КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1201
УДК 004.032.26+004.056.5

Фесьоха Віталій Вікторович
доктор філософії, доцент, докторант
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут, Київ, Україна
ORCID: 0000-0001-6612-1970
vitaliifesokha@gmail.com

Субач Ігор Юрійович
доктор технічних наук, професор, завідувач кафедри
Інститут спеціального зв'язку та захисту інформації
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна
ORCID: 0000-0002-9344-713X
igor_subach@ukr.net

МОДЕЛЬ ПРОГНОЗУВАННЯ СТРУКТУРНИХ ЗМІН У ПРОСТОРІ МОЖЛИВИХ РЕАЛІЗАЦІЙ ТЕХНІК КІБЕРАТАК НА ОСНОВІ ТОПОЛОГІЧНИХ ОБМЕЖЕНЬ ЇХ ЕВОЛЮЦІЇ З ВИКОРИСТАННЯМ ТЕМПОРАЛЬНИХ ГРАФОВИХ НЕЙРОННИХ МЕРЕЖ

Анотація. У контексті проблематики підвищення кіберстійкості інформаційно-комунікаційних систем (ІКС) вирішується наукове завдання прогнозування структурних змін технік кібератак у просторі можливих їх реалізацій на прикладі таксономії MITRE ATT&CK. Актуальність зазначеного обумовлена об'єктивними обмеженнями існуючих підходів до полювання на нові способи реалізації кіберзагроз (попередження кібератак ще до їхньої реалізації), зокрема засобами машинного навчання. Так, існуючі типи штучних нейронних мереж, що використовуються для прогнозування кібератак (технік кібератак), такі як рекурентні, трансформери, згорткові, графові, темпоральні графові та автокодувальники, хоч і враховують різні аспекти структури даних (простір ознак, часові залежності, глобальний контекст, графову структуру, латентні представлення, розподіл даних), апроксимуючи функцію взаємозалежності між даними виявляють лише статистичну структуру, що не дозволяє повною мірою враховувати стійкі структурні еволюційні закономірності. У зв'язку з цим, розроблено модель прогнозування структурних змін технік кібератак у просторі можливих реалізацій на основі топологічних обмежень їх еволюції з використанням темпоральних графових нейронних мереж. Суть запропонованої моделі полягає у коригуванні результатів прогнозування темпоральної графової мережі на основі топологічного аналізу версій технік кібератак шляхом визначення їх структурної сумісності за спільною участю у компонентах зв'язності та циклічних структурах, що відображають стійкі топологічні характеристики їх еволюції. Доцільність даного підходу зумовлена цінністю виявлення потенційних векторів трансформації кібератак у просторі можливих їх реалізацій, що дає змогу підвищувати кіберстійкість ІКС до майбутніх класів кібератак. Оцінка ефективності застосування запропонованої моделі демонструє підвищення точності прогнозування на 15%, F1-міри на 8% при збереженні рівня повноти 70%, що свідчить про значне зменшення кількості хибнопозитивних спрацьовувань.

Ключові слова: кіберстійкість; інформаційно-комунікаційні системи, прогнозування; техніки кібератак; нейронні мережі; темпоральні графові нейронні мережі; топологічний аналіз даних; закономірності.

ВСТУП

Відповідно до положень Стратегії кібербезпеки України [1] необхідним є своєчасне й ефективне реагування на кібератаки, забезпечення режиму постійної готовності до реальних та потенційних кіберзагроз, виявлення та усунення передумов до їх виникнення, забезпечивши тим самим кіберстійкість, передусім об'єктів критичної інформаційної інфраструктури. Відтак, досягнення зазначених цілей в умовах постійного удосконалення способів реалізації кібератак потребує неперервного розвитку підходів до своєчасного їх передбачення та попередження.

Постановка проблеми. Одним з найефективніших підходів до виявлення нових способів реалізації кіберзагроз (попередження кібератак ще до їхньої реалізації) є проактивний кіберзахист, серед напрямків якого особливе місце посідає прогнозування, оскільки на відміну від моделювання кібератак, виявлення аномалій чи тестування кібербезпеки ІКС, спрямоване на визначення потенційно можливих майбутніх їх модифікацій.

Однак, ефективність прогнозування значною мірою ускладнюється характером еволюції сучасних кібератак (технік кібератак). Так, особливістю нових кібератак є те, що переважна їх більшість є модифікаціями попередніх, раніше відомих зразків певного класу або реалізованих шляхом використання відомих підтехнік із застосуванням, наприклад, раніше невідомих вразливостей [2-3]. Дійсно, з точки зору сторони здійснення деструктивного впливу значно простіше змінити окремі параметри або етапи реалізації існуючої кібератаки з метою уникнення виявлення системами кіберзахисту ніж розробляти принципово нову. До того ж, необмежений доступ зловмисників до сучасних технологій штучного інтелекту, хоч і надає можливості щодо швидкої генерації нових способів реалізації кібератак та обробки великих обсягів даних (накопиченого досвіду) [4], все ж забезпечує отримання рішень, які зазвичай не є принципово іншими та виникають у межах простору можливих реалізацій технік кібератак.

На основі викладеного можна зробити висновок, що їх розвиток має не випадковий, а закономірний характер, що дає змогу розглядати розвиток технік кібератак як процес еволюції в просторі можливих реалізацій.

Зазначене обумовлює доцільність подальших наукових досліджень, спрямованих на використання закономірностей еволюції технік кібератак у задачах їх прогнозування.

Аналіз останніх досліджень і публікацій [5-10] за даною тематикою дає змогу узагальнено виокремити такі напрями прогнозування кібератак:

1. Прогнозування появи або типу кібератаки [5-6]: завдання прогнозування формулюється як визначення ймовірності появи певної кібератаки або її типу на основі попереднього аналізу подій. Для розв'язання таких завдань використовуються різні архітектури штучних нейронних мереж, зокрема рекурентні мережі, згорткові мережі та їх гібридні комбінації, що дає змогу враховувати часові залежності у послідовностях подій та складні нелінійні залежності між ознаками.
2. Прогнозування наступної дії/стадії кібератаки [7-8]: кібератака розглядається як послідовність дій, що відповідають різним технікам або фазам її реалізації. Суть підходу полягає у застосуванні штучних нейронних мереж для визначення найбільш імовірного наступного кроку зловмисника. Для розв'язання даного завдання використовуються рекурентні нейронні мережі, трансформери або їх модифікації, які здатні моделювати залежності між попередніми і майбутніми подіями.

3. Прогнозування сценарію/послідовності розвитку кібератаки [9-10]: кібератака моделюється у вигляді графа взаємозв'язків між подіями, уразливостями або техніками кібератаки, тоді як завдання прогнозування полягає у визначенні можливого подальшого розвитку сценарію кібератаки. Для розв'язання такого роду завдань використовуються графові нейронні мережі, оскільки дозволяють враховувати структурні залежності між елементами кібератаки та прогнозувати можливі шляхи її поширення в ІКС.

Підсумовуючи, доцільно зазначити, що сучасні підходи до прогнозування кібератак та/або технік кібератак, зокрема на основі методів машинного навчання, мають об'єктивні обмеження. Різноманітні типи штучних нейронних мереж, які використовуються для прогнозування кібератак, такі як рекурентні, трансформери, згорткові, графові, темпоральні графові та автокодувальники, хоч і враховують різні аспекти структури даних (простір ознак, часові залежності, глобальний контекст, графову структуру, латентні представлення, розподіл даних), апроксимуючи функцію взаємозалежності між даними виявляють переважно лише статистичну структуру, що не дає змоги повною мірою враховувати стійкі структурні закономірності еволюції кібератак.

У зв'язку з цим, окремого розгляду заслуговують публікації, присвячені дослідженню еволюції кібератак, оскільки виявлення закономірностей їх розвитку є важливою передумовою підвищення ефективності прогнозування. Прикладом таких досліджень, що представлені у науковій літературі у відносно незначній кількості є роботи [11-14].

У роботі [11] запропоновано підхід, який використовує темпоральні векторні представлення для моделювання взаємозв'язків між елементами кібератак. Метод дає змогу аналізувати контекст використання різних компонентів кібератак та відстежувати зміну їх взаємозв'язків у часі, що, у свою чергу, забезпечує виявлення тенденцій розвитку і трансформацій кібератак, а також отримання узагальненого уявлення про їх еволюцію.

У роботі [12] запропоновано підхід до аналізу еволюції кіберзагроз на основі методів обробки природної мови та тематичного моделювання. Для цього інформація про кіберінциденти аналізується з текстових джерел, після чого формується граф знань, що відображає зв'язки між загрозами, подіями та їх характеристиками. Такий підхід дає змогу відстежувати зміну структури кіберзагроз у часі та виявляти нові тенденції їх розвитку.

У роботі [13] проведено системний аналіз еволюції програм-вимагачів, починаючи від ранніх форм шкідливого програмного забезпечення до сучасних складних кібератак. Показано, що розвиток шкідливих програм супроводжується ускладненням механізмів шифрування, появою нових моделей та інтеграцією з іншими техніками кібератак. Проведений аналіз дає змогу простежити закономірності розвитку цього класу кібератак та визначити характерні напрями їх подальшої еволюції.

У роботі [14] запропоновано підхід до дослідження еволюції технік кібератак на основі топологічного аналізу даних. Техніки кібератак розглядаються як елементи багатовимірного простору ознак, до якого застосовуються методи персистентної гомології. Отримані результати дають змогу виявляти глобальні топологічні закономірності еволюції технік кібератак, що відображають стійкі структурні властивості їх розвитку та можуть бути використані для подальшого аналізу і прогнозування кіберзагроз.

Аналіз наведених підходів [11-13] свідчить, що дослідження еволюції кібератак зосереджені переважно на виявленні статистичних або семантичних закономірностей їхнього розвитку. До того ж, зазначені підходи не дозволяють виявляти глобальні структурні закономірності розвитку технік кібератак, що зберігаються незалежно від зміни окремих їхніх характеристик. При цьому варто зазначити, що еволюція кібератак відбувається не лише на рівні самих технік, а й у просторі можливих реалізацій технік, що формується різними способами їх застосування, комбінаціями з іншими техніками та умовами функціонування ІКС. Саме в цьому просторі виникають нові варіанти реалізації кібератак та змінюються їх структурні взаємозв'язки. З цієї причини прогнозування доцільно здійснювати не лише на рівні окремих технік, а на рівні структурних змін у просторі можливих реалізацій технік кібератак. Для цього у статті використано результати дослідження [14], в якому застосовано топологічний аналіз даних для виявлення стійких структурних властивостей еволюції технік кібератак, що дає змогу доповнити статистичні можливості штучних нейронних мереж інформацією про глобальну структуру їх взаємозв'язків.

Метою статті є розробка моделі прогнозування структурних змін у просторі можливих реалізацій технік кібератак на основі топологічних обмежень їх еволюції з використанням темпоральних графових нейронних мереж.

РОЗРОБКА МОДЕЛІ

Оскільки у роботі [14] виявлення закономірностей еволюції кібератак здійснювалось на рівні технік з таксономії [15], як безпосереднього відображення поведінки зловмисної активності в ІКС у вигляді конкретних прийомів реалізації, то завдання прогнозування структурних змін технік кібератак у просторі можливих їх реалізацій також вирішується на основі [15]. При цьому зазначена таксономія технік кібератак природним чином може бути представлена у вигляді графа, вершини якого відповідають технікам, тактикам і платформам, а ребра відображають різні типи взаємозв'язків між ними.

У зв'язку з цим, завдання прогнозування структурних змін технік кібератак може бути сформульовано як прогнозування майбутньої структури відповідного графа. Для вирішення даного завдання доцільним є використання темпоральних графових нейронних мереж [16], які дають змогу враховувати структурні залежності між елементами графа та моделювати їх еволюцію у часі. Вихідні дані:

$V = \{v_1, \dots, v_i, \dots, v_T\}$ – впорядкована у часі множина версій технік кібератак [15], де v_i описує стан графу G_t у момент часу t;

Кожній v_i відповідає гетерогенний граф $G_t = (N_t, E_t)$, де N_t – множина вершин графа, E_t – множина зв'язків між ними;

$Th(v_i) = \{th_{1i}, \dots, th_{ji}, \dots, th_{mi}\}$ – множина технік кібератак у $v_i \in V$.

Обмеження і допущення:

– поля Detection і Mitigation виключено з ознакового простору з метою уникнення внесення захисних процедур в еволюційні патерни технік;
– відповідність технік між v_i та v_{i+1} здійснюється за Mitre_id;
– обрана множина версій технік кібератак 14.1-17.1: 14.1-17.0 для аналізу, 17.1 для порівняння результатів прогнозування;
– структурні зміни між версіями визначаються появою нових або зміною існуючих зв'язків між техніками.

Необхідно: побудувати модель вигляду $F:\{G_1,\dots,G_T\}\to G'_{T+1}$ для формалізації процесу прогнозування майбутньої структури графа G_T технік кібератак з урахуванням топологічних обмежень їх еволюції, сформованих на основі виявлених топологічних закономірностей їх розвитку [14].

Формування простору можливих реалізацій технік кібератак. Простір можливих реалізацій S технік кібератак розглядаємо як багатовимірний простір, у якому кожна техніка th_{ji} описується набором ознак x_i, що характеризують можливі способи її реалізації, умови застосування та взаємозв'язки з іншими техніками, що дає змогу перейти від розгляду технік як ізольованих елементів таксономії до їх представлення у вигляді точок у спільному ознаковому просторі $\mathbb{R}^d$. Так, кожній техніці th_{ji} ставиться у відповідність вектор ознак $x_i=(x_{i1},x_{i2},\dots,x_{id})\in\mathbb{R}^d$, який описує її властивості, зокрема належність до певної тактики, можливі платформи застосування, рівень привілеїв, спосіб реалізації, а також інші характеристики, що визначають контекст використання техніки. Множина векторів для кожної th_{ji} формує простір можливих реалізацій технік кібератак $S=\{x_1,x_2,\dots,x_n\}\subset\mathbb{R}^d$.

Необхідність визначення простору S зумовлена потребою аналізу взаємозв'язків між техніками кібератак на основі положення відносно одна одної, що дає змогу розглядати структуру можливих комбінацій їх використання, а також зміни цих взаємозв'язків у різних версіях таксономії. Іншими словами, така інтерпретація таксономії [15] дає змогу досліджувати еволюцію технік кібератак як зміну структури їх розташування у просторі S та використовувати ці зміни для подальшого прогнозування.

Виявлення топологічних закономірностей еволюції технік кібератак. Топологічні закономірності еволюції технік кібератак отримуємо на основі методу запропонованого в [14], який базується на застосуванні топологічного аналізу даних, зокрема апарату персистентної гомології [17], що дозволяє досліджувати глобальну структуру взаємозв'язків між елементами багатовимірного простору ознак. Так, для кожної версії технік кібератак v_i формується множина точок, де кожна точка відповідає окремій техніці. На основі відстаней між даними точками будується відповідний симпліційний комплекс, до якого застосовується математичний апарат персистентних гомологій $H_k(K_\varepsilon)$ з метою відстеження еволюції H_k у міру зростання порогу ε, при якому будується комплекс. Для кожного класу H_k фіксується пара "народження – зникнення" (b_i,d_i) на основі (1).

$$(H_k(K_\varepsilon),\iota)\cong\bigoplus_i I_{[b_i,d_i]}, \tag{1}$$

де K_ε – комплекс на рівні порогу ε, ι – індуковані включення, які задають відображення $H_k(K_\varepsilon)\to H_k(K_{\varepsilon'})$, $I_{[b_i,d_i]}$ – інтервальний модуль.

Сукупність зазначених пар утворює діаграму персистентності $P_k=\{(b_i,d_i)\}$. На рисунку 1 представлено персистентну діаграму гомологічних класів H_0,H_1 версії технік кібератак 14.1, де сині і помаранчеві точки не техніки, а топологічні структури.

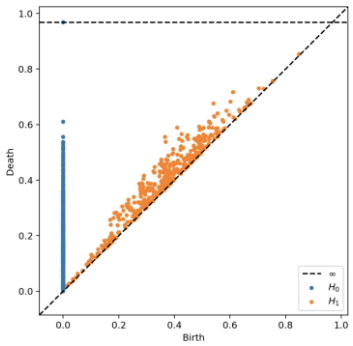

Рис. 1. Персистентна діаграматгомологічних класів H_0, H_1 версіїтехнік кібератак 14.1

Компоненти зв'язності H_0 відповідають групам технік кібератак, що формують взаємопов'язані області у просторі можливих реалізацій. З практичної точки зору це означає, що відповідні техніки мають подібні властивості або використовуються у схожих контекстах реалізації кібератак. Циклічні структури H_1 відображають наявність альтернативних структурних зв'язків між техніками кібератак, які утворюють замкнені ланцюги їх взаємодії. У контексті кібератак дані структури можуть відповідати повторюваним комбінаціям використання технік або різним варіантам реалізації схожих сценаріїв кібератак.

Для дослідження еволюції топологічної структури між різними версіями таксономії технік кібератак було використано підхід vineyard [18], який дозволяє відстежувати зміну топологічних характеристик у часі. Це дає можливість визначати, які топологічні структури зберігаються у різних версіях таксономії, а які виникають або зникають у процесі її еволюції.

Отримані результати дозволили виявити стійкі топологічні закономірності еволюції технік кібератак, що відображають стабільні структурні властивості їх розвитку у просторі можливих реалізацій. Саме ці закономірності у подальшому використовуються для формування топологічних обмежень еволюції технік кібератак та підсилення процесу прогнозування їх структурних змін.

Формування топологічних обмежень еволюції технік кібератак. На основі виявлених у топологічних закономірностях еволюції технік кібератак [14] формується механізм топологічного обмеження прогнозування, який враховує структурні взаємозв'язки між техніками кібератак, виявлені за допомогою персистентної гомології. При чому компоненти зв'язності H_0 не використовуються у формуванні обмежень прогнозування, оскільки подібність технік кібератак або їх використання у схожих контекстах реалізації вже враховується графовою нейронною мережею у процесі навчання. Іншими словами H_0 описує геометрію даних, тоді як H_1 – структуру взаємодій.

У зв'язку з цим, для кожної техніки кібератак th_{ji} визначається множина її топологічних сусідів $N_{H1}(th_{ji})$, яка формується на основі циклічних структур H_1, отриманих у процесі аналізу персистентних діаграм. Належність технік до спільних циклічних структур відображає наявність стійких структурних взаємозв'язків між ними у просторі можливих реалізацій технік кібератак.

Нехай у – об'єкт, з яким може бути пов'язана техніка кібератак th_{ji} (у відповідності до графового блоку простору ознак з [14] – тактика, платформа). Позначимо множину технік, які вже мають зв'язок з у відомій версії таксономії на онові (2).

$$Th_{v_i}(y) = \{th_{ik} \in Th_{v_i} \mid (th_{ik}, y) \in E_t\} \quad (2)$$

Тоді для пари (th_{ji}, y) вводимо функцію топологічної підтримки, яка визначається як частка топологічних сусідів $N_{H1}(th_{ji})$ техніки th_{ji}, що вже мають зв'язок з об'єктом y (3):

$$F_{top}^{sub}(th_{ji}, y) = \frac{count(N_{H1}(th_{ji}) \cap Th_{v_i}(y))}{count(N_{H1}(th_{ji})}, \quad (3)$$

де $count()$ – потужність множини.

Функція топологічної підтримки $F_{top}^{sub}(th_{ji}, y)$ за своєю суттю є аналогічною показнику підтримки, що використовується в задачах пошуку асоціативних правил для оцінки частоти спільної появи елементів [19]. У запропонованій моделі ця ідея використовується для оцінки узгодженості прогнозованого зв'язку між техніками кібератак з їх топологічним оточенням.

Таким чином, отримане значення використовується як апріорна інформація для коригування результатів прогнозування темпоральної графової мережі.

Нехай $p_{gnn}(th_{ji}, y)$ – значення, що прогнозується графовою нейронною мережею для можливого зв'язку між технікою th_{ji} та об'єктом y, тоді скориговане значення визначається у відповідності до виразу (4):

$$\tilde{p}(th_{ji}, y) = p_{gnn}(th_{ji}, y) + \lambda F_{top}^{sub}(th_{ji}, y) \quad (4)$$

де λ – коефіцієнт ваги топологічного обмеження.

На основі викладеного, остаточна ймовірність появи зв'язку між технікою th_{ji} та об'єктом y визначається засобами сигмоїдної функції (5) [20].

$$P(th_{ji}, y) = \sigma\left(\tilde{p}(th_{ji}, y)\right) \quad (5)$$

Таким чином, сформовані топологічні обмеження не забороняють можливі структурні зміни у графі технік кібератак, а коригують результати прогнозування шляхом врахування структурних закономірностей їх еволюції.

Прогнозування структурних змін у просторі можливих реалізацій технік кібератак на основі топологічних обмежень їхньої еволюції.

Послідовність версій таксономії технік кібератак [15] може бути подана у вигляді послідовності гетерогенних графів $G_1, G_2, \dots, G_T$, де кожен граф $G_t = (N_t, E_t)$ відображає структуру взаємозв'язків між техніками, тактиками, а також платформами у версії t: $N_t = N_t^{tech} \cup N_t^{tactic} \cup N_t^{platform}$, а множина технік $Th_{v_i} \in N_t$ представлена у просторі S.

Таким чином, завдання прогнозування полягає не у визначенні нових зв'язків у графі, а у визначенні таких структурних змін, які відповідають можливим новим комбінаціям та варіаціям реалізації технік кібератак у просторі S.

Для цього засобами темпоральної графової мережі на основі версій $G_1, G_2, \dots, G_T$ обчислюється оцінка можливого нового зв'язку між технікою th_{ji} та цільовим об'єктом y. Задамо оцінку можливого нового зв'язку функцією (6):

$$p_{gnn}(th_{ji}, y) = f_\theta(th_{ji}, y, H_T) \quad (6)$$

де θ – параметри темпоральної графової мережі; H_T – історія еволюції графа до моменту T.

Тоді, коригуємо отриману оцінку з урахуванням попередньо визначеної топологічної підтримки (3), сформованої на основі циклічних структур H_1. У результаті скориговане значення обчислюється на основі (4), а ймовірність появи зв'язку технікою th_{ji} та об'єктом y на основі (5).

Однак, на відміну від класичного порогового прийняття рішення (відкидання прогнозованих зв'язків з ймовірністю менше порогового значення), у моделі запропоновано формування прогнозованих зв'язків шляхом відбору кандидатів для кожної техніки окремо на основі (7):

$$Select\big(P\big(th_{ji}, y\big), \tau, k, \delta\big) \tag{7}$$

де τ – мінімальне порогове значення ймовірності; k – максимальна кількість зв'язків, що зберігаються для однієї техніки; δ – допустиме відхилення від найкращого прогнозованого значення у разі використання адаптивного відбору.

Процедура (7) передбачає два можливі режими:

– режим по замовчанню, в якому для кожної техніки th_{ji} обираються не більше ніж k зв'язків з найбільшими значеннями ймовірності, що перевищують τ;
– режимі адаптивного відбору, в якому додатково враховується δ.

Необхідність реалізації процедури (7) у двох режимах викликана потребою врахування ситуацій, коли декілька можливих зв'язків мають близькі значення прогнозованої ймовірності. У таких випадках жорстке обмеження k може призводити до втрати альтернативних варіантів розвитку структури кібератаки. Тому до прогнозу доцільно включити всі зв'язки, значення яких відрізняються від найкращого прогнозу не значно.

Як наслідок, множина прогнозованих зв'язків визначається аналітичним виразом (8):

$$E'_{T+1} = \bigcup_{th_{ij} \in Th_{v_i}} Select\big(P\big(th_{ji}, y\big), \tau, k, \delta\big) \tag{8}$$

У результаті виконання описаних кроків модель формує прогнозовану множину структурних змін у графі технік кібератак. До таких змін належать нові або модифіковані зв'язки між техніками кібератак та елементи контексту їх реалізації (тактиками та платформами), що визначають можливі нові комбінації застосування технік. Сукупність таких зв'язків формує прогнозований граф (9):

$$G'_{T+1} = (N_T, E'_{T+1}) \tag{9}$$

Таким чином, простір S визначає область можливих реалізацій технік кібератак, темпоральна графова нейронна мережа оцінює ймовірності нових структурних зв'язків у цьому просторі, а топологічні обмеження коригують отримані оцінки з урахуванням стійких закономірностей еволюції технік кібератак. Саме це дає змогу прогнозувати не окремі техніки кібератак, а структурні зміни у просторі можливих їх реалізацій.

Отже, відповідно до сформульованої постановки задачі та на основі визначеного простору можливих реалізацій технік кібератак та сформованих топологічних обмежень їх еволюції, модель прогнозування структурних змін у просторі можливих реалізацій технік кібератак може бути представлена як функція (10):

$$F: \{S, G_1, G_2, \dots, G_T, F_{top}^{sub}\} \rightarrow G'_{T+1} = (N_T, E'_{T+1}) \quad (10)$$

де S – простір можливих реалізації кібератак; G_t – граф технік кібератак у версії t; F_{top}^{sub} – топологічні обмеження еволюції технік кібератак.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для оцінки запропонованої моделі використовувався підхід до порівняння прогнозованої структури графа технік кібератак з реальною структурою, що з'являється у наступній версії таксономії – 17.1 [15].

Якість прогнозування визначалася на основі порівняння справжньої множини зв'язків графа версії 17.1 та прогнозованою множиною зв'язків.

Було обрано такі категорії результатів прогнозування [21]:

– True Positive – зв'язки, які були спрогнозовані моделлю і дійсно з'явилися у версії 17.1;
– False Positive – зв'язки, які були спрогнозовані моделлю, але відсутні у реальній структурі графа;
– False Negative – зв'язки, які існують у справжньому графі версії 17.1, але не були спрогнозовані моделлю.

На основі цих значень було обчислено стандартні метрики оцінювання якості прогнозування [21]: Точність (Precision), Повнота (Recall), F1-міра.

Суть експерименту полягала в порівнянні результатів прогнозування зв'язків графа темпоральною нейронною мережею у класичному застосуванні (TGNN) та результатів прогнозування темпоральною нейронною мережею з топологічними обмеженнями еволюції технік кібератак (TGNN+TDA), виявленими на версіях 14.1-17.0. У таблиці 1 наведено порівняння отриманих результатів прогнозування.

Таблиця 1

Порівняння отриманих результатів прогнозування

Показники	TGNN	TGNN+TDA
Точність	0.58	0.73
Повнота	0.70	0.70
F1-міра	0.64	0.71

Варто зазначити, що отримані значення показників прогнозування не можуть безпосередньо порівнюватися з результатами, які наводяться у задачах традиційної класифікації або прогнозування подій кібератак, де значення точності можуть перевищувати 0,9. У даному дослідженні вирішувалася значно складніша задача – прогнозування структурних змін у розрідженому графі можливих реалізацій технік кібератак, що передбачає визначення нових потенційних зв'язків між техніками. Через велику кількість можливих комбінацій та високу розрідженість графа навіть помірні значення метрик прогнозування свідчать про ефективність запропонованого підходу.

На рисунку 2 представлено результати прогнозування структурних змін технік кібератак у вигляді отриманих графів для версії технік 17.1.

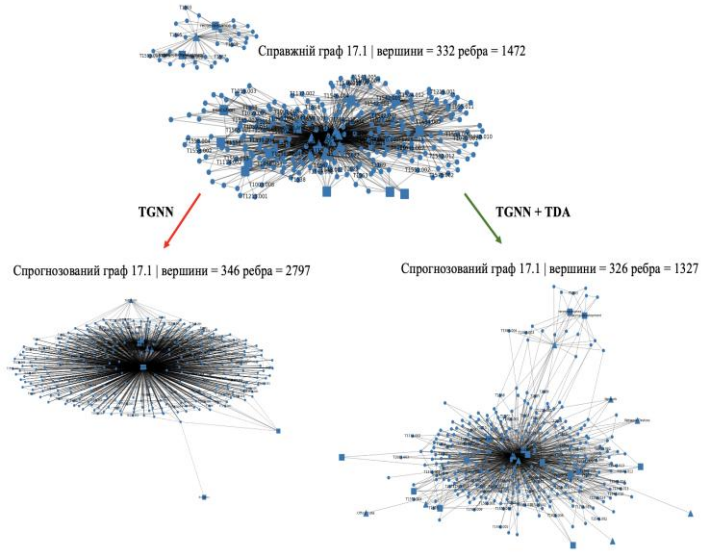

Рис. 2. Результати прогнозування структурних змін технік кібератак у вигляді отриманих графів для версії технік 17.1

З наведених результатів видно, що застосування запропонованого підходу до прогнозування структурних змін технік кібератак, на відміну від класичного застосування темпоральної графової мережі, де кількість згенерованих ребер переважає реальну кількість майже вдвічі, що свідчить про значну кількість хибнопозитивних результатів, забезпечило генерацію вершин та ребер у кількості, значно ближчій до існуючої версії 17.1 з таксономії [15].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті запропоновано модель прогнозування структурних змін технік кібератак у просторі можливих реалізацій на основі топологічних обмежень їх еволюції з використанням темпоральних графових нейронних мереж. На відміну від існуючих підходів, що зосереджені переважно на прогнозуванні окремих подій або наступних дій зловмисника, запропонований підхід спрямований на прогнозування структурних змін у графі взаємозв'язків між техніками кібератак, що дозволяє враховувати можливі нові комбінації їх використання. Сформовано простір можливих реалізацій технік кібератак, виявлено топологічні закономірності їх еволюції на основі персистентної гомології та побудовано механізм топологічних обмежень прогнозування, який враховує циклічні структурні залежності між техніками кібератак. Інтеграція зазначених обмежень у процес прогнозування забезпечила змогу доповнення статистичних можливостей темпоральної графової нейронної мережі інформацією про глобальну структуру взаємозв'язків між техніками.

Результати дослідження показали, що використання топологічних обмежень дозволяє підвищити точність прогнозування з 0,58 до 0,73 при збереженні значення повноти на рівні 0,70 та збільшити значення F1-міри з 0,64 до 0,71. Отримані результати свідчать про ефективність використання топологічного аналізу даних для підсилення прогнозування структурних змін у розріджених графах технік кібератак.

Перспективним напрямком подальших наукових досліджень є розробка моделі адаптації ІКС на основі отриманих результатів прогнозування структурних змін технік кібератак у просторі можливих їх реалізацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. President of Ukraine. (2021). *Cybersecurity strategy of Ukraine* (Decree No. 447/2021, August 26).
2. Fesokha, V. V., Subach, I. Yu., Korotaiev, S. O., & Yuriiovych, S. I. (2020). Zero-day polymorphic cyberattacks detection using fuzzy inference system. *Austrian Journal of Technical and Natural Sciences, 5–6*, 8–13.
3. Fesokha, V. V., & Kysylenko, D. Yu. (2024). Model for determining invariant components in malware behavior based on integration of fuzzy logic and genetic algorithms. *Systems and Technologies of Communication, Informatization and Cybersecurity, 6*, 232–241. https://doi.org/10.58254/viti.6.2024.19.232
4. Fesokha, V. (2024). Features of confrontation between defensive and offensive artificial intelligence in cyberspace. *International Science Journal of Engineering & Agriculture, 3*(4), 105–114. https://doi.org/10.46299/j.isjea.20240304.11
5. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access, 7*, 41525–41550. https://doi.org/10.1109/ACCESS.2019.2908264
6. Zhang, C., Zhou, J., Li, Y., et al. (2020). Network attack prediction based on LSTM. *IEEE Access, 8*, 107367–107376. https://doi.org/10.1109/ACCESS.2020.3000753
7. Ahmed, Y., Azad, M. A., & Asyhari, T. (2024). Rapid forecasting of cyber events using machine learning-enabled features. *Information, 15*(1), 36. https://doi.org/10.3390/info15010036
8. Shen, Y., Mariconti, E., Vervier, P.-A., & Stringhini, G. (2019). Attack2Vec: Leveraging temporal word embeddings to understand the evolution of cyberattacks. In *Proceedings of the 28th USENIX Security Symposium* (pp. 905–921).
9. Wang, S., Chen, Z., Yan, Q., et al. (2021). Cyber attack path prediction based on graph neural networks. *IEEE Access, 9*, 125258–125268. https://doi.org/10.1109/ACCESS.2021.3110976
10. Polatidis, N., Pimenidis, E., Pavlidis, M., Papastergiou, S., & Mouratidis, H. (2018). From product recommendation to cyber-attack prediction: Generating attack graphs and predicting future attacks. *arXiv*. https://doi.org/10.48550/arXiv.1804.10276
11. Sleeman, J., Finin, T., & Halem, M. (2019). *Temporal understanding of cybersecurity threats*. University of Maryland, Baltimore County.
12. Ramsdell, K. A. W., & Esbeck, K. E. (2021). *Evolution of ransomware*. MITRE Corporation. https://healthcyber.mitre.org/wp-content/uploads/2021/08/Ransomware-Paper-V2.pdf
13. Fesokha, V., & Subach, I. (2025). Method for detecting patterns in the evolution of cyberattack techniques based on topological data analysis. *Cybersecurity: Education, Science, Technique, 29*(1), 717–731. https://doi.org/10.28925/2663-4023.2025.29.933
14. MITRE Corporation. (2025). *MITRE ATT&CK®*. https://attack.mitre.org
15. Rossi, E., Chamberlain, B., Frasca, F., Eynard, D., Monti, F., & Bronstein, M. (2020). Temporal graph networks for deep learning on dynamic graphs. *arXiv*. https://doi.org/10.48550/arXiv.2006.10637
16. Carlsson, E., Carlsson, G., & de Silva, V. (2006). An algebraic topological method for feature identification. *International Journal of Computational Geometry & Applications, 16*(4), 291–314. https://doi.org/10.1142/S021819590600204X
17. Cohen-Steiner, D., Edelsbrunner, H., & Morozov, D. (2006). Vines and vineyards by updating persistence in linear time. In *Proceedings of the 22nd Annual Symposium on Computational Geometry* (pp. 119–126). https://doi.org/10.1145/1137856.1137877
18. Agrawal, R., & Srikant, R. (1994). Fast algorithms for mining association rules. In *Proceedings of the 20th International Conference on Very Large Data Bases* (pp. 487–499).
19. Dubey, S. R., Singh, S. K., & Chaudhuri, B. B. (2021). Activation functions in deep learning: A comprehensive survey and benchmark. *arXiv*. https://doi.org/10.48550/arXiv.2109.14545
20. Bilen, A., & Özer, A. B. (2024). Cyber-attack method and perpetrator prediction using machine learning algorithms. *PeerJ Computer Science, 10*, e1917.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Vitalii Fesokha
PhD in Information systems and technologies, Associate Professor, Postdoctoral researcher
Kruty Heroes Military Institute of Telecommunications and Information
Technologies, Kyiv, Ukraine
ORCID: 0000-0001-6612-1970
vitaliifesokha@gmail.com

Ihor Subach
Doctor of Technical Science, Professor, Head of the Department
Institute of Special Communications and Information Protection
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: 0000-0002-9344-713X
igor_subach@ukr.net

MODEL FOR PREDICTING STRUCTURAL CHANGES IN THE SPACE OF POSSIBLE IMPLEMENTATIONS OF CYBERATTACK TECHNIQUES BASED ON TOPOLOGICAL CONSTRAINTS OF THEIR EVOLUTION USING TEMPORAL GRAPH NEURAL NETWORKS

Abstract. In the context of the issue of increasing the cyber resilience of information and communication systems (ICS), the scientific task of predicting structural changes in cyberattack techniques in the space of their possible implementations is solved using the MITRE ATT&CK taxonomy as an example. The relevance of the above is due to the objective limitations of existing approaches to hunting for new ways of implementing cyberthreats (preventing cyberattacks before their implementation), in particular by means of machine learning. Thus, existing types of artificial neural networks used to predict cyberattacks (cyberattack techniques), such as recurrent, transformer, convolutional, graph, temporal graph and autoencoders, although they take into account various aspects of the data structure (feature space, temporal dependencies, global context, graph structure, latent representations, data distribution), approximating the function of interdependence between data, reveal only a statistical structure, which does not allow fully taking into account stable structural evolutionary patterns. In this regard, a model for predicting structural changes in cyberattack techniques in the space of possible implementations based on topological constraints on their evolution using temporal graph neural networks has been developed. The essence of the proposed model is to adjust the results of predicting a temporal graph network based on topological analysis of versions of cyberattack techniques by determining their structural compatibility through joint participation in connectivity components and cyclic structures that reflect stable topological characteristics of their evolution. The feasibility of this approach is due to the value of identifying potential vectors of cyberattack transformation in the space of their possible implementations, which makes it possible to increase the cyber resilience of the ICS to future classes of cyberattacks. An assessment of the effectiveness of the proposed model demonstrates a 15% increase in prediction accuracy and an 8% increase in F1-measure while maintaining a completeness level of 70%, indicating a significant reduction in the number of false positives.

Keywords: cyber resilience; information and communication systems; forecasting; cyberattack techniques; neural networks; temporal graph neural networks; topological data analysis; patterns.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. President of Ukraine. (2021). *Cybersecurity strategy of Ukraine* (Decree No. 447/2021, August 26).
2. Fesokha, V. V., Subach, I. Yu., Korotaiev, S. O., & Yuriiovych, S. I. (2020). Zero-day polymorphic cyberattacks detection using fuzzy inference system. *Austrian Journal of Technical and Natural Sciences, 5–6*, 8–13.

3. Fesokha, V. V., & Kysylenko, D. Yu. (2024). Model for determining invariant components in malware behavior based on integration of fuzzy logic and genetic algorithms. *Systems and Technologies of Communication, Informatization and Cybersecurity*, *6*, 232–241. https://doi.org/10.58254/viti.6.2024.19.232
4. Fesokha, V. (2024). Features of confrontation between defensive and offensive artificial intelligence in cyberspace. *International Science Journal of Engineering & Agriculture*, *3*(4), 105–114. https://doi.org/10.46299/j.isjea.20240304.11
5. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access*, *7*, 41525–41550. https://doi.org/10.1109/ACCESS.2019.2908264
6. Zhang, C., Zhou, J., Li, Y., et al. (2020). Network attack prediction based on LSTM. *IEEE Access*, *8*, 107367–107376. https://doi.org/10.1109/ACCESS.2020.3000753
7. Ahmed, Y., Azad, M. A., & Asyhari, T. (2024). Rapid forecasting of cyber events using machine learning-enabled features. *Information*, *15*(1), 36. https://doi.org/10.3390/info15010036
8. Shen, Y., Mariconti, E., Vervier, P.-A., & Stringhini, G. (2019). Attack2Vec: Leveraging temporal word embeddings to understand the evolution of cyberattacks. In *Proceedings of the 28th USENIX Security Symposium* (pp. 905–921).
9. Wang, S., Chen, Z., Yan, Q., et al. (2021). Cyber attack path prediction based on graph neural networks. *IEEE Access*, *9*, 125258–125268. https://doi.org/10.1109/ACCESS.2021.3110976
10. Polatidis, N., Pimenidis, E., Pavlidis, M., Papastergiou, S., & Mouratidis, H. (2018). From product recommendation to cyber-attack prediction: Generating attack graphs and predicting future attacks. *arXiv*. https://doi.org/10.48550/arXiv.1804.10276
11. Sleeman, J., Finin, T., & Halem, M. (2019). *Temporal understanding of cybersecurity threats*. University of Maryland, Baltimore County.
12. Ramsdell, K. A. W., & Esbeck, K. E. (2021). *Evolution of ransomware*. MITRE Corporation. https://healthcyber.mitre.org/wp-content/uploads/2021/08/Ransomware-Paper-V2.pdf
13. Fesokha, V., & Subach, I. (2025). Method for detecting patterns in the evolution of cyberattack techniques based on topological data analysis. *Cybersecurity: Education, Science, Technique*, *29*(1), 717–731. https://doi.org/10.28925/2663-4023.2025.29.933
14. MITRE Corporation. (2025). *MITRE ATT&CK®*. https://attack.mitre.org
15. Rossi, E., Chamberlain, B., Frasca, F., Eynard, D., Monti, F., & Bronstein, M. (2020). Temporal graph networks for deep learning on dynamic graphs. *arXiv*. https://doi.org/10.48550/arXiv.2006.10637
16. Carlsson, E., Carlsson, G., & de Silva, V. (2006). An algebraic topological method for feature identification. *International Journal of Computational Geometry & Applications*, *16*(4), 291–314. https://doi.org/10.1142/S021819590600204X
17. Cohen-Steiner, D., Edelsbrunner, H., & Morozov, D. (2006). Vines and vineyards by updating persistence in linear time. In *Proceedings of the 22nd Annual Symposium on Computational Geometry* (pp. 119–126). https://doi.org/10.1145/1137856.1137877
18. Agrawal, R., & Srikant, R. (1994). Fast algorithms for mining association rules. In *Proceedings of the 20th International Conference on Very Large Data Bases* (pp. 487–499).
19. Dubey, S. R., Singh, S. K., & Chaudhuri, B. B. (2021). Activation functions in deep learning: A comprehensive survey and benchmark. *arXiv*. https://doi.org/10.48550/arXiv.2109.14545
20. Bilen, A., & Özer, A. B. (2024). Cyber-attack method and perpetrator prediction using machine learning algorithms. *PeerJ Computer Science*, *10*, e1917.

Отримано редакцією журналу / Received: 25.01.26
Прорецензовано / Revised: 15.02.26
Схвалено до друку / Accepted: 26.03.26