage S., Dodd M. „The stream cipher Mickey-128“- eSTREAM proposal at http://www.ecrypt.eu.org/stream/ mickey128p2.html

2. De Canniere Ch., Preneel B. “Trivium Specifications” – eSTREAM proposal at http://www.ecrypt.eu.org/stream/ triviump2.html

3. Hell M., Johansson T., Meier W. “Grain – a stream cipher for constrained environments” – eSTREAM proposal at http://www.ecrypt.eu.org/stream/grainp2.html

МІЖРІВНЕВА СИСТЕМА ЗАХИСТУ WEB-СЕРВЕРУ

Р.Л. Пташкін[1], В.В. Палагін[2]

[1]Черкаський науково-дослідний експертно-криміналістичний центр МВС України,
[2]Черкаський державний технологічний університет
Черкаси, Україна
[1]ndekc.ck@gmail.com, [2]palahin@ukr.net

Дана робота присвячена питанню взаємодії між різними технологічними рішеннями, що в сучасності є найпопулярнішими при створенні web-серверів. Авторами запропонований метод реалізації взаємодії, що оснований на створенні файлових міток на рівні web-додатку з чітко визначеними типом та структурою. Різні технологічні рішення в ході обробки запитів користувачів мають аналізувати ці файлові мітки та здійснювати необхідні ситуативні заходи з забезпечення захисту. Метод дозволяє уникнути певних атак та забезпечує повне блокування зловмисника вже після здійснення ним першого запиту.

Ключові слова: Кіберзахист, web, nginx, php.

Вступ

В ході проведення аналізу популярності сучасних технологічних рішень, котрі застосовуються для створення web-серверів, встановлено, що безперечне лідерство займає симбіоз такого програмного забезпечення, як Nginx та Perl/PHP/Python під керуванням Linux-подібної операційної системи [1]. Якщо провести аналіз векторів здійснення кібератак та виділити найвразливіші технологічні рішення, то майже очевидним буде той факт, що переважна більшість вразливостей знаходиться на рівні web-додатків [1,2]. Якщо розглянути десять найсучасніших систем керування контентом, то можна стверджувати, що мова програмування PHP є фактичним лідером при створенні

web-ресурсів різних напрямків – від майданчиків інтернет магазинів до персоналізованих блогів.

Однією з проблем забезпечення належного рівня захисту web-додатків є фактична відсутність взаємодії між різними рівнями web-серверу. Тобто, в разі виявлення загрози на рівні web-додатку, відсутній алгоритм впливу на інші рівні web-серверу окрім, як зупинка виконання та виведення помилки. В той же час зловмисник, з метою вивчення інфраструктури, може циклічно переводити роботу web-додатку в режим помилки й поступово змінюючи вектор атаки виявити критичну вразливість [1].

Метою дослідження є здійснення ефективного аналізу сучасних технологій, що застосовуються для створення web-додатків, та здійснити пошук методів та алгоритмів, котрі б дали змогу розробити ефективну систему міжрівневої взаємодії різних технологій з подальшою побудовою багатошарової автоматизованої системи реагування на інциденти кібербезпеки.

Постановка проблеми

Якщо спростити структуру web-серверу та розглянути лише ключові його елементи, можна сформувати базовий маршрут виконання запиту користувача. Тобто, запит до web-ресурсу загалом буде переданий в програмний засіб web-серверу (nginx). В разі запиту статичного файлу запит буде завершений відвантаженням необхідного файлу. В разі звернення до файлу web-додатку запит буде переданий в оболонку мови програмування, де необхідний файл почне оброблятись інтерпретатором та виконуватись (рисунок 1) [3].

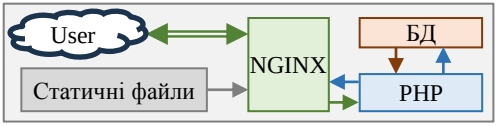


Рисунок 1 - Базова структура web-серверу

В такому режимі в разі виникнення загрози web-додаток має змогу лише повернути помилку. В той час, як на рівні web-серверу для зловмисника не відбудеться жодних змін.

Варіант вирішення

Авторами проаналізовано деякі готові технологічні рішення та наявні технології, котрі б дозволили реалізувати взаємодію між рівнем web-додатку та рівнем web-серверу. Одним з ефективних шляхів вирішення є створення на рівні програмного коду web-додатку певних стандартизованих файлових міток. Такі файлові мітки повинні містити необхідні відомості про запит та в автоматичному режимі аналізуватимуться на рівні web-серверу при обробці кожного запиту (рисунок 2).

Рисунок 2 - Структура web-серверу з файловими мітками

Реалізація навіть такого мінімального рівня взаємодії дозволяє в разі виявлення загрози миттєво блокувати не тільки поточний запит, а й всі подальші включно з запитами до статичних файлів. Блокування запитів одночасно унеможливлює здійснення атак циклічним переведенням web-додатку в режим помилки.

Обговорення результатів

Алгоритм захисту web-додатку з застосуванням файлових міток в тестовому режимі було запроваджено на одному з серверів з інформаційними ресурсами Черкаського науково-дослідного експертно-криміналістичного центру МВС України. Практична перевірка роботи здійснювалась як в синтетичних тестах, так й в «живому» режимі. Метою синтетичного тестування було порівняння швидкодії класичних налаштувань web-серверу та налаштувань з файловими мітками. В ході «живого» застосування було виявлено неочікувані результати – при переведенні web-додатку в режим створення файлових міток в разі виявлення підозрілих дій здійснювалось блокування суттєвої кількості запитів. В ході аналізу відомостей, зазначених в файлових мітках,

можливо ідентифікувати як автоматизовані атаки, так й цілеспрямовані запити, котрі мали на своїй меті дестабілізувати чи значно навантажити роботу web-додатку.

Висновки

В ході дослідження було проведено аналіз сучасних технологічних рішень для створення web-серверів та виділено найпопулярніші з них. Метою роботи було пошук підходів та методів здійснення ефективної взаємодії між різними рівнями серверу для здійснення фільтраційних заходів в разі виявлення кібератак чи загроз безпеки web-додатку.

Авторами запропоноване рішення, що основане на створенні певних файлових міток при виявленні загрози чи атаки. Така файлова мітка містить інформацію, котра в повній мірі дозволяє оцінити та проаналізувати загрозу, її походження та критичність.

В ході практичної перевірки дієвості запропонованих методів було встановлено не тільки їх дієвість у вже працюючих web-серверах, а й високу ефективність виявлення загроз. Фактична ефективність системи захисту в цілому суттєво залежить від ефективності аналізу запитів на рівні web-додатку.

Перелік використаних джерел

1. N. Shekokar, H. Vasudevan, S. Durbha, A. Michalas, T. Nagarhalli. Intelligent Approaches to Cyber Security. India: CRC Press, 2024. ISBN: 978-1-032-52161-9;

2. M. Zandstra. PHP 8 Objects, Patterns, and Practice: Mastering OO Enhancements, Design Patterns, and Essential Development Tools. UK: Apress, 2021;

3. D. DeJonghe. NGINX Cookbook. Advanced recipes for high-performance load balancing. 3nd Edition. USA: O'Reilly Media, 2024. ISBN: 978-1-098-15843-9.

ПОШУК УСІЧЕНИХ ДИФЕРЕНЦІАЛЬНИХ ХАРАКТЕРИСТИК СПЕЦІАЛЬНОГО ВИДУ ДЛЯ ШИФРУ LBLOCK

О. П. Якимчук, К. А. Медведцький

НН ФТІ, КПІ ім. Ігоря Сікорського, Київ, Україна

oleksii.yakymchuk@gmail.com, kostmedve-ipt24@lll.kpi.ua

У даній роботі показано можливість побудови диференціальних характеристик спеціального виду на рівні бітів для шифрів, що використовують операцію додавання за модулем два. Наведено високоймовірнісні диференціальні характеристики знайдені для легкого блокового шифру LBlock.

Ключові слова: диференціальний криптоаналіз, усічені диференціали, ймовірність диференціалу

Вступ

Усічений диференціальний криптоаналіз вперше був запропонований Ларсом Кнудсеном у 1994 році [1]. Його ідея полягає в розширені можливостей класичного диференціального криптоаналізу, бо різниці між текстами можуть бути визначені не повністю, а лише частково.

Альтернативний підхід до визначення усіченого диференціала та параметр стійкості до усіченого диференціального криптоаналізу були запропонований у роботі [2]. В нашій роботі пропонується перевірити можливість застосування запропонованого методу для перетворень, що використовують операцію додавання за модулем два та перевірити цей метод на шифрі LBlock [3].

1 Необхідні теоретичні відомості

В роботі [2] запропоновано вигляд усіченого диференціала як пара масок (A, B), де A, B – маски вхідних і вихідних різниць шифруючого перетворення, які визначені так: $\mathrm{A}, \mathrm{B} \in V_n^* = \{0,1,*\}^n$.

В такому випадку, в множині $\Delta(A)$ – всіх можливих різниць, що відповідають масці A – будуть знаходитися усі різниці, які задовольняють наступні умови:

- якщо в A на певній позиції стоїть 0 або 1, то і в різниці на цій позиції точно буде 0 або 1 відповідно;
- якщо в A на певній позиції стоїть *, то в різниці на тій позиції може бути як 0 так і 1.

Усіченою диференціальною характеристикою багатораундового шифруючого перетворення називаємо послідовність масок $A_1, A_2, \dots, A_r$, що є масками різниць між проміжними шифротекстами багатораундового шифруючого перетворення.

Ймовірність переходу маски A в маску B будемо обраховувати за формулою [2]:

$$TDP^f(A, B) = \frac{1}{2^n} \sum_{x \in V_n} [\forall \alpha' \in \Delta(A), \exists \beta' \in \Delta(B): f(x \oplus \alpha') = f(x) \oplus \beta'].$$

Ймовірність усіченої диференціальної характеристики $A_1, A_2, \dots, A_r$ обраховується як добуток всіх послідовних ймовірностей переходу маски A_i в маску A_{i+1}.

LBlock [3] – це легкий блоковий шифр на основі схеми Фейстеля з розміром блоку – 64 біти. Операція XOR застосовується для додавання лівої, після застосування раундової функції) та правої частин стану.

2 Пошук диференціальних характеристик для шифру LBlock

Визначимо як маски усічених диференціалів взаємодіють при застосування до них операції ⊕ (XOR) за допомогою таблиці істинності наведеної в таблиці 1. Якщо узагальнити, то будь-яка взаємодія з елементом * на виході дає результат – *, а для інших елементів діють звичайні правила операції XOR.

Для побудови усіченої диференціальної характеристики для шифру LBlock визначимо маску вхідної різниці, що визначає мінімальні зміни у вхідному тексті – $0^{63}1$.

Методом вибору після кожного раунду усіченого диференціалу з найбільшою ймовірністю було знайдено усічену характеристику для 10-ти раундів шифру LBlock, яка має ймовірність $ETDP = 8.7 \cdot 10^{-18} \approx 2^{-56}$. Кінцева вихідна маска має вигляд – $*^{56}\,01\,*^{6}$. Вона дає можливість передбачити зміну одного біту та не зміну ще одного біту вихідної послідовності після 10-ти раундів шифрування.

Таблиця 1. Таблиця застосування операції XOR для масок

A⊕B	**0**	**1**	*****
0	0	1	*
1	1	0	*
*****	*	*	*

Таким же методом, але вибираючи після кожного раунду усічений диференціал, вихідна маска якого не має елементів *, тобто маска точно співпадає з різницею, отримано диференціальну характеристику для 7-ми раундів шифру LBlock, яка має ймовірність $ETDP = 5.7 \cdot 10^{-14} \approx 2^{-44}$. При спробі продовжити цю диференціальну характеристику перетинається межа для ймовірності диференціальної характеристики в 2^{-64}, що робить вихідну різницю менш ймовірною ніж випадковий вибір будь-якого 64-бітового вектора.

Висновки

У даній роботі було показано можливість застосування методу побудови усічених диференціалів та диференціальних характеристик для перетворень, що використовують операцію додавання за модулем два. Було побудовано усічену диференціальну характеристику для 8-ми раундів шифру LBlock та звичайну диференціальну характеристику для 7-ми раундів цього ж шифру.

Перелік посилань

1. Knudsen L. Truncated and Higher Ordered Differentials. – 1008-е вид. – 1994. – с. 196 – 211. – URL: https://link.springer.com/chapter/10.1007/3-540-60590-8_16

2. Якимчук О. П. Метод оцінювання стійкості блокових шифрів до криптоаналізу на основі усічених диференціалів : магістерська дис. : 113 Прикладна математика / Якимчук Олексій Петрович. – Київ, 2020. – 69 с. – URL: https://ela.kpi.ua/handle/123456789/34327

3. Wenling W. LBlock: A Lightweight Block Cipher [Електронний ресурс] / W. Wenling, Z. Lei // Cryptology ePrint Archive, Paper 2011/345. – 2011. – URL: https://eprint.iacr.org/2011/345

АНАЛІЗ АТАК FGSM І МЕТОДІВ ЗАХИСТУ ВІД НИХ

М.В. Коломицев, Є. І. Ковальчук, С.О. Носок

НТУУ «КПІ ім. І. Сікорського», Навчально-науковий Фізико технічний інститут, м. Київ, Україна

kovalchuk.egor1357@gmail.com

На сьогоднішній день машинне навчання (ML) стає все більш популярним і використовується в різних сферах. Проте разом із зростанням застосування ML збільшується ймовірність атак на ці системи. Одним з найбільш поширених методів атак є Fast Gradient Sign Method (FGSM), який використовує градієнти моделі для створення адверсаріальних прикладів, здатних обманути модель [4]. У роботі детально аналізуються атаки FGSM та методи захисту від них, включаючи адверсаріальне навчання та фільтрацію шуму [2, 1]. Результати експериментів підтверджують ефективність розроблених методів захисту, що дозволяють підвищити стійкість систем машинного навчання до атак.

Ключові слова: машинне навчання, атаки, захист, безпека, адверсаріальні приклади, моделі, глибоке навчання, дані, нейронні мережі, вплив

Вступ

Атаки на системи машинного навчання (ML) ста- ють все більш серйозною загрозою із зростанням популярності цих систем та доступністю інформації щодо їх роботи. Зловмисники активно використо- вують різноманітні методи, такі як атаки на дані, моделі та алгоритми, щоб порушити функціонуван- ня систем ML та завдати шкоди їхнім користувачам. Одним з найбільш поширених методів атак є Fast Gradient Sign Method

(FGSM) [6]. Метою даної ро- боти є аналіз основних видів атак FGSM, розробка методів захисту від них.

Аналіз атак FGSM

Fast Gradient Sign Method (FGSM) є одним із най- більш відомих методів генерації адверсаріальних прикладів для атак на моделі машинного навчання, зокрема на нейронні мережі. FGSM використовує градієнти функції втрат моделі для створення но- вого зображення, яке мінімально відрізняється від оригіналу, але призводить до помилкової класифі- кації [3]. Він виробляє адверсаріальні приклади за формулою:

$$x' = x + \epsilon \cdot sign(\nabla J(\theta, x, y))$$

де - оригінальне зображення, ϵ - величина збуре- ння, - градієнт функції втрат, J - функція втрат моделі, θ - параметри моделі, - правильна мітка.

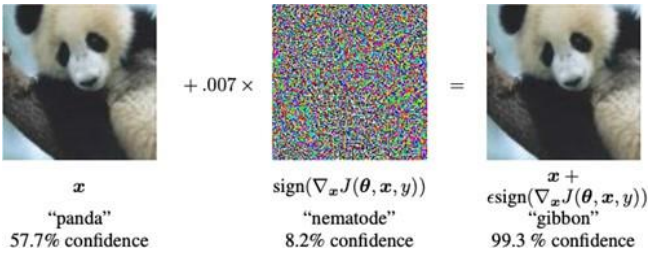


Рис. 1. Демонстрація FGSM

Існуючі підходи до захисту від атак FGSM

Існує декілька підходів до захисту від атак FGSM, зокрема:

- Адверсаріальне навчання: Модель навчається на адверсаріальних прикладах, що дозволяє їй краще розпізнавати та відкидати шкідливі зразки.

– Розширення даних (Data Augmentation): Додавання шуму до навчальних даних для покращення стійкості моделі до атак.

– Методи об’єднання моделей (Model Ensembling): Використання декількох моделей для прийняття рішень замість однієї.

– Gradient Masking: Цей метод знижує ефективність атак шляхом приховування або спотворен- ня градієнтів, які використовуються для генера- ції адверсаріальних прикладів [5].

Gradient Regularization: Регуляризація градієнтів включає додавання додаткових термінів до функції втрат, щоб зменшити чутливість моделі до невеликих змін у вхідних даних, що допома- гає підвищити стійкість до атак [1].

Методи захисту від атак FGSM

Адверсаріальне навчання є одним з найпопулярніших методів захисту від атак FGSM. Модель навчає-ться одночасно на оригінальних та адверсаріальних даних, що допомагає їй виявляти та відкидати шкі- дливі зразки. Це значно підвищує стійкість моделі до атак, але вимагає значних обчислювальних ресурсів і часу.

Методи об’єднання моделей (Model Ensembling) передбачають використання декількох моделей для прийняття рішень. Це підвищує стійкість системи до атак, оскільки кожна модель може мати різні вразливості, і атака, ефективна проти однієї моделі, може не спрацювати проти іншої.

Gradient Masking є методом, який зменшує ефективність атак шляхом спотворення або приховува- ння градієнтів, які використовуються для генерації адверсаріальних прикладів. Це досягається шляхом модифікації моделі або її тренувального процесу, щоб знизити інформацію, яку можна отримати з градієнтів. Хоча цей метод може значно зменшити успішність атак,

він не завжди забезпечує повний захист і може бути обійдений більш складними методами атак.

Gradient Regularization включає додавання додаткових термінів до функції втрат під час тренування моделі, щоб зменшити її чутливість до невеликих змін у вхідних даних. Це робить модель більш стій- кою до атак, оскільки навіть малі зміни у вхідних даних не викликають значних змін у виході моделі. Метод є досить ефективним, але може збільшувати обчислювальні витрати під час тренування.

Цей метод включає попередню обробку даних для виявлення і видалення потенційних адверсаріальних прикладів до того, як вони потрапляють на вхід мо- делі. Це може включати використання різних філь- трів, алгоритмів виявлення аномалій або методів очищення даних. Хоча захист на рівні даних може бути ефективним для запобігання деяким атакам, він може бути менш ефективним проти складних атак, які створюють приклади, що дуже схожі на реальні дані.

Експериментальна частина

Для оцінки ефективності методів захисту від атак FGSM було проведено серію експериментів з використанням моделей машинного навчання, навчених на датасеті CIFAR-10. Використовувались такі метрики, як точність класифікації, стійкість до атак та якість зображень після додавання обрахованого шуму.

Результати експериментів

Результати експериментів показали наступне:

1. Точність класифікації: Моделі, навчені з використанням адверсаріальних прикладів, показали підвищену точність класифікації на тестових наборах, які містять адверсаріальні приклади. Середня точність таких моделей становила 66.

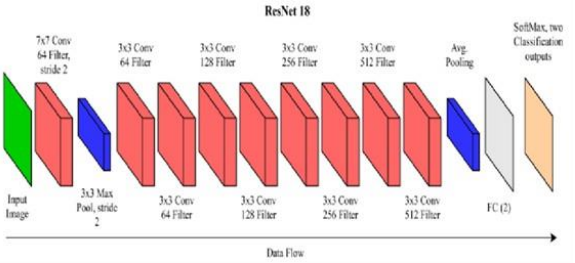


Рис. 2. Архітектура обраної для експериментів моделі

2. Стійкість до атак: Використання методів об'єднання моделей (Model Ensembling) значно підвищило стійкість систем до атак FGSM. Си- стема, що складається з п'яти моделей, показала вищу стійкість до атак, підвищивши точність на тестових адверсаріальних даних до 74
3. Візуалізація точності: Нижче наведені графіки точності для базової та адверсаріальної моделей. Вони ілюструють значну різницю в точності між базовою моделлю та моделлю, захищеною адверсаріальним навчанням, на тестових набо- рах з адверсаріальними прикладами. Зокрема, модель, захищена адверсаріальним навчанням, демонструє стабільніші результати на всіх набо- рах даних, що свідчить про її підвищену стій- кість до атак.
4. Порівняння точностей моделей: Результати по- казують, що адверсаріальна модель має кращу стійкість до атак, порівняно з базовою моделлю. Це підтверджується також іншими дослідження- ми, де зазначається, що адверсаріальні методи навчання підвищують загальну стійкість моде- лей до різних типів атак.
5. Порівняння точностей моделей: Результати по- казують, що адверсаріальна модель має кра- щу стійкість до атак, порівняно з базовою мо- деллю. Це свідчить про ефективність викори- стання

адверсаріального навчання та методів об’єднання моделей. В таблиці нижче наведе- но порівняння точностей моделей на чистих та адверсаріальних даних.

6. Графіки точностей: Порівняння точностей на чи- стих даних та на даних, згенерованих за допомо- гою FGSM, показує, що моделі, захищені адвер- саріальним навчанням та методами об’єднаннямоделей, демонструють значно кращі результа-ти у порівнянні з базовими моделями.

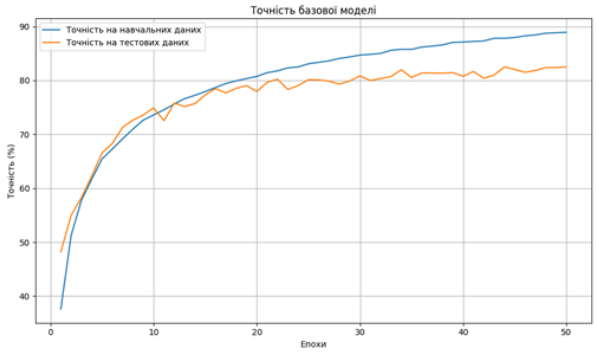


Рис. 3. Точність базової моделі

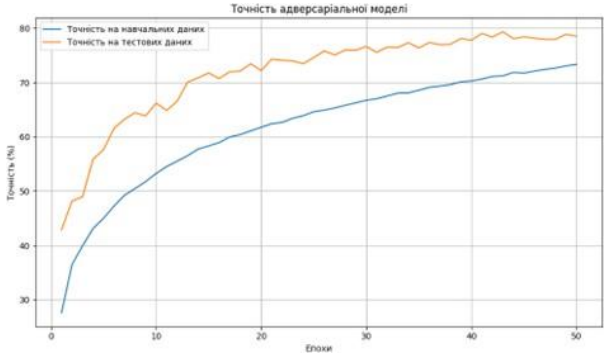


Рисунок 4 - Точність адверсаріальної моделі

Табл. 1. Точність моделей на чистих та адверсаріальних тестових даних

Model	Clean Acc (%)	Adv Acc (%)
Base	82	48
Adv	79	66
Ensemble	87	74
Adv. Ensemble	82	76

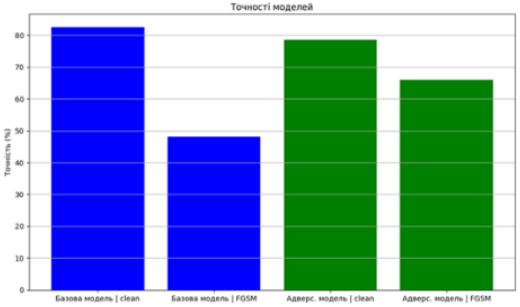


Рисунок 5 - Точності моделей на чистих та адверсаріаль- них даних

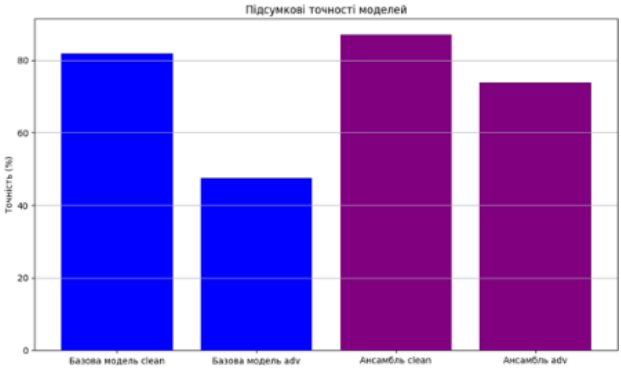


Рисунок 6 - Підсумкові точності моделей

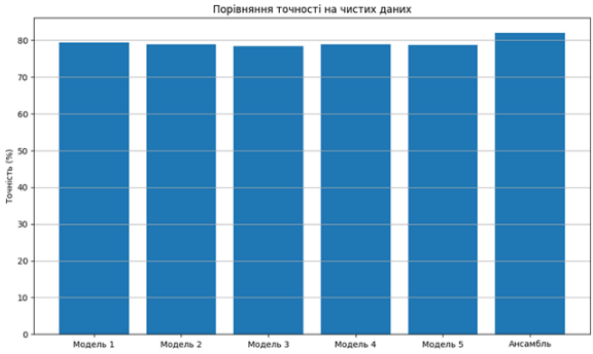


Рисунок 7 - Порівняння точності на чистих даних

Рисунок 8 - Порівняння точності на даних згенерованих за допомогою FGSM

Висновки

Атаки FGSM є серйозною загрозою для систем машинного навчання, але існує декілька ефективних методів захисту від них. Адверсаріальне навчання та методи об’єднання моделей значно підвищують стійкість моделей до атак. Результати експериментів підтверджують ефективність розроблених методів захисту, що дозволяє підвищити надійність і безпеку систем машинного навчання. Подальші дослідження

можуть бути спрямовані на оптимізацію цих методів та їх інтеграцію в реальні системи

Перелік використаних джерел

1. Adversarial Machine Learning: Attack Surfaces, De- fence Mechanisms, Learning Theories in Artificial Intelligence / A. S. Chivukula, X. Yang, B. Liu, W.Liu, W. Zhou. — 5th ed. — 2022. — 321 p. — URL:

2. https://www.amazon.com/Adversarial-Deep-Le arning- Cybersecurity- Taxonomies/dp/3030997 715.

3. Hall P., Curtis J., Pandey P. Machine Learning for High-Risk Applications. — 5th ed. — 2022. — 466 p. — URL: https://www.amazon.com/Machin e-Learning-High-Risk-Applications-Responsi ble/dp/1098102436f.

4. *Mądry A.*, *Schmidt L.* A Brief Introduction to Adversarial Examples.

5. *Mok K.* Google Develops 'Adversarial Example' Images that Fool Both Humans and Computers.

6. Overcoming Adversarial Attacks for Human-in-the- Loop Applications / R. McCoppin, M. Kennedy, P. Lukyanenko, S. Kennedy.

7. *Rosebrock A.* Adversarial images and attacks with Keras and TensorFlow. — 10/19/2018.

РОЗРОБКА МЕТАМОДЕЛІ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ РІЗНИХ РІВНІВ

Личик В.В., Гальчинський Л.Ю.

НТУУ «Київський політехнічний інститут імені Ігоря Сікорського». Україна, м. Київ

lychyk.vlad@gmail.com, hleonid@gmail.com

Концепція забезпечення кіберстійкості може бути застосована до різноманітних середовищ, які створила людина. Мова йде про ланцюги поставок, транспортні та логістичні мережі, і про таку актуальну наразі сферу для України, як теплова енергетика.

Ключові слова: кіберстійкість, метамодель, об'єкт критичної інфраструктури.

Вступ

Можна виділити такі найбільш повні та значимі методології кіберстійкості для різноманітних систем:

- методологія групи Лінкова;
- інженерна структура кібервідмовостійкості MITRE;
- методологія керування стійкістю CERT (CERT-RMM).

Методології лягають в основу розробки певних метрик та так званих фреймворків. Проте, дані методики дають змогу лише проводити якісну оцінку стійкості конкретних моделей, а не кількісну. Тому отримання конкретних моделей, спираючись на які можна проводити об'єктивне оцінювання резильєнтності, залишається відкритим питанням. Наразі кібербезпека хоч і залишається найбільш ключовою проблемою, проте охоплює лише сферу підтримки організацій та систем у певному початковому стані. Звідси слідує аспект відмовостійкості в цілому, а саме для систем, при наявності певних загроз. Таким

чином, завдання та проблематика лежать у площині передбачення цих раптових збоїв та у подальшій реакції на них. Тобто, необхідно розробити план дій для їх усунення, щоб система різного рівня могла повернутися із низької функціональності.

Виклад основного матеріалу

Абсолютна більшість сучасних систем, в тому числі тих, які відносяться і до критичної інфраструктури, мають величезну кількість рівнів та є складними у побудові. А тому і для таких об'єктів потрібні системи керування з багатьох рівнів. До того ж, необхідно також враховувати можливість виходу об'єкта критичної інфраструктури з ладу при відмові його контролера, тобто саму відмовостійкість та збій програмного, або ж апаратного забезпечення у активному положенні контролера. Що в свою чергу може негативно впливати на сам об'єкт критичної інфраструктури.

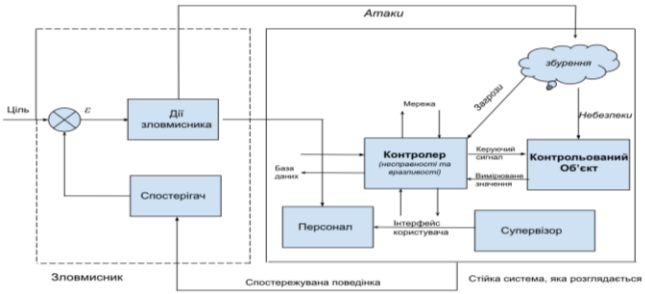


Рисунок 1 - Сучасна система керування об'єктом критичної інфраструктури

Наступним етапом є побудова метамоделі для узагальнених випадків, яка в свою чергу дає змогу перейти до створення моделей конкретних об'єктів та визначення кількісних показників, зокрема встановлення зв'язку між самою кіберстійкістю та ризиком.

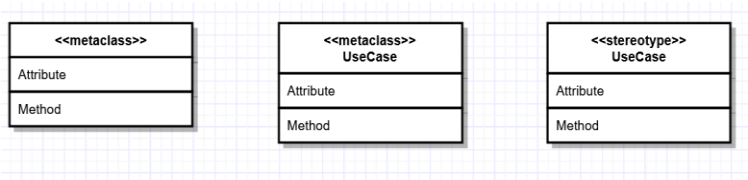


Рисунок 2 - Перший рівень метамоделі (ілюстративний концепт)

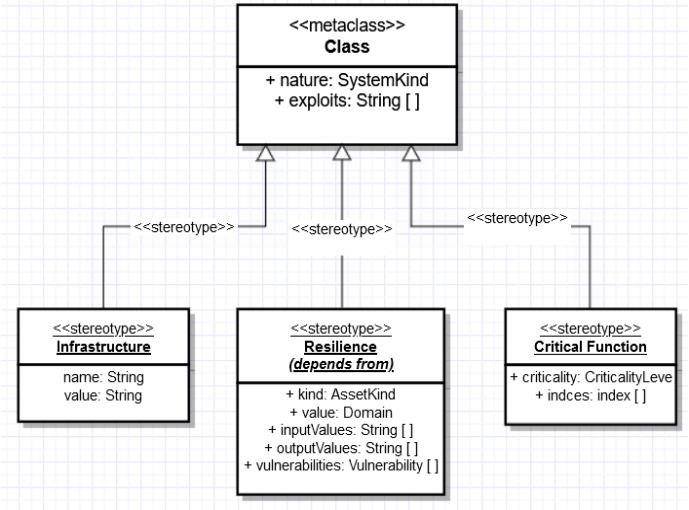


Рисунок 3 - Профіль кіберстійкості UML

Висновок

На даний момент найбільшою проблемою та водночас найбільш пріоритетною задачею є кількісна оцінка резильєтності, тобто перехід від якісних порівняльних характеристик конкретних методик до їх кількісних показників. В свою чергу, отримання метамоделі та її профілів UML-даних на різних доменах дає змогу перейти до побудови діаграми прецедентів. Що в свою чергу дозволить працювати з існуючими політиками безпеки на конкретних підприємствах та об’єктах критичної інфраструктури.

Перелік посилань

1. Janusz Zalewski, Steven Drager, William McKeever, Andrew J Kornecki, Denny Czejdo (2015). Modeling Resilience and Its Essential Components for Cyberphysical Systems. Conference: 2015 Federated Conference on Computer Science and Information Systems. https://doi.org/ 10.15439/2015F414

2. Гальчинський Л., Личик В. (2023). Метрики оцінки кібервідмовостійкості (аналітичне оглядове дослідження). *Інформаційні технології та суспільство*, 2 (8), 27-33. https://doi.org/10.32689/maup.it.2023.2.3

3. Linkov I., Baiardi F., Florin M.V., et al. Applying Resilience to Hybrid Threats. IEEE Secur. Priv. 2019, 17, 78–83. doi:10.1109/ MSEC.2019.2922866. Bellini, E.; Marrone, S.;Marulli, F. Cyber Resilience Meta-Modelling: The Railway Communication Case Study. Electronics 2021, 10, 583. https://doi.org/10.3390/electronics1005058

4. Bellini, E.; Marrone, S.; Marulli, F. Cyber Resilience Meta-Modelling: The Railway Communication Case Study. Electronics 2021, 10, 583. https://doi.org/10.3390/ electronics10050583.

5. Bodeau D, Graubart R, McQuaid R, Woodill J (2018) Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods. (The MITRE Corporation, Bedford, MA), MITRE Technical Report. https://www.mitre.org/sites/default/files/2021-11/prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

МЕТОД ДОВЕДЕННЯ НАЯВНОСТІ ТРАНЗАКЦІЇ НА ОСНОВІ КВАТЕРНАРНОГО ГЕШ-ДЕРЕВА

Лужецький В.А., Рогачевський Д.Б., Козира В.А.

Вінницький національний технічний університет,
Вінниця, Україна

v.luzhetskyi@vntu.edu.ua, dimonrogach@gmail.com,
vovakozira@gmail.com

Запропоновано метод доведення наявності транзакції на основі кватернарного геш-дерева. Наведено порівняльний аналіз з методом доведення на основі бінарного геш-дерева Меркля.

Ключові слова: доведення Меркля, бінарне геш-дерево, кватернарне геш-дерево.

Вступ

Технологія блокчейн набуває все більшого поширення в сучасному світі, відкриваючи нові можливості в різноманітних галузях завдяки високому рівню захищеності. Важливу роль в цій технології відіграє дерево Меркля.

Дерево Меркля дозволяє перевіряти наявність та цілісність транзакції з достатньо невеликою обчислювальною потужністю та пропускною здатністю [1]. Однак для деяких застосувань потрібно покращувати ці характеристики. Одним із підходів до цього є використання кватернарного дерева геш-значень.

Метод доведення Меркля

Для n даних висота бінарного геш-дерева дорівнює $\log_2 n$, а кількість геш-значень цього дерева обчислюється за формулою:

$$C_2 = n + \sum_{i=0}^{k} 2^i,$$

де $k =]log_2 n[- 1$.

За допомогою дерева Меркля нескладно довести наявність та цілісність певної транзакції з їх набору без передавання цього набору. Для перевірки потрібно лише надати транзакцію та шлях до кореня Меркля у вигляді набору геш-значень.

Якщо геш-значення, обчислене згідно зі шляхом, збігається з геш-значенням кореня Меркля, то транзакція є наявною та цілісною [2].

Нехай потрібно перевірити наявність і цілісність транзакції t_2 з бінарного геш-дерева, що складене для 16 транзакцій. Шлях до кореня Меркля буде складатися з геш-значень, які наведено на рис. 1.

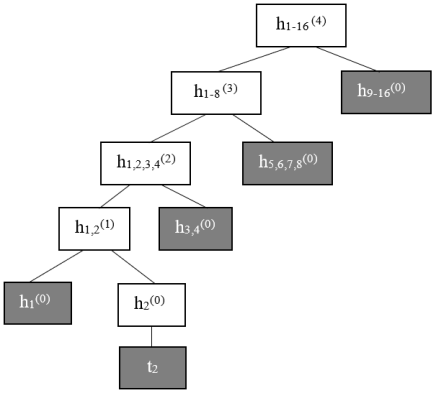


Рис 1. – Шлях від транзакції t_2 до кореня Меркля

Для бінарного геш-дерева, яке складається з n транзакцій, реалізація шляху потребує виконання $\log_2(n) + 1$ кроків. Шлях складається з $\log_2(n)$ геш-значень. У наведеному прикладі потрібно реалізувати 5 кроків обчислення геш-значень для 4 геш-значень і однієї транзакції.

Метод доведення на основі кватернарного геш-дерева

Кватернарне геш-дерево наведене на рис. 2 відрізняється від бінарного геш-дерева Меркля тим, що для отримання геш-значення наступного рівня потрібно

використовувати 4 геш-значення попереднього рівня замість 2. Саме це забезпечує меншу висоту кватернарного геш-дерева порівняно з бінарним.

Для n даних висота кватернарного геш-дерева дорівнює $\log_4 n$, а кількість геш-значень цього дерева обчислюється за формулою:

$$C_4 = n + \sum_{i=0}^{k} 4^i,$$

де $k =]log_4 n[- 1$.

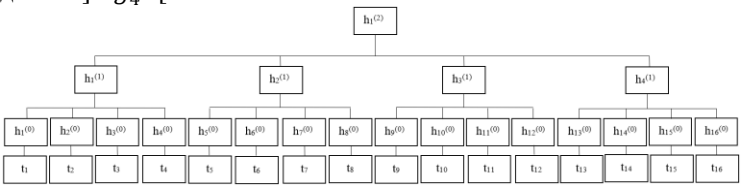


Рис 2. – Кватернарне геш-дерево

Отже, для зберігання кватернарного геш-дерева потрібно в 1,5 рази менше пам'яті порівняно з використанням бінарного геш-дерева.

Приклад шляху для доведення наявності та цілісності транзакції t_2 наведено на рис. 3.

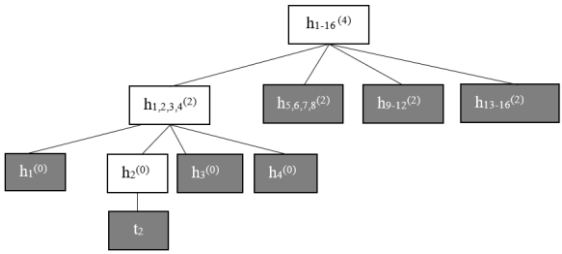


Рис 3. – Шлях від транзакції t_2 до кореня кватернарного геш-дерева

Для кватернарного геш-дерева, яке складається з n транзакцій, реалізація шляху потребує виконання $\log_4(n) + 1$ кроків. Шлях складається з $3 \times \log_4(n)$ геш-значень. У наведеному прикладі потрібно реалізувати 3 кроків обчислення геш-значень для 6 геш-значень і однієї транзакції.

Згортка 4 геш-значень до одного геш-значення може бути реалізована з використанням геш-функції на основі кватерніонів [3]. В цьому випадку складність доведення на основі кватернарного геш-дерева буде дорівнювати – $132(\log_4(n)+1)$ операцій, тоді як для бінарного дерева на основі SHA-256 потрібно виконати $320(\log_2(n)+1)$.

Наприклад, для n = 1024 кількість операцій зменшується в 4,44 рази.

Висновки

Кватернарне геш-дерево має такі переваги порівняно з бінарним геш-деревом:

1. Менший обсяг геш-значень для зберігання дерева.
2. Менший час побудови геш-дерева.
3. Пришвидшення процесу доведення.

Перелік використаних джерел

1. Що таке дерево Меркля і яка його роль у блокчейні ? URL: https://learn.bybit.com/ru/ blockchain/what-is-merkle-tree/ (дата звернення: 16.05.2024).

2. Дерева і доведення Меркля - INCRYPTED. INCRYPTED. URL: https://incrypted.com/ derevya-merkla/ (дата звернення: 19.05.2024).

3. Лужецький В. А., Баришев Ю. В. Підхід до паралельного гешування даних на основі моделі кватерніона. *Захист інформації і безпека інформаційних систем* : матеріали IX міжнар. науково-техн. конф., м. Львів, 25–26 трав. 2023 р. Львів, 2023. С. 81–82.

НАЦІОНАЛЬНА СИСТЕМА КІБЕРБЕЗПЕКИ: ЗАСАДИ РОЗБУДОВИ

Ящук Валентина Ігорівна,
Львівський державний університет безпеки життєдіяльності, Львів, Україна,
valentina.lender@gmail.com

Досліджено теоретичні та практичні аспекти формування та розвитку національної системи кібербезпеки України. Обґрунтовано необхідність створення комплексної системи кіберзахисту, що охоплює правові, організаційні, технічні та інші заходи. Визначено ключові принципи побудови національної системи кібербезпеки та охарактеризовано основні компоненти національної системи кібербезпеки. Запропоновано шляхи удосконалення національної системи кібербезпеки України.

Ключові слова: інформаційна безпека, стратегія кібербезпеки, система кібербезпеки, забезпечення кібербезпеки.

Вступ

XXI століття знаменується активним формуванням шостого технологічного укладу (біо-, нано-, інфо-, когнотехнологій, їх конвергенцією) та ризиками, з якими стикається цивілізація внаслідок упровадження новітніх технологій, зокрема їх використання у кіберпросторі.

Питома вага кіберзагроз у сфері загроз національній безпеці країн змінюється, і ця тенденція в процесі розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту зростає [1]. Посилення такого впливу на функціонування структур управління як національних, так і транснаціональних формує повністю нову безпекову ситуацію з викликами нового технологічного рівня. Міжнародні центри сили зазнають перерозподілу сфер впливу у кіберпросторі, збільшується їх бажання через такий поділ забезпечити втілення власних геополітичних інтересів.

Виклад основного матеріалу

Структуру Національної системи забезпечення кібербезпеки у розрізі рівнів управління наведено на рис.1.

Рисунок 1 - Національна система забезпечення кібербезпеки, розроблено автором на основі [2]

Кіберпростір разом з іншими територіями визнано одним з потенційних театрів воєнних дій, тому здатність держави захищати свої національні інтереси в ньому розглядається як важлива складова кібербезпеки. Набирає сили тенденція до створення нового типу військ – кібервійськ, до завдань яких входить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а також проведення превентивних наступальних операцій у кіберпросторі, спрямованих на ураження обчислювальних мереж та інформаційних систем збройних сил противника, а також виведення з ладу критично важливих об'єктів противника шляхом руйнування інформаційних систем, що керують такими об'єктами.

Водночас прогнозується зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у цифровому просторі, що проявлятимуться, насамперед, у розширенні кола країн, які намагатимуться створити власну кіберрозвідку, оволодіти передовими технологіями розвідувально-підривної діяльності у

кіберпросторі, посилити державний контроль за національними сегментами мережі Інтернет.

Негативною ознакою технологічного розвитку, пов'язаного із загальним поширенням цифрових технологій, розширенням Інтернет-середовища, є критично зростаючий технічний рівень інструментарію втілення кіберзагроз, від чого ландшафт таких загроз охоплює все більше сфер життєдіяльності. Кібератаки, їх різновиди стають все більш інтелектуальними та небезпечними, створюючи реальну загрозу критичній інфраструктурі.

Зловмисники активно працюють над пошуком вразливостей у активах (систем управління) і розробляють для цього унікальні за своїми характеристиками. Розширення використання кіберпростору терористичними організаціями (кібертероризм) стає глобальним трендом. Об'єктами терористичних кібератак є об'єкти атомної енергетики, системи управління електропостачанням, авіаційний та залізничний транспорт, магазини стратегічних видів сировини, системи водопостачання, а також хімічні й біологічні об'єкти.

Нові виклики приносить перехід на 5G-мережі, робота яких в суттєвій мірі залежить від правильної роботи програмного забезпечення, що через новизну технології може створити нові, не повністю передбачені загрози. Технології «Інтернету речей», «розширеної реальності», «розумних міст» активно доповнюються новими – «гіперавтоматизацією», «розумним компонуванням бізнесу», «кібербезпековою мережею», «розподіленою хмарою», «Інтернет-поведінкою» тощо.

Радикально змінюючи глобальний лад, пандемія коронавірусу COVID-19 матиме тривалий вплив на світовий порядок. Зростає залежність від цифрових засобів спілкування, що ставить під загрозу обмін інформацією, захист персональних даних. Поширення загроз та ускладнення їх впровадження змушує уряди провідних країн удосконалювати архітектуру національних систем кібербезпеки, змінювати стратегію протидії.

Швидкоплинний цифровий світ потребує формування більш збалансованої та ефективної національної системи

кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового оточення, забезпечуючи громадянам України безпечне функціонування національного сегмента кіберпростору та створюючи нові можливості для цифровізації всіх сфер суспільного життя.

Висновки

Все, викладене вище зумовлює необхідність дослідження засад розбудови національної системи кібербезпеки, відповідно до якої Україна прагне створити максимально відкритий, вільний, стабільний і безпечний кіберпростір, де враховуються права і свободи людини, підтримуються соціальний, політичний і економічний розвиток.

Список посилань

1. Ящук В.І. Роль та місце стратегії кібербезпеки України у забезпеченні інформаційної безпеки держави / В. І. Ящук // Moderní aspekty vědy: XLII. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. P. 259-286.

2. Стратегія кібербезпеки України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

3. Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392. [Електронний ресурс]. Режим доступу: https://www.president.gov.ua/documents/3922020-35037.

SYSTEM APPROACH TO THE INFORMATION SECURITY

Domarev V., Domarev D.

System approach of the in the information security process is a way of thinking and analysis, in obedience to which the security system is considered as an aggregate of interconnected elements, having a common goal – to provide the information security. The ISS creation process implies the establishing of a strict logical and functional connections between the heterogeneous security components. Thus, importance of the separate ISS elements properties decreases, and the general system tasks come forward. As the practice shows, the quality of the mentioned interconnections mainly determines the general efficiency of the protection system.

Representation model of the information security system

The IS model is presented on a Fig. 1 in the simplified form. The basic task of the model is the decision support of the ISS creation and functioning.

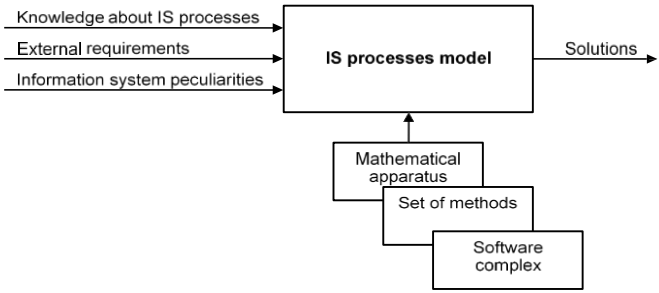


Fig. 1. Simplified representation of the IS model

Description of the approach to the formation of the IS model

Three coordinates are considered, being the three groups of IS model components (Fig. 2):

1. What does it consist of (BASES);

2. What is it intended for (DIRECTIONS);
3. How does it work (STAGES).

BASES, or component parts of almost any complex system (including information security systems) are:

1. Legislative, normative-legal and scientific base;
2. Structure and tasks of subdivisions, providing security of information technologies;
3. Organizationally-technical and regime means;
4. Program-technical methods and tools.

STAGES (sequence of steps) of the ISS creations, are based on existent methods of the ISS creation:

1. Determination of informational and technical assets;
2. Determination of set of possible threats and information loss channels;
3. Estimation of vulnerability and risks of information in the information system according to present set of threats and loss channels;
4. Determination of requirements to the information security system;
5. Choosing the means of information security providing and their specifications;
6. Introduction and organization of the use of the chosen methods and means of security;
7. Control of the integrity and management of the security system.

DIRECTIONS in providing security of information technologies are formed based on the specific features of information system. In general case, the following DIRECTIONS historically formed are considered:

1. Providing security of the information system objects;
2. Providing security of processes, procedures and programs for information processing;
3. Providing security of communication channels;
4. Suppression of side electromagnetic radiations;
5. Management of the security system.

All this can be presented as a "matrix" (fig. 3), which helps to unite logically the components of "BASES", "DIRECTIONS" and "STAGES" using the principle “each with each”. The matrix as a two-dimensional table is formed in

each case, based on the particular tasks of a definite ISS creation for certain information system.

The Matrix elements are numbered in the following way:

- first digit (X00) represents the number of the element in "STAGES" block,
- second digit (0X0) represents the number of the element in "DIRECTIONS" block,
- third digit (00X) represents the number of the element in "BASES" block.

Matrix elements representation

The content of each MATRIX element describes the interconnection of components in the created ISS. Such an approach gives an opportunity to build up the correct strategy in the creation of the complex security systems, constantly considering the logical connections between the numerous ISS elements and thus to get exactly a SYSTEM, but not a set of individual solutions.

Matrix properties

The offered ISS presentation model as a three-dimensional matrix allows not only the strict tracing of the interconnections between the security elements, but can also be used as an ISS creation guide. It is possible to start the creation of the security system from any of the offered general questions. When all the 140 answers will be ready, it will become clear, what is already present, and what is needed to achieve the set purpose.

To compose the ISS creation task, all 140 matrix elements are filled with the corresponding requirements, making a complete technical specification. Besides, it is possible to formulate the requirements based on any standards – international, European, Ukrainian, Russian, American, etc.

Using the approach based on the three-dimensional matrix, it is also possible to estimate the efficiency of ISS being created or already existent. Here, the corresponding estimations must be put by all the 140 indexes (matrix elements). All the evaluation methods are applicable.

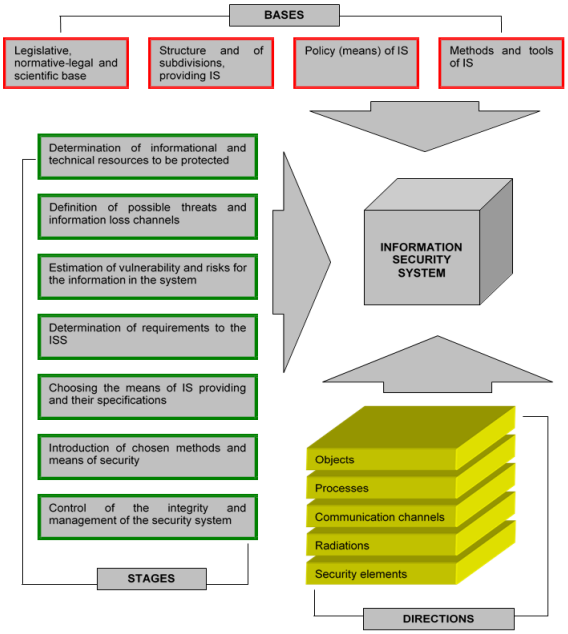


Fig. 2. IS components

<<< Stages	Directions >>>	010				020				030				040				050			
		Information system objects protection				Program and process security				Communication channels protection				Side radiations				Security system management			
	Bases >>>	Base	Structure	Measures	Means	Base	Structure	Measures	Means	Base	Structure	Measures	Means	Base	Structure	Measures	Means	Base	Structure	Measures	Means
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Determination of information to be protected	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Definition of threats and information loss channels	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Estimation of vulnerability and risks	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Determination of requirements to the ISS	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Choosing the means of IS providing	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Introduction and use of chosen methods and means	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Control of the integrity and management of the security	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Fig. 3. Matrix elements numeration

МАТЕМАТИЧНІ ПРИНЦИПИ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ RSA, ECC ТА AES: ЇХ ЗАСТОСУВАННЯ ДЛЯ ЗАХИСТУ КІБЕРПРОСТОРУ

Кобус О.С., Бондаренко С.Ю.

КТЗК ЦКБ ННІ ІБ СК НА СБ України, Київ, Україна

kobus_olena@ukr.net, bondarenko.stephan@ukr.net

Криптографічні алгоритми відіграють вирішальну роль у захисті інформації в кіберпросторі. авторами досліджуються математичні принципи, що лежать в основі трьох фундаментальних криптографічних алгоритмів: RSA (Rivest-Shamir-Adleman), ECC (криптографія еліптичних кривих) та AES (Advanced Encryption Standard). RSA покладається на обчислювальну складність факторизації великих цілих чисел, ECC базується на алгебраїчній структурі еліптичних кривих над скінченними полями, а AES використовує принципи перестановки та підстановки для створення безпечного шифрування з симетричним ключем. Проаналізовано застосування цих алгоритмів у захисті кіберпростору, висвітлено їхні сильні та слабкі сторони в різних контекстах безпеки. Дослідження підкреслює важливість вибору відповідних криптографічних методів на основі конкретних вимог безпеки, обчислювальної ефективності та стійкості до нових загроз.

Ключові слова: RSA, криптографія еліптичних кривих, вдосконалений стандарт шифрування, криптографічні алгоритми, захист кіберпростору, інформаційна безпека, криптографія з відкритим ключем, шифрування з симетричним ключем, обчислювальна складність, кібербезпека.

У цифрову епоху захист інформації має першорядне значення. Криптографічні алгоритми є невід'ємною частиною захисту комунікацій, забезпечення цілісності

даних та збереження конфіденційності. У цьому дослідженні ми розглянемо три фундаментальні криптографічні алгоритми: RSA, ECC та AES. В основі кожного алгоритму лежать окремі математичні принципи, які визначають його функціональність і безпеку.

RSA – це криптографічна система з відкритим ключем, яка ґрунтується на складності факторизації великих складених чисел. Алгоритм включає три основні етапи: генерацію ключа, шифрування та дешифрування. RSA - це криптографічна система з відкритим ключем, яка використовує складність факторизації великих складених чисел. Алгоритм був розроблений у 1977 році Роном Рівестом, Аді Шаміром та Леонардом Адлеманом [1]. Безпека RSA ґрунтується на теорії чисел, зокрема на властивостях простих чисел і модулярної арифметики. Процес генерації ключа полягає у виборі двох великих простих чисел і їх перемноженні для отримання складеного числа. Це складене число формує модуль, який використовується як в публічному, так і в приватному ключах. Вибирається відкрита експонента і обчислюється відповідна їй закрита експонента. Відкритий ключ складається з модуля і відкритого показника, тоді як закритий ключ складається з модуля і закритого показника.

В RSA шифрування виконується за допомогою відкритого ключа одержувача. Відкрите повідомлення перетворюється на зашифрований текст шляхом піднесення повідомлення до степеня відкритого ключа, а потім взяття модуля отриманого значення. Розшифрування виконується за допомогою закритого ключа в зворотному порядку: піднесенням зашифрованого тексту до степеня з приватним показником і взяттям модуля отриманого результату. Безпека RSA ґрунтується на обчислювальній складності розкладання складеного числа на прості множники. Хоча теоретично це просто, розкладання великих чисел на прості множники стає експоненціально складнішим зі збільшенням їх розміру [2, с. 174]. Це робить RSA безпечним для практичних цілей, припускаючи досить великі розміри ключів. Однак залежність RSA від великих

ключів може призвести до неефективності обчислень і зберігання даних.

Криптографія еліптичних кривих (ECC) базується на алгебраїчній структурі еліптичних кривих над скінченними полями. Запропонована незалежно Нілом Кобліцом і Віктором С. Міллером в середині 1980-х років, ECC пропонує інший підхід до криптографії з відкритим ключем, забезпечуючи еквівалентну безпеку традиційним алгоритмам, таким як RSA, але зі значно меншими розмірами ключів. Еліптична крива визначається рівнянням, і безпека ECC виникає з проблеми дискретного логарифмування еліптичних кривих (ECDLP). Ця проблема полягає в знаходженні скалярного множника за двома точками на кривій – завдання, яке є обчислювально нездійсненним за допомогою сучасних технологій. Генерація ключів ECC передбачає вибір випадкового цілого числа в якості закритого ключа і обчислення відповідного відкритого ключа шляхом виконання скалярного множення в заздалегідь визначеній точці на еліптичній кривій. Шифрування та дешифрування в ECC також покладаються на операції з точками еліптичної кривої, що гарантує безпечний зв'язок. Сила ECC полягає в його стійкості до ECDLP. Менші розміри ключів, необхідні для ECC у порівнянні з RSA, означають, що ECC може запропонувати швидші обчислення, знижене енергоспоживання і менше використання пам'яті. Така ефективність робить ECC особливо придатним для мобільних пристроїв та інших середовищ з обмеженими ресурсами. ECC використовується в різних додатках, включаючи безпечний перегляд веб-сторінок (TLS/SSL), зашифрований обмін повідомленнями та безпеку мобільних пристроїв.

Advanced Encryption Standard (AES) – це алгоритм шифрування з симетричним ключем, який шифрує дані блоками фіксованого розміру. AES був створений Національним інститутом стандартів і технологій (NIST) у 2001 році як заміна старому стандарту шифрування даних (DES). Алгоритм заснований на серії чітко визначених

перетворень, що застосовуються до блоку даних, забезпечуючи надійний захист від широкого спектру криптографічних атак. AES працює з блоками даних розміром 128 біт, з розмірами ключів 128, 192 або 256 біт. Процес шифрування включає кілька раундів перетворень, включаючи підстановку, перестановку і змішування, для перетворення відкритого тексту в зашифрований. Розшифрування полягає у зворотному перетворенні цих перетворень для отримання вихідного відкритого тексту.

Список використаних джерел:

1. Mathematics in cyber security. LinkedIn: Log In or Sign Up. URL: https://www.linkedin.com/pulse/mathematics-cyber-security-naveen-l-pcffc (дата звернення: 23.05.2024).
2. F. Mallouli, A. Hellal, N. S. Saeed, and F. A. Alzahrani, "A survey on cryptography: comparative study between RSA vs ECC algorithms, and RSA vs El-Gamal algorithms," in 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2019, pp. 173-176.

АЛГОРИТМИ ТА МЕТОДИ ЗАПОБІГАННЯ І ПРОТИДІЯ КІБЕРАТАКАМ

Борматов Р.С., Рог В.Є.
Харківський національний університет внутрішніх справ
https://orcid.org/0000-0002-7443-5125

Запобігання та протидія кібератакам є критично важливими для захисту інформаційних систем та даних. Сучасні кіберзагрози вимагають комплексного підходу, який включає використання різних алгоритмів та методів. Нижче розглянемо основні з них:

Впровадження засобів захисту

Засоби захисту включають різні технології та програмне забезпечення для забезпечення безпеки:

Антивірусні програми та антишпигунське ПЗ: захист від шкідливого програмного забезпечення.

Міжмережеві екрани (файрволи): контроль мережевого трафіку для запобігання несанкціонованого доступу.

Системи запобігання вторгненням (IPS): активний моніторинг та блокування підозрілого трафіку.

Шифрування даних: захист даних під час їх зберігання та передачі [1].

Алгоритми виявлення аномалій

Використання алгоритмів машинного навчання та штучного інтелекту для виявлення аномалій у поведінці користувачів та систем:

Алгоритми кластеризації: групування даних для виявлення нетипової поведінки.

Методи машинного навчання: навчання на основі історичних даних для прогнозування та виявлення аномалій.

Системи виявлення вторгнень (IDS): аналіз трафіку та поведінки систем для виявлення потенційних загроз [2].

Реакція на інциденти

Ефективна реакція на кіберінциденти включає:

План реагування на інциденти: розробка та впровадження чітких процедур реагування на інциденти.

Група реагування на інциденти (CSIRT): створення спеціалізованих команд для оперативного реагування на кіберінциденти.

Моніторинг та аналіз журналів: постійний моніторинг логів для виявлення та розслідування інцидентів.

Відновлення після атак

План відновлення після атак включає:

Резервне копіювання даних: регулярне створення резервних копій критичних даних.

План відновлення бізнесу: розробка та тестування планів відновлення бізнес-процесів після інцидентів.

Аналіз та покращення: після інциденту аналізуються причини та впроваджуються заходи для уникнення подібних ситуацій у майбутньому.

Висновок

Запобігання та протидія кібератакам вимагають комплексного підходу, який поєднує технічні, організаційні та освітні заходи. Важливо постійно адаптувати стратегії безпеки до нових загроз та регулярно оцінювати ефективність застосованих методів.

Література

1. Мережеве виявлення та реагування. Intelligent IT Distribution. URL: https://iitd.com.ua/merezheve-vijavlennja-ta-reaguvannja/ (дата звернення: 16.05.2024).

2. Желєзняк В.В., Мясіщев О.А., Лєнков С.В., Сєлюков Д.О. (2018) Аналіз методів та алгоритмів моніторингу обчислювальних мереж. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка, (58), 107–113. вилучено із https://miljournals.knu.ua/index.php/zbirnuk/article/view/293

МОДУЛЬ ВИДАВАННЯ ЕЛЕКТРОННИХ НАПРАВЛЕНЬ В МЕДИЧНИХ ЗАКЛАДАХ

В. С. Ланова, Ю.В. Баришев

Вінницький національний технічний університет

Вінниця, Україна

lanovaia02y@gmail.com,
yuriy.baryshev@vntu.edu.ua

У роботі проаналізовано процес видавання електронних направлень та вимоги до його кібербезпеки. Запропоновано підхід до захисту даних на основі гібридної моделі зберігання даних. Наведено результати реалізації та тестування модуля, який реалізує запропонований підхід.
Ключові слова: кібербезпека, персональні дані, критична інфраструктура, блокчейн, бази даних, медицина.

Вступ

Важливість захисту медичної інформації підкреслюється багатьма законодавчими актами, включаючи Загальний регламент з охорони даних (GDPR) [1] та Закон України «Про захист персональних даних» [2]. Недотримання цих вимог може призвести до штрафів.

Системи видавання електронних направлень залежно від реалізації мають недоліки або пов’язані з наявністю єдиної точки відмови, або зі зберіганням надлишкового обсягу даних і низькою продуктивністю.

Метою роботи є покращення захисту медичних даних, шляхом гібридного поєднання блокчейну та реляційної бази даних.

Для досягнення мети необхідно розв’язати такі завдання: розробити модель зберігання даних; розробити модуль видавання направлень; провести тестування.

Результати роботи

Для забезпечення стійкого рівня захисту персональних даних пацієнтів необхідно забезпечити захист цілісності,

доступності та конфіденційності. При цьому централізовані сховища сприяють забезпеченню конфіденційності, а децентралізовані — доступності та цілісності. Таким чином, доцільно поєднати централізовані та децентралізовані сховища зберігання даних, задля виконання поставлених вимог до захисту персональних даних [3].

Було розроблено модуль видавання електронних направлень на додаткові обстеження, який працює наступним чином: на веб-сторінці відкривається форма для внесення даних, які необхідні для формування направлення на додаткові обстеження (рис. 1). Після того, як направлення буде сформовано, лікар матиме змогу завантажити файл з усіма даними, які містяться в цьому направленні. Також розроблено систему оповіщення пацієнта через смс (рис. 2) та листом на пошту, де міститься номер направлення та спеціаліст, до якого направлення видано.

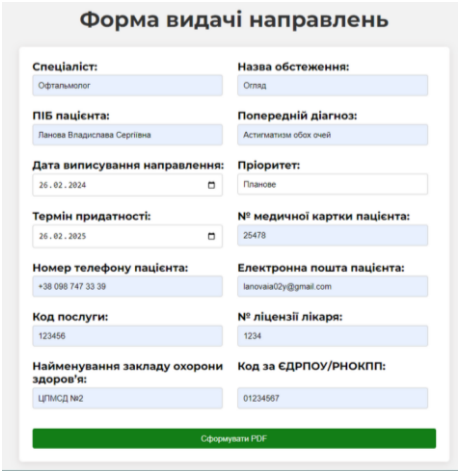


Рисунок 1 – Вигляд заповненої форми для видавання направлень

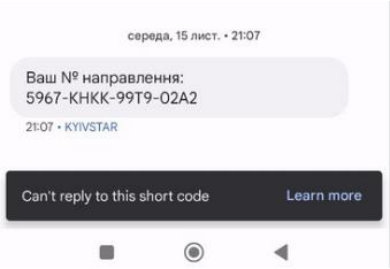


Рисунок 2 – Вигляд успішно надісланого смс на телефон

Розподіл даних поміж централізованим та децентралізованим сховищами дозволяє забезпечити належний рівень захисту конфіденційності даних, які там зберігаються. При цьому зберігання неконфіденційних даних в децентралізованих сховищах, наприклад в блокчейні, дозволяє покращити захист їх цілісності та доступності.

Висновки

Таким чином, можна зробити висновок, що розроблений модуль видавання електронних направлень на додаткові обстеження працює належним чином та має можливість бути впровадженим в медичну сферу в Україні, оскільки він передбачає захист одночасно трьох критеріїв захищеності: захист цілісності та доступності забезпечує блокчейн, а захист конфіденційності – реляційна база даних.

Гібридне поєднання централізованих та децентралізованих сховищ даних є адекватним рішенням та має можливість бути застосованим не лише в медицині, а й в освіті, а також для захисту інших об’єктів критичної інфраструктури.

Перелік використаних джерел

1. General Data Protection Regulation (GDPR), Official Journal of the European Union L 119, 04.05.2016; with cor. L

127, 23.05.2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed: 20.05.2024).

2. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. Дата оновлення: 27.04.2024. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 20.05.2024).

3. Баришев Ю., Ланова В. Метод захищеного зберігання медичних даних на основі реляційної бази даних та блокчейну. *Наукові праці ВНТУ*. № 3. URL: https://doi.org/10.31649/2307-5376-2023-3-9-17 (дата звернення: 20.05.2024).

COGNITIVE MODELING IN CYBERSECURITY: REVIEW, BASIC COGNITIVE MODEL OF CYBER THREAT

Nakonechna Yu.V.

Ihor Sikorsky KPI, Kyiv, Ukraine

nakonechna.yu@gmail.com

This paper proposes method that improves the comprehension of cognitive elements related to cybersecurity incidents by employing modeling using cognitive maps that depict essential processes and terms relevant to cybersecurity incidents, and allows to use computational methods to optimize defense measures.

Keywords: Cyber incident, cognitive model, threat, risk, suggestive influence, informational impact.

Introduction

Cognitive sciences combine psychology, linguistics, philosophy, computational and neurosciences to explore the human mind. In cyber security it enables incorporation of methods, security protocols, computer-generated knowledge, and expert insights. This integration, based on routine tasks, generates awareness of the cybersecurity landscape. In cybersecurity, cognitive modeling refers to R&D to replicate human thinking for understanding and predicting cyber attacks.

Problem

Cognitive modeling applications in cybersecurity are still relatively new and unexplored. Cyber attacks continue to pose significant threats despite advancements in cybersecurity. Prior to the attack, the attacker employs cognitive processes, such as reconnaissance, planning, and execution. Same goes for the defender. We propose a basic cognitive model blueprint based on fundamental terms: security, threat and risk to help in identifying and understanding the processes involved.

Cognitive models in cybersecurity

A cognitive model is a theoretical construct that represents the processes involved in human thinking, problem-solving, and understanding. In adaptive learning systems these models are essential for generating diagnostic reports, offering feedback, and enabling personalized evaluations [1].

Cognitive models in cybersecurity aim to gain insights into decision-making, behavior, and strategies [2]. The interrelationships between components in cyberspace are highly intricate, with each component interacting with others from society, economics, politics, information technology etc. These models can be used to understand human factors that impact cybersecurity and identify opportunities for automation in cybersecurity.

Conceptual framework

We construct a cognitive model in two stages. First creating an initial model around fundamental cyber incident aspects - threat, risk, countermeasures and attack (and their features) - and then refining it using cognitive attributes in three dimensions - Knowing, Applying and Reasoning [1]. This allows us to describe relations between cognition and data, knowledge and typical processes, involved in cyber incident, and visualize relationships between cyber incidents aspects hierarchically, determining most influential cognitive attributes and representing model as a knowledge graph.

Basic cognitive model of cyber threat

Cognitive modeling is a way to represent knowledge of systems which are characterized of uncertainty and complex processes. We will rely on a cognitive map which is a model of a studied system in the form of a directed graph defined using a set of sets:

$$CM =< C, F, W > \quad (1)$$

where $C = C_i$ is the set of graph vertices i.e., concepts or factors that have the greatest importance in terms of studying the

system being considered; $F = F_k$ is the set of edges representing the relationships between concepts;; $W = W_{ij}$ is the set of all edge weights (relationships). It is assumed that the connections between concepts can be positive - «strengthening» the influence of concept C_i on concept $C_j(W_{ij} > 0)$, or negative «weakening» the influence of concept C_i on concept C_j $(W_{ij} < 0)$.

In the simplest case, $W_{ij} = +1$ or $W_{ij} = -1$, in which case it is called a signed directed graph [3].

On the first stage of the model construction let us consider Threat, Risk, Attack Characteristics and Countermeasures as graph vertices, which are all connected with set of edges. Then we rely on Lockheed Martin's intrusion kill chain [4]: reconnaissance, weaponization, delivery, exploitation, installation, command and control, actions on objectives. As we accentuate on suggestive influence and informational impact as cyber incidents, aiming person, relying on psychological vulnerabilities and manipulation techniques, the adversaries exploit the target audience's susceptibility to misinformation, creating a cascading effect that can have far-reaching consequences.

On the second stage the model construction we define sub-models for each key concept (Threat, Risk, Attack Characteristics and Countermeasures), based both on Lockheed Martin's chain and Knowing, Applying and Reasoning as different dimensions on cognitive attributes. E.g. for Threat concept we define:

• Knowing: - Determination of types of threats. - Identification of sources of threats. - Understanding of threat mechanisms.

• Applying: - Use of information gathering methods to identify threats. - Using monitoring tools to track threats.

• Reasoning: - Analysis of collected information for threat assessment. - Building hypotheses regarding the potential impact of threats.

On the last stage we used cognitive mapping to set weights to the edges representing the relationships between concepts with expert-based approach. This allows us move to

mathematical modeling and possibility to evaluate mutual impact of concepts.

Summary

We propose a way to better understanding cognitive aspects of cybersecurity incidents through the usage of modeling via cognitive maps built around fundamental processes and key terms of cybersecurity incident, allowing to move cognitive processes to computational field which allows to optimize cyber incident countermeasures via cognitive attributes.

References

1. Siyu Sun, Xiaopeng Wu, Tianshu Xu, A Theoretical Framework for a Mathematical Cognitive Model for Adaptive Learning Systems // Behav. Sci. 2023, vol. 13, p. 406.

2. Vladislav D. Veksler, Norbou Buchler, Blaine E. Hoffman, Daniel N. Cassenti, Char Sample, and Shridat Sugrim, Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users // Frontiers in Psichology, 2018, vol 9, article 691.

3. Nakonechna Y.V. Proposing of suggestive influence detection and classification method based on fuzzy logic and feature driven analysis // Theoretical and Applied Cybersecurity Theoretical and Applied Cybersecurity. – 2023.– Vol. 5, no. 1.

4. Sandeep Narayanan, Ashwinkumar Ganesan, Karuna Joshi, Tim Oates, Anupam Joshi and Tim Finin, Cognitive Techniques for Early Detection of Cybersecurity Events // 2018.

ДОБРОВІЛЬНА ГЕОГРАФІЧНА ІНФОРМАЦІЯ ТА ЇЇ РІЗНОВИДИ В ЗАДАЧАХ ПРИЙЯТТЯ РІШЕНЬ

С. Ю. Даншина
Національний аерокосмічний університет
ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна,

s.danshyna@khai.edu

У роботі проаналізовано світовий досвід створення і використання VGI, її переваги та особливості. Зазначено, що українська спільнота активно спирається на ці дані у засобах аналітики, створюючи інтерактивні карти, геопортали та картографічні сервіси. Також підтверджено, що створення VGI не суперечить сучасному законодавству, що потребує урахування певних ризиків від її використання.
Ключові слова: неогеографія, відкрити джерела інформації, краудсорсинг, картографування, геопортал

Вступ

Розповсюдження концепції Web 2.0 впливає на звичні галузі діяльності людини, стимулює розвиток академічних наук, формує їх нові напрямки. Неогеграфія – набір інструментів, технологій і методів online-картографування із залученням картографів-непрофесіоналів для актуалізації наявної інформації, її контролю, первинного створення локалізованих у просторі даних різної природи. Геопросторові технології перетворюються в web-технології, більш доступні для користувачів. Один із аспектів цього геовебу пов'язаний із краудсорсингом географічних даних та особливостями їх подання в Інтернеті. Для опису цього явища використовують різні терміни, найбільш поширеним з яких є «добровільна географічна інформація» [1].

VGI: її особливості та сфери застосування

Добровільна географічна інформація (Volunteered Geographic Information (VGI)) – просторово-пов'язаний контент користувачів, який збирають, обробляють і добровільно розповсюджують непрофесіонали з використанням картографічних систем [2, 3]. Особливості VGI наведено на рис. 1.

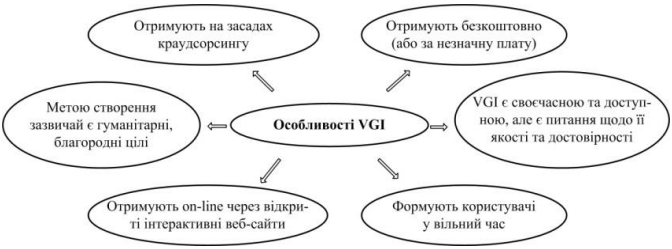


Рисунок 1 - Особливості добровільної географічної інформації

Незважаючи на те, що поняття VGI виникло нещодавно, фіксується значний науковий інтерес до цього виду інформації та її ролі у певних проєктах. Так, аналізуючи дані з бази наукових публікацій ScienceDirect (https://www.sciencedirect.com), зазначимо, що VGI в певних картографічних проєктах надає однаково точні дані, як і ті, що формують спеціальні картографічні агентства. При цьому в певних випадках VGI має перевагу перед більш дорогими засобами надання інформації – «очі на місцях»: оскільки учасники мають унікальні знання місцевих умов, мають доступ до певних подій тощо [2, 3]. Особливо це помітно в випадках надання інформації про наслідки стихійних лих, надзвичайних ситуацій, бойових дій та ін. При цьому основний недолік VGI – сумнівна якість і невисока достовірність – для певних проєктів спростовується численними дослідженнями: наприклад, дослідники CEGIS підтвердили точність VGI, надану до Національного картографічного корпусу, її включено до офіційних баз даних «Національної карти» [3, 4]. При

цьому мотивація волонтерів, їх небайдужість, прагнення до змін у соціальній культурі та поведінці приводять не лише до формування певної online - спільноти, але до реальних змін в організації суспільного життя, соціального оточення, в підвищенні доступності соціальних послуг тощо [2, 4].

Різновиди VGI та їх використання

Зазначені особливості та переваги використання VGI не залишилися непомітними: в Україні її успішно застосовують у картографічних сервісах і геопорталах. Серед таких прикладів відзначимо геопортал «Ecomapa» – інтерактивну карту Міністерства захисту довкілля та природних ресурсів України, інтерактивну карту Руйнувань – геопортал, створений за підтримки Міжнародного фонду «Відродження», Locator.ua – сервіс пошуку організацій і послуг на online - мапі України тощо. Тут, на відміну від класичного створення та використання VGI, її збирають і застосовують за сприянням певних владних органів і комерційних структур. Основною метою подібних сервісів, орієнтованих на використання VGI, є отримання зворотного зв'язку від громади задля покращення певних аспектів суспільного життя. Саме благородна ціль, прагнення зміни в навколишньому середовищі, контроль за діями адміністративних структур стимулює створення та надання цього типу інформації.

Також зазначимо існування певного виду географічної інформації, створення та розповсюдження якої стимулюється чинним законодавством, наприклад, Законами України «Про топографо-геодезичну та картографічну діяльність», «Про національну інфраструктуру геопросторових даних», Постановою Кабінету Міністрів України «Про порядок надходження, ведення обліку, зберігання та використання матеріалів Державного картографо-геодезичного фонду України, їх валідацію» та ін.

Наявне законодавство визначає правові та організаційні засади створення, функціонування та актуалізації геопросторових даних для ефективного прийняття

управлінських рішень, задоволення потреб суспільства в усіх видах географічної інформації тощо [5]. І хоча вважати цей вид інформації добровільною можна умовно, але реалізація принципу «…інтероперабельності та інтегрування геопросторових даних, одержаних з різних джерел» передбачає, що засобами краудсорсингу під час створення інфраструктури геопросторових даних нехтувати не можна.

Висновок

Таким чином, VGI – це тип інформації, який вже зараз є ефективним джерелом даних для прийняття управлінських рішень для задоволення потреб суспільства. Її поширення не лише на добровільних засадах стає корисним у засобах аналітики на основі відкритих джерел інформації. Але з урахуванням її особливостей слід уже зараз оцінювати та враховувати можливі ризики, пов'язані з її використанням і поширенням.

Перелік використаних джерел

1. Corbett, J., Legault, G. Neogeography: Rethinking Participatory Mapping and Place-Based Learning in the Age of the Geoweb // GIScience Teaching and Learning Perspectives: col. Monograph, Springer, 2019, P. 123 – 143.

2. Volunteered Geographic Information: Interpretation, Visualization and Social Context: collective monograph; edited by D. Burghardt, E. Demidova, D. A. Keim, Springer, 2024, 310 p.

3. Volunteered Geographic Information – Режим доступу: https://www.usgs.gov/

4. Goodchild, M. F. Assuring the quality of volunteered geographic information // Spatial Statistics, 2012, Vol. 1, P. 110 – 120. DOI: 10.1016/j.spasta.2012.03.002

5. Про національну інфраструктуру геопросторових даних: Закон України від 13 квітня 2020 р., № 554-IX // Відомості Верховної Ради, 2020, № 37, Ст. 277.

АНАЛІЗ ВПЛИВУ ВІЙСЬКОВИХ ДІЙ НА КЛІМАТИЧНІ ЗМІНИ

Кісіль Д.Д., Ковальова В.О.
Національний аерокосмічний університет
ім. М.Є. Жуковського «ХАІ»
М. Харків, Україна
kovalyova.vera.a@gmail.com

У даній роботі розглянуті параметри впливу військових дій на зміну кліматичної системи. Розроблено загальну схему таких параметрів з ціллю оновлення системи моніторингу навколишнього середовища із залученням спеціалістів різних сфер та рівнів.
Ключові слова: кліматична система, військові дії, викиди, моніторинг

Вступ

Активні бойові дії на території України впливають не тільки на розвиток країни, але і на кліматичну систему в цілому. Аналіз існуючих даних показав масштабність впливу, що обумовлює необхідність оновлення системи моніторингу енергетичного балансу кліматичної системи. Один із варіантів ефективних змін – дослідження кожного комплексного параметру впливу на кліматичні зміни із залученням спеціалістів різних сфер та рівнів. Метою роботи є підвищення ефективності системи моніторингу змін кліматичної системи в умовах проведення військових дій.

Основні показники зміни клімату

Багатомісячний військовий конфлікт, викликаний повномасштабним вторгненням Росії в Україну, завдає значних збитків і спричиняє гуманітарну кризу. Громадська інфраструктура зазнає постіних руйнувань, а навколишнє середовище потерпає від завданої шкоди. Ця війна негативно впливає на глобальний клімат, викликаючи значні викиди вуглекислого газу та інших парникових газів в атмосферу [1].

Найбільш використовуваним показником зміни клімату є середня температура Землі. Але цей показник не є найкращим індикатором стану клімату. Для його аналізу використовують загальне накопичення енергії кліматичною системою [2]. Зовнішній енергетичний баланс кліматичної системи змінюється через людську діяльність або через природні коливання Сонця чи вулканів. Зміна концентрації парникових газів, сонячної радіації чи кількість дрібних частинок у атмосфері призводить до зміни енергетичного балансу кліматичної системи. Наприклад, збільшення викидів парникових газів призведе до збереження більшої кількості теплового випромінювання у системі та викличе накопичення енергії. У атмосфері додаткова енергія йде нагрівання повітря. Це викликає зміни у різних шарах атмосфери. Це призводить до більш мінливої атмосфери, в якій вітри можуть стати сильнішими. Крім того, змінюється «гідрологічний цикл». Коли повітря нагрівається на 1 градус, воно може містити на 7 відсотків більше вологи, а це означатиме більше випаровування та опади і, отже, більший ризик повеней.

Вплив військових дій на зміни клімату

Понад 5% глобальних викидів пов'язані з конфліктами чи воєнними діями [3], але більшість країн приховують справжні масштаби викидів та їх впливу на енергетичний баланс кліматичної системи. В умовах, коли зміна клімату відбувається і прискорюється, дуже важливо зрозуміти і мінімізувати викиди від усіх видів громадської діяльності, чи то в мирний час, чи під час війни. Але викиди від військової діяльності потребують нових підходів до моніторингу навколишнього середовища.

Аналіз енергетичного балансу кліматичної системи повинен включати викиди CO_2 від польотів літаків, баків та палива від інших транспортних засобів, а також викиди, що утворюються під час виготовлення та вибуху бомб, артилерії та ракет. Таким чином, загальний аналіз впливу військових дій на енергетичну систему повинен включати наступні параметри: викиди CO_2 внаслідок військових дій;

пожежі; викиди, спричинені авіаційною діяльністю; реконструкція забудови; викиди, спричинені масовим переміщеням населення. У 2023 р. Міністерством охорони навколишнього середовища та природніх ресурсів України був проведений аналіз впливу військових дій на території України на зміни кламату [4]. Для більш детального аналізу потрібно розглядати кожний показник впливу як комплексний та аналізувати кожну складову. На рисунку 1 показана загальна схема аналізу впливу військових дій на кліматичні зміни. Для моніторингу ситауції необхідно визначити ряд показників, обов'язкових для реєстрації, та сформувати базу даних, з якою можуть працювати спеціалісти різних сфер.

Розподілення таблиць баз даних поміж спеціалістами різних сфер дасть можливість робити більш детальний аналіз з меншою кількістю припущень та ймовірних величин. При цьому варто зазначити, що одним із варіантів залучення спеціалістів може бути включення студентів відповідних спеціальностей до команди операторів баз даних. Це дасть можливість підвищити швидкість оновлення баз даних та водночас підготувати кваліфікованих спеціалістів.

Висновки

Посилення та продовження військових дій в Україні та в інших країнах призводить до глобальних змін кліматичної системи в цілому. Тому важливою задачею є реєстрація та аналіз такого впливу з ціллю зменшення навантаження на навколишнє середовище. Для цього було проведено аналіз різних досліджень впливу військових дій на кліматичні зміни. Розроблено систему параметрів для оцінки екологічнго стану навколишнього середовища.

Рисунок 1 – Аналіз впливу військових дій на клімат

Перелік посилань

1. Climate damage caused by Russia's war in Ukraine. [Електронний ресурс] URL: https://climatefocus.com/publications/climate-damage-caused-by-russias-war-in-ukraine/

2. Opvarmningens efterslæb. [Електронний ресурс] URL: https://www.dmi.dk/klima/temaforside -energiens-rejse-i-klimasystemet/opvarmningens-efterslab

3. Ny rapport fra FN's klimapanel. [Електронний ресурс] URL: https://www.dmi.dk/klima/temaforside-fns-klimapanel/sjette-hovedrapport-del1

4. Climate damage caused by Russia's war in Ukraine. [Електронний ресурс] URL: https://climatefocus.com/wp-content/uploads/2023/12/20231201_ClimateDamageWarUkraine18monthsEN.pdf

ОЦІНКИ СЕКРЕТНОСТІ ТА ВИТРАТ НА РЕАЛІЗАЦІЮ КРИПТОСИСТЕМИ НА ОСНОВІ ЛІНІЙНИХ РІВНЯНЬ З ВИКОРИСТАННЯМ ЛОГАРИФМІЧНИХ ПІДПИСІВ

Є. Котух[1], Г. Халімов[2]
[1]НТУ «Дніпровська Політехніка, Дніпро, Україна
[2]Харківський Національний Університет Радіоелектроніки, Харків, Україна
yevgenkotukh@gmail.com, hennadii.khalimov@nure.ua

Обчислювально складні задачі - «складні проблеми» для вирішення яких потрібно значний обсяг ресурсів. Криптографія використовує ці задачі як основу для створення безпечних схем. У доповіді представлено оцінки секретності та витрат на реалізацію криптосистеми на основі лінійних рівнянь з використанням логарифмічних підписів, що була розроблена авторами.
Ключові слова: лінійні рівняння, логарифмічний підпис, криптографія з відкритим ключем.

Вступ

До недавнього часу у криптографії з відкритим ключем широко використовувалися дві складні проблеми. Проблеми факторизації цілих чисел RSA та дискретного логарифмування в скінченних циклічних групах DLOG лежать в основі багатьох криптосистем [1-3]. У 1994 році Шор [4] показав, що ці класичні складні проблеми можуть бути легко розв'язані на квантовому комп'ютері. Квантовостійкі криптосистеми, засновані різних математичних підходах використовують обчислювально складні задачі [5]. Ми ризикнемо припустити, що будь-який криптоалгоритм, який має властивості регулярності у своїх структурованих даних, буде зламаний квантовим комп'ютером. Ми замінюємо поняття важкорозв'язної проблеми на задачу, що має множину рівнозначних розв'язків без регулярностей, коли всі розв'язки є

рівноймовірними. У представленій в [6] криптосистемі логарифмічна підпис є базовим криптопримітивом, що реалізує безключове шифрування і факторизацію за ключем логарифмічної підпису.

Оцінки секретності та витрат на реалізацію

Таблиця 1 - Витрати на ключі

m	Витрати на секретні ключі					Витрати на публічні ключі		
	$\lvert\beta_K\rvert = 2Km$ байт	$\lvert t_K\rvert = Km$ байт	$\lvert\tau_K\rvert = Km$ байт	$\lvert\psi\rvert = m^2$ байт	$\lvert\beta_K\rvert+\lvert t_K\rvert+\lvert\tau_K\rvert+\lvert\psi\rvert$ байт	$\lvert\gamma_K\rvert = \lvert\beta_K\rvert$ байт	$\lvert\lambda_K\rvert = \lvert\alpha_K\rvert$ байт	$\lvert\gamma_K\rvert+\lvert\lambda_K\rvert$ байт
8	256	128	128	8	520	256	32	288
16	1024	512	512	32	1080	1024	32	1056
32	4096	2048	2048	128	8320	4096	32	4128
64	16384	8192	8192	512	33280	16384	32	16416

Таблиця 2 - Витрати на розшифрування

m	Розмір шифру тексту U біт	Розмір шифру тексту V біт	Число множень λ_K на двійкову матрицю ψ розмірності $m \times m$	Число додавань $\gamma_K + \lambda_K$ m - бітових слів L	Число додавань $\gamma_K + \lambda_K$ зі словами $t_K + \tau_K$	Число додавань при наведенні системи лінійних рівнянь $L(K-L)/2$	Число обчислень β_K^{-1}
8	64	64	8	8	8	32	8
16	128	128	8	8	8	32	8
32	256	256	8	8	8	32	8
64	512	512	8	8	8	32	8

Таблиця 2 - Оцінки секретності

m	Атака вгадування через підбір вхідного тексту 2^{-Lm}	Атака грубої сили вгадування ψ 2^{-m^2}	Атака грубої сили вгадування ψ через записи у блоці $2^{-(m^2-m)}$	Атака на матрицю ψ через систему рівнянь 2^{-2m^2}
8	2^{-64}	2^{-64}	2^{-56}	2^{-128}
16	2^{-128}	2^{-256}	2^{-240}	2^{-512}
32	2^{-256}	2^{-1024}	2^{-992}	2^{-2048}
64	2^{-512}	2^{-4096}	2^{-4032}	2^{-8192}

Висновки

Для атаки пошуку вхідного тексту за заданим шифром тексту можлива квантова атака на основі алгоритму Гровера з експоненційною складністю . Звісно ж , що поліноміальні атаки на алгоритм не можливі дані в алгоритмі (записи масивів γ_{k_1,k_2} і λ_{k_1,k_2}) структуровані як випадкові набори без регулярностей . Криптосистема на основі неповний системи лінійних рівнянь щодо логарифмічних підписів є хорошим кандидатом для постквантової криптографії. Аналізуючи отримані результати в табл. 1-3 зазначимо, що в залежності режимів реалізації запропонована система визначає можливість гнучкого використання в рішенні задач захисту інформації в різних телекомунікаційних системах з різними вимогами, щодо параметрів криптографічно системи. Неповнота реалізована в алгоритмі для лінійних систем рівнянь гарантує нерозв'язність щодо секретних логарифмічних підписів та секретного матричного перетворення.

Література

1. Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public- key cryptosystems. Communications of the Association for Computing Machinery, 21(2):120–126, 1978

2. Michael O. Rabin. Digital signatures and public key functions as intractable as factorization. Technical Report MIT/LCS/TR- 212, Massachusetts Institute of Technology, January 1979.

3. Shafi Goldwasser and Silvio Micali. Probabilistic encryption and how to play mental poker keeping secret all partial information. In 14th ACM STOC, pages 365–377. ACM Press, May 1982

4. Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In 35th FOCS, pages 124–134. IEEE Computer Society Press, November 1994.

5. Robert J. McEliece. A public key cryptosystem based on algebraic coding theory. The deep space network progress report 42- 44, Jet Propulsion Laboratory, California Institute of Technology, January/February 1978. https://ipnpr.jpl. nasa.gov/progress_report2/42-44/44N.PDF.

6. Gennady Khalimov, Yevgen Kotukh, Maksym Kolisnyk, Svitlana Khalimova, Oleksandr Sievierinov. LINE: Cryptosystem based on linear equations for logarithmic signatures, Cryptology ePrint Archive, https://ia.cr/2024/697

МЕТОДОЛОГІЯ ЗАПОБІГАННЯ КОМП'ЮТЕРНИМ АТАКАМ НА ПРОМИСЛОВІ СИСТЕМИ НА ОСНОВІ АДАПТИВНОГО ПРОГНОЗУВАННЯ ТА САМОРЕГУЛЯЦІЇ

Костюк Ю.В.

Державний торговельно-економічний університет, 02156, м. Київ, Україна, kostyuk.yu@ukr.net

Робота присвячена розробці методології запобігання комп'ютерним атакам на сучасні промислові системи з використанням адаптивного прогнозування та саморегуляції. Методи продемонстрували ефективність у виявленні атак та забезпеченні безперервного функціонування ПС.

Ключові слова: промислові системи, комп'ютерні атаки, кіберстійкість, адаптивне прогнозування, саморегуляція, автоматична реконфігурація

Вступ

Стрімка цифровізація технологічної інфраструктури, розвиток хмарних і сенсорних технологій, концепції Інтернету речей привели до появи нової технологічної парадигми, що полягає у виникненні кіберфізичних систем, які інтегрують інформаційну та фізичну складові в єдиному виробничому циклі [1-3]. Цифровізація промислової інфраструктури відкрила широкі можливості для реалізації комп'ютерних атак, вектор яких змістився в бік несанкціонованого отримання можливості управління системою та порушення коректності її функціонування.

Постановка проблеми

Запобігання комп'ютерним атакам на промислові системи (ПС), що дозволяє не допустити виходу незворотних фізичних процесів з-під контролю, ускладнене через зростання кількості нових типів комп'ютерних атак,

обмежений час на протидію атакам та відсутність єдиної методології, що поєднує раннє виявлення атак і протидію їм [2-3]. Перелічені особливості визначають наукову проблему створення методології запобігання комп'ютерним атакам на ПС, тобто створити єдину методологію запобігання комп'ютерним атакам на промислові системи, спрямовану на випереджувальну саморегуляцію системи при прогнозуванні небажаних тенденцій у даних, що надходять від компонентів ПС. Основу підходу складають методи, що дозволяють на ранній стадії виявляти будь-які типи комп'ютерних атак і протидіяти їм шляхом автоматичної реконфігурації структури ПС.

Виклад основного матеріалу

Враховуючи високу варіативність протоколів обміну даними та велику кількість вразливостей у компонентах сучасних ПС, не можна виключати втрату контролю за потоками даних, що може призвести до прихованого нелегітимного впливу зловмисників на роботу ПС. Розв'язання задачі забезпечення інформаційної безпеки ускладнюється також необхідністю оперативної обробки великих обсягів різнорідних даних від компонентів ПС.

Завдання запобігання комп'ютерним атакам на ПС включають аналіз і адаптивний прогноз стану компонентів ПС, саморегуляцію структури ПС та оцінку кіберстійкості як інтегрального показника якості виконаного процесу саморегуляції. Методологія запобігання комп'ютерним атакам об'єднує методи прогнозування та саморегуляції, які виключають проведення атаки, а також оцінку збереження захищеності ПС шляхом формалізації умов кіберстійкості [1-2]. Принцип інваріантності полягає в універсальному представленні сукупності функцій інформаційної інфраструктури ПС, необхідних для формування середовища коректного перебігу фізичних процесів, та в ранньому виявленні будь-яких типів комп'ютерних атак, що забезпечить запас часу для реакції на атаку. Саморегуляція структури ПС повинна виконуватися таким чином, щоб виключити можливість реалізації комп'ютерної атаки або

нейтралізувати її наслідки [1-3]. Принцип кіберстійкості полягає в узгодженні процесів раннього виявлення комп'ютерних атак і саморегуляції структури ПС, а також у визначенні умов, за яких можливо збереження коректного функціонування ПС в умовах комп'ютерних атак. Така методологія спрямована на ПС з гнучкою, динамічною мережевою інфраструктурою та надлишковим складом компонентів і зв'язків між ними.

Методи виявлення комп'ютерних атак включають: мультифрактальний аналіз, дискретне вейвлет-перетворення та адаптивне прогнозування [1, 3]. Ці методи спрямовані на аналіз часових рядів з метою виявлення аномалій, які потенційно характеризують вплив комп'ютерної атаки на функціонування ПС.

Найкращі результати продемонстрував метод виявлення комп'ютерних атак на основі адаптивного прогнозування, який поєднує рекурсивний алгоритм фільтра Калмана та алгоритм машинного навчання Random Forest, що забезпечують раннє виявлення атаки шляхом адаптивної екстраполяції характеристик ПС та автоматичну класифікацію отриманих значень. Метод раннього виявлення комп'ютерних атак успішно виявив всі атаки завдяки точному передбаченню фільтром Калмана поведінки часових рядів як у нормальному стані, так і при атаках. Архітектура системи запобігання комп'ютерним атакам для ПС з розвиненою мережею інфраструктурою розроблена на прикладі інтелектуальних мереж енергопостачання (Smart Grid). У архітектурі враховано специфіку сучасних ПС, а саме: наявність механізмів взаємодії між фізичними та інформаційними складовими ПС; наявність об'єднань компонентів, які реалізують певні функціональні послідовності цільової функції; вимога до кіберстійкості та безперервності функціонування ПС; необхідність забезпечення саморегуляції ПС у разі збоїв або комп'ютерних атак; здатність системи запобігання атакам до накопичення знань і самонавчання, еволюційний захист.

Висновки

Таким чином, всі розглягуті методи продемонстрували свою ефективність у частині виявлення комп'ютерних атак на основі адаптивного прогнозування та в частині саморегуляції з використанням графів перекриттів. Методологія запобігання комп'ютерним атакам на сучасні промислові системи включає: графову модель функціонування ПС; адаптивне прогнозування шляхом екстраполяції часових рядів, сформованих із значень характеристик ПС; автоматичну реконфігурацію ПС, яка забезпечує кіберстійкість.

Список літератури

1. Куцаєв В. В. Радченко М. М. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла // Збірник наукових праць ВІТІ. Київ, 2018. Вип. 2. С. 67–76.
2. Субач І., Фесьоха В., Фесьоха Н. Фесьоха Н. О. Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі. Information Technology and Security. 2017. Т. 5, № 1. С. 29–41.
3. Zero-day polymorphic cyberattacks detection using fuzzy inference system / V. V. Fesokha et al. Austrian Journal of Technical and Natural Sciences. p. 8–13. URL: https://doi.org/10.29013/ajt-20-5.6-8-13.

ІНТЕЛЕКТУАЛЬНІ МЕТОДИ КІБЕРБЕЗПЕКИ

Виглазов В.С.

Харківський національний університет внутрішніх справ

vuglazovvadum@gmail.com

В тезах доповіді розглянуто застосування штучного інтелекту (ШІ) в сфері кібербезпеки, зокрема фокусуючись на його ролі як нового фронту в боротьбі за захист цифрового світу. Вказано ключові переваги ШІ, такі як автоматизація завдань, підвищення точності та ефективності, проактивна оборона та розширення масштабів. Наведено конкретні приклади застосування ШІ, зокрема у сфері виявлення аномалій, прогнозування та запобігання атакам, автоматизації реагування на інциденти та управлінні доступом.

Ключові слова: штучний інтелект, кібербезпека, кібернапад, захист даних, інформація, ідентифікація.

Вступ

Сучасний світ переповнений інформацією, а цифрова сфера стає все більш складною та вразливою. Кіберзагрози еволюціонують, стаючи все більш витонченими та складними для виявлення традиційними методами. Тому постає необхідність у нових, інноваційних рішеннях, які здатні не тільки протистояти, але й передбачати та запобігати кібернападам. І саме тут на допомогу приходить штучний інтелект (ШІ).

Виклад основного матеріалу

Інтелектуальні методи кібербезпеки ШІ — це новий фронт в боротьбі за цифровий світ. Їхні можливості відкривають безпрецедентні можливості для захисту даних та систем від загроз, які були раніше недоступні.

*Ключові переваги ШІ у сфері кібербезпеки***.** Автоматизація та швидке реагування: ШІ здатний автоматизувати рутинні завдання, як-от аналіз великих

обсягів даних та виявлення підозрілих активностей, що дозволяє економити час і ресурси.

Покращена точність та ефективність: ШІ-системи можуть аналізувати дані значно швидше та ефективніше, ніж люди, виявляючи тонкі аномалії та нестандартні поведінки, які можуть бути провісниками кібератак.

Проактивна оборона: ШІ може аналізувати великі обсяги даних, виявляючи потенційні загрози на ранніх стадіях, що дозволяє реагувати на них проактивно та запобігати атакам.

Розширення масштабів: ШІ може працювати з величезними обсягами даних та контролювати кібербезпеку в складних мережах, що неможливо зробити людині [1].

Приклади застосування ШІ у сфері кібербезпеки: Виявлення аномалій та зловмисних програм: ШІ-системи можуть аналізувати мережевий трафік, активність користувачів та програмне забезпечення, щоб виявити підозрілі патерни та зловмисні програми.

Прогнозування та запобігання атакам: ШІ може аналізувати великі обсяги даних та прогнозувати потенційні кіберзагрози, допомагаючи вчасно вживати заходів для їх запобігання.

Автоматизація відповіді на інциденти: ШІ може автоматизувати реагування на кібернапади, наприклад, блокуючи зловмисні дії або відновлюючи системи.

Управління доступів та ідентифікації: ШІ може використовуватись для підвищення безпеки систем шляхом аналізу поведінки користувачів та визначення ризиків[2].

Етичні та соціальні аспекти: Незважаючи на величезний потенціал ШІ у сфері кібербезпеки, існують і етичні, та соціальні аспекти, які потрібно враховувати.

Privacy concerns: ШІ-системи збирають величезні обсяги даних, що піднімає питання приватності і конфіденційності інформації.

Bias in AI: ШІ-системи можуть успадковувати упередження від даних, на яких вони навчаються, що може привести до дискримінації або неправильних рішень.

Job displacement: Автоматизація завдань ШІ може призвести до втрати робочих місць у сфері кібербезпеки.[3]

Висновки

Інтелектуальні методи кібербезпеки, незважаючи на свою прогресивність та ефективність, є лише одним з багатьох інструментів у боротьбі за безпеку в цифровому світі. Вони не замінюють, а доповнюють традиційні методи, надаючи нові можливості для виявлення та запобігання загрозам. Важливо пам'ятати, що кібербезпека – це не одноразова акція, а постійний процес адаптації до еволюціонуючих загроз. Інтелектуальні методи, такі як машинне навчання та аналітика великих даних, дозволяють нам швидше аналізувати великі обсяги інформації, виявляти нетипові патерни та спрогнозувати можливі атаки. Вони, як досвідчені детективи, збирають докази, вивчають сліди злочинців і допомагають розкривати злочини у цифровому світі.

Однак, не слід забувати про людський фактор. Навіть найдосконаліші технології потребують людського контролю та розуміння. Інтелектуальні методи – це лише інструмент, а не самостійний борець з кіберзлочинністю. Важливо розвивати людський капітал у сфері кібербезпеки, готувати фахівців, які вміють ефективно використовувати інтелектуальні методи та розуміти їх обмеження.

Нарешті, ключовим фактором у боротьбі з кіберзагрозами є проактивність. Інтелектуальні методи дають нам інструменти для прогнозування і запобігання атакам, а не лише реагування на них після факту. Це дозволяє нам перейти від пасивного захисту до активної оборони, що значно підвищує безпеку цифрового світу.

Перелік посилань

1. Сем Фокс. Шість викликів та перспективи сфери безпеки - як впоратися з ними. Mediacom. 28.02.2024. URL: https://mediacom.com.ua/shi-u-sferi-bezpeki-vikliki-ta-perspektivi/ (дата звернення: 23.05.2024).

2. Застосування ШІ у кібербезпеці: роль, застосування та переваги. Блог компанії Wezom. URL: https://wezom.com.ua/ua/blog/zastosuvannya-shi-u-kiberbezpetsi-rol-ta-perevagi (дата звернення: 23.05.2024).

1. Москаленко В.В. Основи штучного інтелекту та кібербезпека. Силабус освітнього компонента. Національний технічний університет "Харківський політехнічний інститут". URL: https://web.kpi.kharkov.ua/pm/wp-content/uploads/sites/120/2024/04/DZUK_Osnovy-shtuchnogo-intelektu-dlya-kiberbezpeky.pdf (дата звернення: 23.05.2024).

МОДЕЛЮВАННЯ НАСЛІДКІВ ПІДРИВУ СЕРЕДНЬОДНІПРОВСЬКОЇ ГЕС З ВИКОРИСТАННЯМ ГЕОІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Красовська І.Г., Руденко Н.Ю.

Національний аерокосмічний університет
ім. М. Є. Жуковського
«Харківський авіаційний інститут», Харків, Україна
ines75ma@ukr.net, n.y.rudenko@student.khai.edu

Оцінка ступені потенційного затоплення території внаслідок гіпотетичного підриву Середньодніпровської ГЕС. Створення 3D-моделі зони можливого затоплення та візуалізація зон ризику на карті з використанням геоінформаційних технологій.
Ключові слова: Середньодніпровська ГЕС, обробка зображень, 3D-модель, ArcMap, ArcGIS, ArcScene, супутниковий знімок, SRTM.

Вступ

Трагедія підриву Каховської ГЕС, що сталася 6 червня 2023 року, призвела до масштабної катастрофи. Ця подія спричинила підтоплення міст, екологічну катастрофу і евакуацію тисяч людей. Для запобігання подібних ситуацій і їх наслідків, необхідно чітко та точно знати, що і як може трапитись. Один із найефективніших підходів – використання геоінформаційних технологій. Як приклад розглянемо Середньодніпровську ГЕС, що може виявитися корисним для підвищення безпеки на подібних об’єктах.

Загальні відомості середньодніпровської гес

Середньодніпровська ГЕС – п’ята за розміром в країні. Її потужність становить 352 МВт, в той час як Каховська ГЕС шоста за розміром і потужність її являє собою 351 МВт [1].

Місто Кам’янське розташоване на берегах Кам’янського водосховища, нижче греблі Середньодніпровської ГЕС за 35 км на захід від міста Дніпро. Протяжність із сходу на захід – 22 км, з півночі на південь – 18 км. Площа території міста – 13799 га. Місцевість являє собою рівнину, розділену річкою Дніпро і Кам’янським водоймищем на дві частини: правобережну і лівобережну. Поверхня правобережної частини рівнини горбиста, лівобережна – полого-хвиляста, на окремих ділянках майже плоска [2].

Отримання знімків

Для виконання даної роботи було завантажено два види знімків: SRTM та космічний знімок – Sentinel-2 за 24.08.2022 (Рис. 1).

а. б.

Рисунок 1 – Завантажені знімки:
(а) – SRTM, (б) – Sentinel-2

Методика створення картографічної моделі можливої зони затоплення

Для побудови 3D моделі рельєфу використано програмне забезпечення QGIS. Дані SRTM обраної місцевості було перетворено в ізолінії за допомогою інструменту «Ізолінії». Наступним кроком було створення TIN моделі в ArcMap. Завершальним етапом було побудовано 3D модель рельєфу та накладено супутниковий знімок. Для аналізу зони можливого затоплення було

створено полігональний шейп-файл річок, який також накладено на 3D модель (Рис. 2).

Рисунок 2 – 3D модель рельєфу

Вивчивши карту затоплення від Каховської ГЕС, було встановлено, що найбільший радіус затоплення становив близько 9 км. Для дослідження взято саме це значення, оскільки Каховське та Кам'янське водосховища мають майже однаковий об'єм води. Результатом є побудова карти зони можливого затоплення та 3D модель. Для наглядного аналізу без урахування рельєфу та з урахуванням рельєфу (TIN - моделі) (рис. 3).

Отже, дослідивши буферну зону затоплення враховуючи рельєф місцевості, можна прослідкувати, що, подібно до ситуації з підривом Каховської ГЕС, у разі подібної аварії на Середньодніпровській ГЕС, більше постраждає правий берег річки Дніпро.

а. б.

Рисунок 3 – 3D модель зон можливого підтоплення

(а) – без урахування рельєфу; (б) – з урахування рельєфу

Висновки

У результаті дослідження було проведено детальний аналіз та моделювання можливого затоплення території внаслідок гіпотетичного підриву Середньодніпровської ГЕС. Застосування геоінформаційних технологій дозволило побудувати 3D модель рельєфу та створити зону можливого затоплення для подальшого аналізу. Результати показали серйозні наслідки для правого берега річки Дніпро, подібно до підриву Каховської ГЕС. Це свідчить про важливість використання геоінформаційних технологій для передбачення та запобігання негативним наслідкам техногенних катастроф.

Перелік посилань

1. Шість найпотужніших гідроелектростанцій України [Електронний ресурс]. – Режим доступу: https://shotam.info/shist-naypotuzhnishykh-hidroelektrostantsiy-ukrainy/ – 18.04.2024.

2. Аналітична інформація про екологічний стан міста Кам'янського та стан виконання природоохоронних заходів Екологічної програми міста Кам'янського на 2016–2020 роки [Текст] / Додаток 1 до рішення міської ради. С. 143. – Режим доступу: https://so.kam.gov.ua/ua/osxfile/pg/280519707068349_d5_1o/

ВІДКРИТІ ДИСТАНЦІЙНІ ДАНІ ЯК ОСНОВА ДОВГОТРИВАЛИХ ЕКОЛОГІЧНИХ СПОСТЕРЕЖЕНЬ

П. О. Лаптій

Національний аерокосмічний університет ім.
М. Є. Жуковського «Харківський авіаційний інститут»,
Харків, Україна, p.o.laptii@khai.edu

У роботі розглянуто метод вимірювання екологічної якості шляхом застосування індексу RSEI, що базується на аналізі відкритих даних дистанційного зондування Землі (ДЗЗ). Обгрунтовано використання основних складових індексу і наведено формули для його розрахунку. Показано, як застосування відомих найпоширеніших індексів аналізу даних ДЗЗ та їх модифікація дає змогу оцінити екологічну якість. Конкретизовано необхідні вхідні дані і обрано оптимальних шлях отримання даних ДЗЗ.
Ключові слова: екологічне середовище, відкриті джерела інформації, екологічний індекс, дистанційне зондування.

Вступ

З впровадженням стратегії сталого розвитку необхідність створення екологічного середовища постійно підвищується, набуваючи статусу найважливішої задачі розвитку країни. І хоча концепцію створення екологічного середовища ще остаточно не сформовано, її роль полягає в такому: зі швидким розвитком суспільства та економіки, створення екологічного середовища є важливим напрямком у боротьбі з деградацією навколишнього середовища.

У масштабах країни створення екологічного середовища зосереджене на створенні системи екологічного захисту та відновленні порушених екосистем. Це поєднує оцінку та збереження лісового господарства, рослинного покрову, водних ресурсів, боротьбу з ерозією ґрунтів, покращення стану пасовищ тощо.

Створення екологічного середовища передбачає реалізацію таких етапів:

1. Етап захисту: Заборона на вирубку лісів, використання біологічних методів захисту…
2. Етап відновлення: Використання штучних методів, таких як посадка дерев.
3. Етап управління: Застосування заходів для запобігання деградації, таких як збереження ґрунтів та боротьба з опустелюванням.

Основні вхідні дані

Вихідними даними для оцінювання екологічного середовища місцевості є: географічні координати, площа поверхні, що аналізують, чисельність населення та кількість населення пунктів, доступність водних ресурсів, рельєф, середнє річна температура, індекси вологості, кількість опадів тощо.

Джерела дистанційних даних

Landsat має найдовший безперервний архів мультиспектральних зображень, який добре підходить для довготривалих екологічних спостережень. Для цього дослідження використовувались знімки Landsat 5, Landsat 7 та Landsat 8 Surface Reflectance Tier 1 з 1991 по 2021 рік, надані Центром геологічної служби США на платформі GEE. У цьому дослідженні були використані видимий, ближній інфрачервоний, середньоінфрачервоний та тепловий інфрачервоні діапазони з Landsat 5, Landsat 7 та Landsat 8 (канали 1–7 для Landsat 5, Landsat 7 та смуги 2–7, 10 для Landsat 8).

Екологічний індекс місцевості на основі даних дистанційного зондування Землі

Для оцінювання екологічного стану місцевості скористаємося індексом RSEI – індексом, що дає змогу оцінити екологічну якість (EQ), базуючись лише на даних ДЗЗ [1, 2]. Аналогічний індекс, наприклад, використано в роботі [2] для оцінки стану екологічного середовища.

Як приклад сформуємо індекс RSEI для оцінювання екологічної якості Харківської області.

RSEI будується на чотирьох показниках, що включають зеленість, вологість, тепло та сухість:

$$RSEI = f(\text{Рослинність, Вологість, Тепло, Сухість}), \quad (1)$$

Показник рослинності характеризує рослинність, яку можна оцінити з використанням нормалізованого диференційованого вегетаційного індексу (NDVI). Показник вологості відбиває вологість ґрунту, яку розраховують за вологим компонентом за допомогою Tasseled Cap Transformation. Тепловий індекс відображає температуру, яку оцінюють за температурним індексом поверхні землі (LST). Показник сухості в основному застосовують до відкритого ґрунту та незабудованої поверхні. Його можна оцінити з використанням індексу нормалізованої різниці непроникної поверхні. При цьому на відміну від роботи [2] для Харківської області під час розрахунку RSEI показник рослинності слід модифікувати [3] для того, щоб не спотворити його значення близькими по спектру даними водних мас.

$$MNDWI = (\text{зелений} - SWIR1)/(\text{зелений} + SWIR1), \quad (2)$$

де Green та SWIR1 – значення зеленого та короткохвильового інфрачервоного діапазону 1 на теоретичному знімку Landsat. Для розрахунку RSEI застосовано метод основних компонент (PCA), запропонований у роботі [2] із використанням чотирьох показників.

Перша складова PCA – PC1 найбільш повно відбиває RSEI, оскільки через неї можна пояснити максимальну загальну варіацію сформованого набору даних:

$$RSEI_0 = PC1|\ f\ (Wet, VI, LST, NDSI)| \quad (3),$$

$RSEI_0$ представляє початкове значення індексу RSEI. Вага кожного наступного показника зважується при його порівнянні з PC1.

Вищі значення $RSEI_0$ означають кращу EQ, а нижчі значення $RSEI_0$ означають гіршу EQ. Якщо вищі значення не відображають кращого EQ слід відняти $RSEI_0$ від

одиниці:

$$RSEI = 1 - RSEI_0 = 1 - \{PC1|f(Wet, NDVI, LST, NDISI)|\} \quad (4)$$

Крім того, кожен показник слід нормалізувати в діапазоні [0, 1] перед обчисленням PCA внаслідок різних одиниць вимірювання та діапазонів даних. В цьому випадку використаємо формулу:

$$N I = (I - I)/(I_{max} - I_{min}). \quad (5)$$

Також для порівняння додатково нормалізуємо RSEI в межах [0, 1], тобто

$$RSEI = (RSEI_0 - RSEI_{0\_min})/(RSEI_{0\_max} - RSEI_{0\_min}). \quad (6)$$

Далі, отримане значення RSEI розділено на п'ять рівнів: рівень 1 значення індексу RSEI у діапазоні від 0 до 0,2; рівень 2 – у діапазоні від 0,2 до 0,4, рівень 3 – від 0,4 до 0,6; рівень 4 – від 0,6 до 0,8; рівень 5 – від 0,8 до 1. Ці рівні відповідають відповідно поганому, неповноцінному, середньому, доброму і відмінному рівню EQ.

Висновок

Використання RSEI є ефективним і зручним методом для аналізу EQ на основі відкритих дистанційних даних, оскільки є можливість безконтактного оцінювання якості екологічного середовища, що особливо важливо в умовах обмеженої доступності місць аналізу. Також доступність та різноманітність даних ДЗЗ дає змогу отримати необхідні результати у мінімальні строки.

Перелік використаних джерел

1. Xu, H. A remote sensing index for assessment of regional ecological changes. China Environ. Sci. 2013, 33, 889–897.

2. Hanqiu Xu. remote sensing Detecting Ecological Changes with a Remote Sensing Based Ecological Index (RSEI) Produced Time Series and Change Vector Analysis

3. Xu, H. A study on information extraction of water body with the modified normalized difference water index (MNDWI). J. Remote Sens. 2005, 9, 589–595.

АТАКИ СТОРОННІМИ КАНАЛАМИ НА КРИПТОГРАФІЧНІ АЛГОРИТМИ: МЕТОДИ ВИЯВЛЕННЯ ТА ЗАХИСТУ

Світличний В.А., Гупалюк Г.Я.

Харківський національний університет внутрішніх справ

vit.svet@ukr.net

В тезах доповіді розглянуто деякі особливості атак сторонніми каналами (Side-Channel Attacks). Показані основні загрози для криптографічних систем. Розглянуто основні види атак сторонніми каналами, методи їх виявлення та засоби захисту.

Ключові слова.
криптографія, захист даних, інформація, загрози, надійність та безпека криптографічних систем.

Вступ

Криптографія є ключовим елементом сучасної інформаційної безпеки, забезпечуючи захист даних під час їх передачі та зберігання. Проте, незважаючи на те, що криптографічні алгоритми здатні надійно захищати інформацію, існує загроза у вигляді атак сторонніми каналами (Side-Channel Attacks). Ці атаки спрямовані на витік інформації через непрямі канали, такі як час виконання алгоритму, споживання енергії, електромагнітні випромінювання та інші фізичні прояви роботи обчислювальних пристроїв.

Виклад основного матеріалу

Розглянемо основні види атак, методи їх виявлення та відповідного захисту.

Атаки на основі часу (Timing Attacks). Атаки цього типу базуються на аналізі часу, необхідного для виконання криптографічних операцій. Наприклад, різниця в часі виконання може надати інформацію про довжину ключа або конкретні бітові значення. Зловмисник використовує

цю інформацію для виведення секретів, використовуваних у криптографічного системі, таких як ключі або паролі. Цей тип атаки може бути використаний для злому різних механізмів безпеки, таких як протоколи аутентифікації, перевірка пароля і шифрування [1].

Атаки на основі споживання енергії (Power Analysis Attacks). Вони включають простий аналіз енергоспоживання (Simple Power Analysis, SPA) та диференційний аналіз енергоспоживання (Differential Power Analysis, DPA). SPA використовує очевидні коливання в споживанні енергії, тоді як DPA аналізує статистичні зміни в споживанні енергії для розкриття ключової інформації.

*Атаки на основі електромагнітних випромінювань (Electromagnetic Attacks).*Ці атаки базуються на аналізі електромагнітних полів, що випромінюються пристроєм під час виконання криптографічних операцій. EMB — це форма енергії, яка поширюється у просторі у вигляді хвиль або частинок. EMB має різну довжину хвилі, частоту та потужність, що визначає її спектр та ефекти. EMB може бути видимим (світло) або невидимим (радіохвилі, мікрохвилі, інфрачервоне випромінювання тощо) [2].

Атаки на основі акустичних сигналів (Acoustic Cryptanalysis). Даний тип атак використовує звукові сигнали, які видає пристрій під час роботи. Наприклад, звуки, що виникають в результаті роботи процесора або інших компонентів, можуть містити інформацію про виконувані операції.

Кратко розглянувши основні види атак, перейдемо до методів їх виявлення атак сторонніми каналами:

1. *Моніторинг часу виконання:* Постійний моніторинг часу виконання критичних операцій може допомогти виявити підозрілі аномалії, що свідчать про можливі атаки.

2. *Аналіз енергоспоживання:* Використання високоточних вимірювачів енергоспоживання для виявлення нетипових патернів, що можуть свідчити про атаки.

3. *Електромагнітний аналіз:* Використання спеціалізованого обладнання для моніторингу електромагнітного випромінювання і аналізу на предмет підозрілих змін.

Щодо захисту від атак сторонніми каналами, на нашу думку, необхідно зупинитися на наступних методах.

1. *Введення випадкових затримок (Random Delays):* Введення випадкових затримок в процес виконання криптографічних алгоритмів допомагає приховати часові характеристики, що можуть використовуватись для атак.

2. *Маскування (Masking):* Маскування полягає у додаванні додаткових випадкових даних до ключової інформації, що ускладнює аналіз споживання енергії та інші атаки.

3. *Фізичні засоби захисту:* Використання захисних екранів для зниження електромагнітних випромінювань або акустичних ізоляторів для зменшення звукових витоків. Найпростіший і надійний спосіб захисту інформації від загроз несанкціонованого доступу (НСД) - режим автономного використання ПК одним користувачем у спеціально виділеному приміщенні при відсутності сторонніх осіб. У цьому випадку роль замкненого контуру захисту виконує виділене приміщення, а фізичний захист-вікна, стіни, підлога, стеля, двері. Якщо стіни, стеля, підлога і двері міцні, підлога не має люків, які з'єднуються з іншими приміщеннями, вікна і двері обладнані охоронною сигналізацією, то стійкість захисту буде визна-чатись технічними характеристиками охоронної сигналізації при відсутності користувача в неробочий час [3].

4. *Диференційний електромагнітний емісійний криптоаналіз (DEMA):* Даний метод захисту передбачає застосування технік для заплутування електромагнітних емісій таким чином, щоб вони не несли корисної інформації для зловмисника.

5. *Динамічне переміщення даних:* Регулярне переміщення даних в пам’яті або використання динамічного переміщення обчислень може знизити

ефективність атак, що базуються на аналізі певних патернів.

Висновки

Атаки сторонніми каналами представляють серйозну загрозу для криптографічних систем, оскільки вони використовують фізичні прояви роботи пристроїв, а не вразливості самих алгоритмів. Ефективне виявлення та захист від таких атак вимагає комплексного підходу, що включає як технічні засоби моніторингу і аналізу, так і впровадження захисних заходів на апаратному і програмному рівнях. Розробка і впровадження методів захисту від атак сторонніми каналами є критично важливим напрямком для забезпечення надійності та безпеки сучасних криптографічних систем.

Перелік посилань

1. Тимчасові атаки. Компанія CQR. URL: https://cqr.company/ua/web-vulnerabilities/timing-attacks/ (дата звернення: 21.05.2024)
2. Буряк Г.В., Нікулін О.В., Йовдій Г.Г. Електромагнітна зброя: Від потенціалу до реалізації – ключ до підвищення обороноздатності України – СОЮЗ Золотий вік України. URL: https://zovu.org/elektromagnitnoye-oruzhiye-ot-potentsial/ (дата звернення: 21.05.2024).
3. Олійник А.В., Шацька В.М. Інформаційні системи і технології у фінансових установах - Навчальний посібник - Львів: "Новий Світ-2000", 2006 - 436 с.

ON THE IMPLEMENTATION OF THE PROTOCOL BASED MULTIVARIATE DIGITAL SIGNATURE SCHEMES OVER THE ARITHMETIC RING Z_{2^s}

Vasyl Ustimenko[1] and Tymoteusz Chojecki[2]

[1] University of London (Royal Holloway), UK; University of Maria Curie-Sklodowska, Poland; Institute of Telecommunications and Global Information Space, Kyiv, Ukraine.
Vasyl.Ustymenko@rhul.ac.uk, vasylustimenko@yahoo.pl,
[2] Institute of Mathematics, University of Maria Curie-Sklodowska, Poland.
tymoteusz.chojecki@umcs.pl

This research is partially supported by British Academy Fellowship for Researchers under Risk 2022. and UMCS Mini Grants

Keywords: Digital signatures, Protocol based cryptosystems, Non- commutative Cryptography, Eulerian transformations.

Introduction

One of the popular idea to make a "short" digitat signature is to use a quadratic multivariate public keys defined over the finite commutative ring K. Such a cryptosystem can be treated as a pair of kind (F, T), where F is a quadratic endomorphism of $K[x_1, x_2, \ldots, x_n]$ acting naturally on the affine space Kn and T is a trapdoor accelerator i.e. a piece of information which allows to solve the equation F (x) = b where b, x $\in K^n$ in time $O(n^2)$ and allows the computation of $F(v)$, $v \in K^n$ in time $O(n^2)$. In the case of a public key the computation of the reimage of F without of the knowledge of T has to be NP-hard problem, i.e. reimage is not computable in polynomial time. We refer to this condition as NP-hardness requirement. The most popular finite commutative ring K is a finite field F_q of characteristic two. The properties of such F_q were used in thedefinition of Imai-Matsumoto digital signatures scheme which was one of the

first historical candidates to be a secure multivariate public keys. Well-known "Unbalanced Rainbow like Oil and Vinegar Cryptosystem" (ROUV) public key from this class were considered as strong candidate for NIST certification. Finally appropriate cryptanalysis for ROUV was found (see [3], [2]) but the search for new secure digital schemes is continue (see [4] and further references).

General scheme of asymmetric cryptosystem

We will use pairs (F, T), $deg(F) = 2$ or $deg(F) = 3$ without the consideration of NP-hardness requirement for F in the case of $K = Z_2s$, $s > 1$ for the construction of efficient digital signature schemes. Security of the asymmetric algorithms rests on the selected semigroup based algorithms of Noncommutative Cryptography (see [1]).

In fact we use the composition FG of the quadratic or cubic bujective map F with Eulerian endomorphism G sending each variable xi to a monomial term of kind $a(x_1)^{a(1)}(x_2)^{a(2)} \ldots (x_n)^{a(n)}$, $a \in K^*$, $a(i) \in Z_2s - 1$. We select F and G preserving the subvariety $W_n = (K^*)^n$ of K^n and acting bijectively on this subvariety. Assume that G^{-1} stands for an Eulerian endomorphism H such that restrictions of GH and HG on W_n are identity transformations. Noteworthy that FG has nonpolynomial density but the density of $G^{-1}F^{-1}$ of linear degree is $O(n^3)$ or $O(n^4)$ for $deg(F) = 2$ and $deg(F) = 3$ respectively. Alice constructs multivariate map F with the trapdoor accelerator T. The piece of information T is subdivided into ${}^1T$ and ${}^2T$. We assume that ${}^1T$ is known publicly but ${}^2T$ is transfered from Alice to Bob in a secure way with use of the Protocol of Noncommutative Cryptography. So Bob poses (F, T). He is able to compute reimages of F. Additionally she generates Eulerian transformation G with Eulerian trapdoor accelerator ${}^3T$, its knowledge allows to compute reimages of G acting on the variety W_n in time $O(n^2)$. The general description of the cryptosystem is the following scheme. Alice and Bob use the semigroup ${}^nES(K)$

of all Eulerian endomorphisms in the case of $K = Z_2s$ for the safe delivery of G from Alice to Bob.

Alice and Bob share element $g \in {}^{n} S(Z_2s)$ and pair of invertible elements h, h^{-1} from this semigroup. Alice takes positive integers $k(A)$ and $r(A)$ and forms $h^{-r(A)}g^{k(A)}h^{r(A)} = g_A$. Bob takes $k(B)$ and $r(B)$ and forms $h^{-r(B)}g^{k(B)}h^{r(B)} = g_B$. They exchange g_A and g_B and compute collision element X as ${}^{A}g = h^{-r(A)}g_B{}^{k(A)}h^{r(A)}$ (Alice) and ${}^{B}g = h^{-r(B)}g_A{}^{k}(B)h^{r(B)}$ (Bob) respectively.

The security of the scheme rest on the Conjugation Power Problem, adver- sary has to solve the problem $h^{-x}g^{y}h^{x} = b$ where b coincides with g_B or g_A. The problem is NP -hard in the case of our highly noncommutative platform ${}^{n}ES(Z_2s)$. The computational complexity of the protocol is $O(n^3)$.

Assume that the collision element is witten in its standard form as

$$x_1 \longrightarrow q_1 a(x_1)^{a(1,1)}(x_2)^{a}(1, 2)\ldots(x_n)^{a(1,n)} = {}^{1}t,.$$

$$x_2 \longrightarrow q_2 a(x_1)^{a(2,1)}(x_2)^{a}(2, 2)\ldots(x_n)^{a(2,n)} = {}^{2}t,$$

$$\ldots.$$

$$x_n \longrightarrow q_n a(x_1)^{a(n,1)}(x_2)^{a}(n, 2)\ldots(x_n)^{a(n,n)} = {}^{n}t,$$

$$q_i \in Z_{*2}s\,,\ a(i,j) \in Z_2s - 1 = t_1.$$

Alice generates elements h and h^{-1} as a products of several Jordan-Gauss transformations of W_n (see [6]), for which the computation of their inverses is feasible. The definition of these transformations are given below.

Let π and σ be two permutations on the set {1, 2, ..., n}. Let K be a finite commutative ring with unity which has nontrivial multiplicative group K^* of order $d = |K^*| > 1$ and $n \geq 1$. We define transformation ${}^{A}JG(\pi, \sigma)$ of the variety $(K^*)^n$, where A is triangular matrix with positive integer entries $0 \leq a(i,j) \leq d$, $i \geq j$ defined by the following closed formula.

$$y_{\pi(1)} = \mu_1 x_{\sigma(1)}{}^{a(1,1)}$$

$$y_{\pi(2)} = \mu_2 x_{\sigma(1)}{}^{a(2,1)} x_{\sigma(2)}{}^{a(2,2)}$$

...

$$y_{\pi(n)} = \mu_n x\, x_{\sigma(1)}{}^{a(n,1)} x_{\sigma(2)}{}^{a(n,2)} \ldots x_{\sigma(n)}{}^{a(n,n)}$$

where $(a(1,1), d) = 1$, $(a(2,2), d) = 1$, ..., $(a(n,n), d) = 1$.

We refer to ${}^{A}JG(\pi, \sigma)$ as Jordan –Gauss multiplicative transformation or simply JG element. It is an invertible element of ${}^{n}ES(K)$ actingd on W_n with the Jordan - Gauss inverse. Notice that in the case $K = Z_m$ straightforward process of computation the inverse of JG element is connected with the factorization problem of integer m. If $n = 1$ and m is a product of two large primes p and q the complexity of the problem is used in RSA public key algorithm.

Additionally Alice selects Jordan-Gauss elements $J_1, J_2, \ldots, J_k$, $k > 1$, $k = O(1)$ and compute element $G = (J_1 J_2 \ldots J_k)$. She takes the standard form of G of kind

$$x_1 \to q_1' a(x_1)^{b(1,1)} (x_2)^{b(1,2)} \ldots (x_n)^{b(1,n)} = {}^{1}g,.$$

$$x_2 \to q_2' b(x_1)^{b(2,1)} (x_2)^{b(2,2)} \ldots (x_n)^{b(2,n)} = {}^{2}g,$$

....

$$x_n \to q_n' a(x_1)^{b(n,1)} (x_2)^{b(n,2)} \ldots (x_n)^{b(n,n)} = {}^{n}b,$$

Alice sends the tuple of monomial terms $({}^{1}t^{1}g, {}^{2}t^{2}g, \ldots, {}^{n}t^{n}g)$ to Bob. Herestores the Eulerian transformation G.

We assume that ${}^{2}T$ has a form of the "password" $(q_1, q_2, \ldots, q_n)$. So Alice and Bob can use the map F and compute its reimages.

After the completion of the protocol correspondents can use asymmetric cryptosystem with the plaintexts from $W_n = Z^*{}_2 s$. Bob creates his plaintext $p = (p_1, p_2, \ldots, p_n)$. He computes $F(p) = {}^{1}p$ in time $O(n^2)$ because his knowledge of T, and forms the ciphertext $E(p)$ as $G({}^{1}p) = c$ in time $O(n^2)$ because of his knowledge of the standard form of G.

Alice uses her knowledge on the trapdoor accelerator ${}^{3}T$ and solves $G({}^{1}p) = c$ for p^1 in time $O(n^2)$. Secondly she solves $F(p) = {}^{1}p$ for p in time $O(n^2)$ because of her

knowledge on T . Note that the complexity of the is $O(n^3)$. So the complexity of general scheme is $O(n^3)$ as well. The pair of protocols has to be conducted ones.

So the complexity of the processing of $O(n^t)$, $t > 1$ plaintexts is in fact $O(n^{t+2})$. If $t \leq 1$ then the complexity is $O(n^3)$.

The encryption function $E = G(F(x))$ mapping $(Z_2s)^n$ into itself has a mul-tivariate nature. Note that $F(x_i) = f_i(x_1, x_2, \ldots, x_n)$ where f_i are cubical or quadratic polynomials from $(Z_2s)[x_1, x_2, \ldots, x_n)$ and $G(x_i) = q_i(x_1)^a(i, 1)(x_2)^a(i, 2), \ldots, (x_n)^a(i, n)$, where $q_i \in Z^*_2s$ and $a(i, js-1) \in Z_2s-1$. Recall that a density $d(H)$ of the multivariate map H of K^n is a total number of monomial terms in all $H(x_i)$, $i = 1, 2, ..., n$, So cubical F has $d(F) = O(n^4)$, degree of G is a linear expression $l(n)$ of size $O(n)$. It means that nonbijective map E has linear degree and non-polynomial density. Thus adversary is unable to restore E via the interception of pairs of kind a plaintext p and corresponding ciphertext $E(p)$. So security of the algorithm rests on the security of the used protocol of Noncommutative Cryptography with the platform ${}^nES(Z_2s)$. Alice and Bob can use protocols which rest on the complexity of Conjugacy Problem or more general problem of the decomposition of semigroup element into the word in given generators (see [6]). Both problems are NP-hard.

It can be used for the digital signature in the following way. Assume that correspondents use a stream ciphers with the plaintexts from K^m where K, $m > n$ is one of the commutative ring F_2s-1, Z_2s-1 and B_{s-1} (Boolean ring of order 2^{s-1}). Let π be an effectively computable bijection between Z^{*s} and K some examples can be found in [5]. Alice and Bob create the hash tuple $(t_1, t_2, \ldots, t_n)$ from K^n from the ciphertext and compute $d = (\pi(t_1), \pi(t_2), \ldots, \pi(t_n))$. The knowledge of T allows her to compute the signature $E^{-1}(d) = r$. Bob checks that $E(r) = d$. Thus he is sure that the ciphertext was sent by Alice.

Description of graph based trapdoor accelerator

We implement described above digital scheme with the following pair (F, T). Let K be a commutative ring with the unity. We consider the following incidence structure $A(n, K)$ with the points (p), $p \in K^n$ and lines $[l]$, $l \in K^n$ and incidence relation I given by the condition below. Point $(p) = (p_1, p_2, \ldots, p_n)$ is incident to line $[l] = [l_1, l_2, \ldots, l_n]$ if and only if the following condition I holds $l_2 - p_2 = l_1 p_1$, $l_3 - p_3 = p_1 l_2$, $l_4 - p_4 = l_1 p_3$, $l_5 - p_5 = p_1 l_4, \ldots, l_n - p_n$ is $l_1 p_{n-1}$ if n is even and $l_n \quad p_n = p_1 l_{n-1}$ if n is odd. We refer to the first coordinate $\rho(v)$ of the vertex v (point or line) as the colour $\rho(v)$ of v. For each vertex there is a unique neighbour of the selected colour. So the path of length t in the bipartite graph $\boldsymbol{I}$ is defined by the initial vertex v and the sequence of colours $a_1, a_2, \ldots, a_t$. We assume that $a_i \neq a_{i+2}$ for $i = 1, 2, \ldots, t-2$. We take $K = Z_2 s\,[x_1, x_2, \ldots, x_n]$ and consider the path $W = W(a_1, a_2, \ldots, a_n)$, $a_i \in Z^{*s}$ with starting line $[x_1, x_2, \ldots, x_n]$ and colours of consecutive points $x_1 + a_1$, $x_1 + a_1 + a_3$, $x_1 + a_1 + a_3 + a_5$, ... and colours of consecutive lines x_1, $x_1 + a_2$, $x_1 + a_2 + a_4$, ... The destination vertex of this path will be the vertex v with coordinates $f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, x_2, \quad, x_n)$ where $f_1(x_1) = x_1 + a$ for $a \in K$. We consider a polynomial map $Q = Q(a_1, a_2, \ldots, a_n)$ of kind $x_1 \to f_1(x_1)$, $x_2 \to f_2(x_2). \ldots, x_n \to f_n(x_1, x_2, \ldots, x_n)$. It is clear that the reverse path defines inverse map $F^{-1}(a_1, a_2, \ldots, a_n)$. The transformation of kind $Q(a_1, a_2, \quad, a_n)$ are well investigated (see [7] and further references). They are cubical maps of $(Z_2 s)^n$.

We can prove that distinct tuples $(a_1, a_2, \ldots, a_n)$ correspond to different maps.

So Alice and Bob take $Q = Q(q_1, q_2, \ldots, q_n)$ together with the linear transformation $L : x_1 \to q_1 x_1 + q_2 x_2 + + q_n x_n$, $x_i \to x_i$, $i = 2, 3, \ldots, n$.

They form $Y = LQL^{-1}$. Let H be a bijective multivariate transformation of $(Z_{2^s})^n$. We can compute $H(1, 1, \ldots, 1) = (d_1, d_2, \ldots, d_n)$ and modify H as $^*H : x \to \boldsymbol{H}(x) + (b_1, b_2, \ldots, b_n)$ where $b_i = 1$ if d_i is an even

residue and $b_i = 0$ if d_i is odd. The bijective transformation $*H$ preserves the variety $(Z*_{2^s})^n$. Let $b(H)$ stands for the tuple (b_1, b_2, b_n). Alice and Bob will use cubic map F sending x to $Y(x) + b(Y)$. The knowledge of $(q_1, q_2, \ldots, q_n)$ and the decomposition of Y into the triple L, Q, L^{-1} (trapdoor accelerator ${}^2T$) allows them to compute the value of F and its inverse in time $O(n^2)$. Equations of the graph $A(n, K)$ areannounced publicly (part ${}^1T$ of the trapdoor T).

Remark 1 As we already mention that endomorphism FG has nonpolyno- mial density. In fact the density d_n of $G^{-1}F^{-1}$ is a polynomial one. If $K = Z_q, q = 2^{32}$ we have $d_{16} = 8841$, $d_{32} = 39249$, $d_{64} = 339775$ and $d_{128} = 3101445$.

All of these monomial term have a linear degree in variable n.

Remark 2 The following obfuscation of cryptosystem is reasonable. Alice and Bob conduct two protocols with the platform ${}^nES(K)$ and Alice uses these two collision maps for the delivery of two transformation ${}^1Y$ and ${}^2Y$ for which she knows their decompo- sitions into Jordan-Gauss generators. Then Bob encrypts with the composition of ${}^1Y$, F and ${}^2Y$, Alice uses the sequence $({}^2Y)^{-1}$, F^{-1}, $({}^1Y)^{-1}$ for the decryption.

In this case both encryption and decryption maps have nonpolynomial density.

The obfuscation does not affect theoretical complexity of the cryptosystem but it complicates cryptanalytic studies.

Acknowledgements. This research is partially supported by British Academy Fellowship for Researchers under Risk 2022 and partially supported by British Academy award LTRSF\100333 and UMCS Mini-Grant program.

References

1. Alexei G. Myasnikov, Vladimir Shpilrain and Alexander Ushakov (2011), Noncom- mutative Cryptography and Complexity of Group-theoretic Problems, American Mathematical Society.

2. Anne Canteaut, Franois-Xavier Standaert (Eds.),

Eurocrypt 2021, LNCS 12696, 40th Annual International Conference on the Theory and Applications of Crypto- graphic Techniques, Zagreb, Croa-tia, October 17?21, 2021, Proceedings, Part I, Springer, 2021, 839p.

3. Ward Beullens, Improved Cryptanalysis of UOV and Rainbow, In Eurocrypt 2021, Part 1, pp. 348-373.

4. Smith-Tone, D. (2022), 2F - A New Method for Constructing Efficient Multivariate Encryption Schemes, Proceedings of PQCrypto 2022: The Thirteenth International Conference on Post-Quantum Cryptography, virtual, DC, US.

5. V. Ustimenko, On the cryptosystems based on two Eulerian transformations defined over the commutative rings Z2s , s > 1¡ IACR e-print archive 2024/319.

6. V. Ustimenko, On Eulerian semigroups of multivariate transformations and their cryptographic applications. European Journal of Mathematics 9, 93 (2023).

7. V. Ustimenko, T. Chojecki, M. Klisowski, On the implementations of new graph based cubic Multivariate Public Keys, Proceedings of the 18th Conference on Com- puter Science and Intelligence Systems, ACSIS, Vol. 35, pp. 1179-1184.

ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК МЕТОДАМИ ПОШУКУ АНОМАЛІЙ НА ОСНОВІ МАШИННОГО НАВЧАННЯ

М.В. Коломицев, С.О. Носок, О.Е. Подвисоцька
КПІ ім. І. Сікорського, м. Київ, Україна
olhapodvysotska@gmail.com

На поточний момент існує чимало технологій для детектування мережевих атак, як-от системи виявлення та запобігання вторгненням (IDS, IPD), аналізатори поведінки мережі (NBA), системи управління подіями інформаційної безпеки (SIEM) тощо. Можливості таких інструментів покривають значну частину потреб їхніх користувачів. Проте зі зростанням частоти впровадження штучного інтелекту в процеси управління безпекою з'являються нові перспективи для розвитку підходів, пов'язаних з методами машинного навчання.

Ключові слова: машинне навчання (ML), навчання без учителя, навчання з учителем, кластеризація, класифікація, мережевий трафік, виявлення аномалій, аномалії мережевого трафіку.

Вступ

Однією з можливостей застосування машинного навчання є виявлення аномалій трафіку з метою детектування мережевих атак. Серед наявних підходів виділяють навчання з учителем і без учителя. Цим способам аналізу властиві розмежування, зумовлені здебільшого наявністю чи відсутністю попередньо розміченої вибірки даних. Проте обидва підходи мають свої переваги, які є має сенс об'єднати, створивши певний комбінований метод виявлення аномалій. Метою цієї роботи є вдосконалення існуючих способів виявлення мережевих атак методом пошуку аномалій на основі машинного навчання.

Використання класифікації та кластеризації для аналізу мережевого трафіку

Моделі, що базуються на навчанні з учителем, можуть розпізнавати знайомі патерни атак на основі попередніх інцидентів. Широко застосовуваними алгоритмами є Random Forest, Naïve Bayes, K-Nearest Neighbors (KNN), Support Vector Machine (SVM).

Дослідження вказують на високу точність виявлення відомих атак. Однак очевидним недоліком цих методів є необхідність у наявності попередньо розмічених навчальних наборах. І хоча такі зразки можна отримати із загальнодоступних ресурсів, коли йдеться про пошук підозрілого трафіку на реальних даних, задача ускладнюється.

Алгоритми ж кластеризації є потужним інструментом для роботи з нерозміченими даними. Серед популярних моделей можна виділити K-Means, Density-Based Spatial Clustering of Applications woth Noise (DBSCAN), Isolation Forest, Gaussian Mixture Model (GMM).

Вони можуть виявляти приховані структури, що дозволяє знаходити аномалії, які не вписуються в ці структури. Однак їх ефективність залежить від правильного підбору параметрів, а ресурси для обчислень можуть суттєво зростати зі збільшенням розмірності даних, що аналізуються.

Комбінований метод виявлення аномалій

З огляду на інформацію, викладену вище, пропонується застосовувати комбінований метод для аналізу даних мережевого трафіку. Ідея полягає в об’єднанні двох типів машинного навчання. Очікується, що такий підхід дасть змогу поєднати переваги обох методів і частково нівелювати їхні недоліки.

Пропонується на першому кроці використовувати кластеризацію для попередньої розмітки невеликої частини набору «сирих» даних про мережевий трафік. Розміри цієї частини можуть залежати від активності в мережі. Далі ці

дані стануть навчальною вибіркою для класифікатора, який буде працювати з іншою частиною датасету, а також на тому трафіку, що отримуватиметься в реальному часі. У результаті буде отримано модель навчання з учителем, де в ролі вчителя виступатиме навчання без учителя.

Розмічення даних необхідно проводити з певною періодичністю, яка визначається активністю в конкретної мережі. Наведена умова є доволі природною, позаяк неможливо один лише раз визначити прийнятний приклад трафіку та орієнтуватися лише на нього — підхід має бути динамічним і пристосовуватися до змін.

Переваги запропонованого способу:

- робота на нерозміченому мережевому трафіку;
- прогнозування міток на основі класифікації;
- зменшення витрат обчислювальних ресурсів внаслідок зниження розмірності кластеризованого набору;
- можливість знаходження прихованих структур і навчання класифікатора на основі них;
- дослідження нових даних відокремлено від попередніх.

Для кластеризації було вибрано метод DBSCAN. Важливим етапом перед його використанням є встановлення гіперпараметрів. Зазвичай їх підбирають, спираючись на особливості конкретного датасету чи шляхом перебору списку значень. Метою комбінованого методу є максимально автономна його робота, що не потребуватиме «ручного» налаштування. Тобто, необхідно задати універсальну формулу розрахування параметрів.

Нехай аргументи обчислюватимуться наступним чином. Позначимо k як $n + 1$, де n — кількість предикторів після застосування методу головних компонент, які пояснюють 95% варіації в даних. Тоді:

- ε буде визначатися як середнє значення відстані до k найближчих сусідів;
- MinPts буде дорівнювати значенню k.

Після цього використовуватиметься наївний баєсів класифікатор. Основна його перевага полягає в простоті та швидкодії. Алгоритм не вимагає великої кількості

обчислювальних ресурсів і даних для навчання та може ефективно працювати на датасетах з високою розмірністю, що містять багато предикторів.

Аналіз результатів тестування

Тестування проводилося на датасеті CSE-CIC-IDS2018. Набір містить дані мережевого трафіку та журнали системних подій для досліджень у галузі виявлення вторгнень та кібербезпеки. Містить близько 16 мільйонів записів, зібраних протягом 10 днів і включає 7 різних сценаріїв атак.

	Dst Port	Protocol	Flow Duration	Tot Fwd Pkts	Tot Bwd Pkts	TotLen Fwd Pkts	TotLen Bwd Pkts	Fwd Pkt Len Max	Fwd Pkt Len Min	Fwd Pkt Len Mean	...	Fwd Seg Size Min	Active Mean	Active Std	Active Max	Active Min
0	0	0	112641158	3	0	0	0	0	0	0.000000	...	0	0.0	0.000000	0	0
1	22	6	37366762	14	12	2168	2993	712	0	154.857143	...	32	1024353.0	649038.754495	1601183	321569
2	47514	6	543	2	0	64	0	64	0	32.000000	...	32	0.0	0.000000	0	0
3	0	0	112640703	3	0	0	0	0	0	0.000000	...	0	0.0	0.000000	0	0
4	0	0	112640874	3	0	0	0	0	0	0.000000	...	0	0.0	0.000000	0	0
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
401754	52065	6	2	3	0	31	0	31	0	10.333333	...	20	0.0	0.000000	0	0
401755	53	17	9132	1	1	29	45	29	29	29.000000	...	8	0.0	0.000000	0	0
401756	53	17	37016	1	1	44	104	44	44	44.000000	...	8	0.0	0.000000	0	0
401757	53	17	451	1	1	30	62	30	30	30.000000	...	8	0.0	0.000000	0	0
401758	80	6	77458	3	4	437	859	437	0	145.666667	...	20	0.0	0.000000	0	0

400000 rows × 79 columns

Рисунок 1 — Частина вмісту CSE-CIC-IDS2018

Після тестування методу на даних з інформацією про різні атаки та різною кількістю аномалій було виявлено пряму залежність між співвідношенням класів трафіку та точністю прогнозування: чим вища частка аномальних подій, тим краще модель передбачає класи цих подій. Неточність зумовлено тим, що за налаштування гіперпараметрів на основі розмірності даних, а не ручного підбору, DBSCAN ідентифікує абсолютну більшість об’єктів як викиди. Це створює обмеження у використанні запропонованого методу та чітко визначає випадки, у яких він може бути корисним.

Результати тестування методу на 5 наборах даних представлено у зведеній таблиці нижче.

Таблиця 1 — Результати застосування методу

Нормальний трафік, %	Аномальний трафік, %	Accuracy	Precision	Recall	F1-Score
86,89	13,11	0,22	0,12	0,8	0,21
64,16	35,84	0,61	0,63	0,93	0,75
28,53	71,47	0,77	0,76	0,98	0,86
9,18	90,82	0,91	0,92	0,99	0,95
4,79	95,21	0,98	0,99	0,99	0,99

Висновки

Впровадження комбінованого методу пошуку аномалій в мережевому трафіку дозволяє значно покращити ефективність виявлення загроз. Об'єднання кластеризації та класифікації забезпечує комбінований підхід, що поєднує переваги обох методів, зменшуючи їх недоліки. Використання кластеризації для попередньої розмітки даних дозволяє працювати з нерозміченими датасетами, знижуючи витрати на ручну розмітку та підготовку даних.

Запропонований метод також забезпечує динамічність і пристосовуваність до змін у мережевій активності. Автоматичний підбір гіперпараметрів для алгоритму DBSCAN і використання наївного баєсівського класифікатора дозволяють знизити обчислювальні витрати та підвищити швидкість обробки даних.

Натомість експерименти показали, що алгоритм кластеризації добре виявляє шкідливий трафік у тих ситуаціях, коли його кількість значно переважає над нормальною мережевою активністю. Якщо ж аномалій у мережі майже не спостерігається, метрики якості спрацювання кластеризації значно знижуються. Так, наприклад, за співвідношення 87:13 нормального до аномального трафіку значення *F*1-міри складає близько 0,21. А за співвідношення 5:95 середнє гармонійне наближається до 0,99. Отже, такий метод має чітко визначені обмеження в його використанні.

Перелік використаних джерел

1. IDS 2018 Intrusion CSVs (CSE-CIC-IDS2018). — URL: https://www.kaggle.com/datasets/solarmainframe/ids-intrusion-csv/data?select=02-16-2018.csv

2. Diederik P Kingma, Max Welling (2013). Auto-Encoding Variational Bayes. ArXiv Preprint: 1312.6114. DOI: 10.48550/arXiv.1312.6114

3. Shivangi Verma, Neetu Gupta. Applications of Artificial Intelligence in Cybersecurity. Innovations in Computer Science and Engineering. March 2020. DOI: 10.1007/978-981-15-2043-3_9.

4. Tommaso Romani. Harnessing the Power of K-Means for Anomaly Detection. Medium. Aug 10, 2023. — URL: https://medium.com/@tommaso.romani2000/harnessing-the-power-of-k-means-for-anomaly-detection-24dc71d260a8

5. Shilpa Mahajan,Mehak Khurana,Vania Vieira Estrela. Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection. Wiley, 2024. ISBN: 978-1394196456

6. Alessandro Parisi. Hands-On Artificial Intelligence for Cybersecurity. Packt Publishing, 2019. ISBN: 978-1789804027.

7. María García Gumbao. Best Clustering Algorithms for Anomaly Detection. Medium. Published in Jun 3, 2019. — URL: https://towardsdatascience.com/best-clustering-algorithms-for-anomaly-detection-d5b7412537c8

ЗМІСТ

Міністерство освіти і науки України

Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Навчально-науковий фізико-технічний інститут

THEORETICAL AND APPLIED CYBERSECURITY

Матеріали другої Всеукраїнської науково-практичної конференції

Випуск 2

Підп. до друку 20.06.2024. Формат 60x84 1/16. Папір офс. Гарнітура Times.

Спосіб друку – ризографія. Ум. друк. арк. 8,1. Обл.-вид. арк. 24,36. Наклад 100 пр. Зам. № 15-200.

ТОВ "Інжиніринг" ISBN 978-966-2344-98-1