DOI: 10.58254/viti.8.2025.18.236

УДК 004.056.5

д-р філософії, доцент Фесьоха В. В. ORCID: 0000-0001-6612-1970 (ВІТІ ім. Героїв Крут)
д-р техн. наук, професор Субач І. Ю. ORCID: 0000-0002-9344-713X
(ІСЗЗІ КПІ ім. Ігоря Сікорського)
Кравчик Р. С. ORCID: 0000-0002-0976-9321 (ХНУПС ім. Івана Кожедуба)

МЕТОД ХРОНОЛОГІЧНОЇ РЕКОНСТРУКЦІЇ ПОДІЙ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ДЛЯ ПОТРЕБ КІБЕРЗАХИСТУ НА ОСНОВІ УЗГОДЖЕННЯ ЛОКАЛЬНИХ ЧАСОВИХ ПРОСТОРІВ

У статті розглянуто актуальне наукове завдання хронологічної реконструкції подій в інформаційно-комунікаційних системах (ІКС) в умовах асинхронності їх підсистем (компонентів) і похибок часових міток. На практиці порядок подій, зафіксований у журналах моніторингу, часто не відповідає реальній послідовності внаслідок дрейфу системних годинників, затримок передавання чи обробки даних, а також асинхронності часових шкал різних джерел подій. Сучасні системи кіберзахисту, орієнтовані на кореляцію подій, нерідко покладаються на таку спотворену хронологію, що призводить до хибних висновків під час аналізу кіберінцидентів і значно ускладнює побудову причинно-наслідкових зв’язків між подіями.

Запропоновано метод хронологічної реконструкції подій, який ґрунтується на відмові від припущення про єдиний глобальний час системи, не потребує синхронізації джерел моніторингу, а також відновлює глобальний порядок на основі опорних зв’язків між подіями з різних журналів подій. Передбачено формування множини локальних часових просторів з журналів подій, визначення опорних та стабілізуючих зв’язків між ними, пошук оптимальних часових зсувів засобами методу сіткового пошуку та інтеграцію результатів у єдину хронологію подій ІКС. Проведене експериментальне дослідження із використанням згенерованих даних на основі технік кібератак MITRE ATT&CK підтверджує ефективність запропонованого підходу – досягнуто точності реконструкції 96 %. Отримані результати свідчать, що метод забезпечує високу достовірність відтворення послідовностей подій за відсутності синхронізації годинників між підсистемами.

Запропонований метод може бути використаний у системах моніторингу та аналізу кіберінцидентів у ІКС для підвищення точності кореляції подій і достовірності реконструкції причинно-наслідкових ланцюгів між ними.

Ключові слова: *інформаційно-комунікаційні системи, події, кіберзахист, локальний часовий простір, часова відносність, кореляція подій.*

V. Fesokha, I. Subach, R. Kravchyk. Method of chronological reconstruction of events in information communication systems for cyber security purposes based on the coordination of local time spaces

The article considers the topical scientific task of chronological reconstruction of events in information and communication systems (ICS) in conditions of asynchronism of their subsystems (components) and time stamp errors. In practice, the order of events recorded in monitoring logs often does not correspond to the actual sequence due to the drift of system clocks, delays in data transmission or processing, as well as the asynchrony of the time scales of different event sources. Modern cyber protection systems focused on event correlation often rely on such distorted chronology, which leads to false conclusions during the analysis of cyber incidents and significantly complicates the establishment of cause-and-effect relationships between events.

A method of chronological reconstruction of events is proposed, which is based on rejecting the assumption of a single global system time, does not require synchronisation of monitoring sources, and restores the global order based on reference links between events from different event logs. It provides for the formation of a set of local time spaces from event logs, the determination of reference and stabilising links between them, the search for optimal time shifts using the grid search method, and the integration of results into a single chronology of ICS events. An experimental study conducted using data generated based on MITRE ATT&CK cyberattack techniques confirms the effectiveness of the proposed approach, achieving 96 % reconstruction accuracy. The results show that the method provides high reliability in reproducing event sequences in the absence of clock synchronisation between subsystems.

The proposed method can be used in cyber incident monitoring and analysis systems in ICS to improve the accuracy of event correlation and the reliability of reconstructing cause-and-effect chains between them.

Keywords: *information and communication systems, events, cyber security, local time space, time relativity, event correlation.*

Актуальність та постановка завдання в загальному вигляді. Сучасні ІКС характеризуються високим рівнем динамічності процесів обробки даних, розподіленістю компонентів та інтенсивністю обміну інформацією в реальному часі. В таких умовах надто складно уникнути спотворення часових міток життєвого циклу подій в ІКС внаслідок різноманітних затримок передачі та обробки даних, асинхронності функціонування складових підсистем або дрейфу системних годинників. Це призводить до того, що порядок подій, зафіксований у журналах реєстрації, часто не відображає їх реальну хронологічну послідовність.

Для систем кіберзахисту, функціональне ядро яких орієнтоване на аналіз подій з метою виявлення кібератак, шкідливого програмного забезпечення або ознак аномальної активності, наприклад, Splunk, Elastic SIEM, Microsoft Sentinel, IBM QRadar, така невідповідність має критичне значення [1; 2]. Так, некоректне впорядкування послідовностей подій, руйнує справжні причинно-наслідкові зв’язки між ними, що в результаті призводить до хибних результатів кореляції та втрати розуміння їх глибинної структури.

Зазначене обумовлює актуальність подальших досліджень щодо реконструкції реальної (найбільш вірогідної) хронології подій в ІКС з метою відтворення їх контекстних взаємозв’язків для потреб кіберзахисту.

Аналіз попередніх досліджень. Дослідження проблематики реконструкції хронології подій в гетерогенних ІКС послідовно розвивалися від моделей причинно-наслідкового зв’язку до інтелектуального аналізу часових даних [3–10]. Перші фундаментальні ідеї було сформульовано у роботі [3], де запропоновано концепцію логічної залежності подій та застосування логічних годинників для визначення їх часткового порядку. Даний підхід хоч і став основою для узгодженості подій в ІКС, однак передбачає синхронізовану взаємодію процесів і не враховує спотворення часових міток у журналах подій. Подальший розвиток представлено роботою [4], в якій розглядається концепція віртуального часу, векторних годинників і глобальних станів системи. Кожен процес має вектор значень щодо подій в інших процесах, а кожна подія фіксує поточний стан цього вектора, на основі чого приймається рішення про хронологію подій (якщо подія А має менший вектор, ніж подія В, то А передувала В).

Іншим напрямом вирішення даного завдання став підхід на основі інтервальної логіки [5], що оперує множиною базових відношень між часовими інтервалами подій (між двома інтервалами подій можуть бути лише певні можливі відношення). Однак даний підхід має значні обмеження щодо аналізу фаз життєвого циклу великих обсягів подій з різних джерел, де час може бути неповним або спотвореним. Подібним чином моделі темпоральних баз даних [6] зосереджуються на описі хронології подій двома атрибутами: фактичним часом і часом фіксації, але вимагають достовірності часових міток і не враховують затримки під час реєстрації подій.

Наступний етап досліджень [7], присвячено потоковій обробці неупорядкованих даних в масштабних обчислювальних середовищах. Було запропоновано концепції “час події”, “час обробки” і “позначки синхронізації”, що дали змогу мінімізувати затримки під час потокового аналізу. Підхід хоч і орієнтований на обчислення в реальному часі, проте не спрямований на реконструкцію причинно-наслідкових зав’язків між подіями, що вже були зафіксовані в журналах.

Сучасні наукові праці [8–10] розвивають напрям цифрової криміналістики й аналізу хронології кіберінцидентів. Зокрема, у роботі [8], запропоновано концептуальну модель опису співвідношення між реальною послідовністю подій і їх реконструкцією за цифровими артефактами. Модель розділяє ці простори на квадранти (події: відомі, частково відомі, припущення, невідомі), які відображають різні рівні достовірності даних, що дає змогу систематизувати процес відновлення послідовностей подій в ІКС. Недоліком даного підходу є відсутність формального механізму узгодження подій між незалежними джерелами.

У роботі [9] зосереджено увагу на проблематиці вузького підходу до опису причинно-наслідкових зав'язків у журналах подій. Запропоновано удосконалене журналювання з використанням ідентифікаторів джерел ініціювання подій, що дає змогу відслідковувати причинно-наслідкові зв'язки у межах декількох додатків. Недолік: складна реалізація у гетерогенних ІКС, відсутність алгоритму глобального узгодження подій. У праці [10] досліджено використання великих мовних моделей для автоматизації побудови хронології кіберінцидентів. Модель аналізує текстові описи подій, встановлює їх послідовність і формує певні пояснення, що забезпечує високий рівень автоматизації, однак не гарантує коректного узгодження часових просторів і може генерувати нелогічні послідовності.

Попри значний прогрес у наведених дослідженнях, завдання реконструкції хронології подій в ІКС, залишається не вирішеним у повному обсязі. Існуючі підходи не забезпечують достовірного відновлення послідовностей подій у випадках, коли часові дані спотворені або несинхронізовані між різними підсистемами. Відтак, реконструкція хронології подій в ІКС, потребує врахування їх часової відносності, де часові дані не є абсолютними, а залежать від контексту підсистеми, в межах якої вони були зафіксовані [11]. Кожна підсистема ІКС формує власний локальний часовий простір, у якому події сприймаються в певній послідовності, що може відрізнятися від інших.

Таким чином, завдання відновлення загальної хронології подій в ІКС, полягає не у їх приведені до "універсального часу", а в узгодженні між локальними часовими просторами, які відображають індивідуальну часову перспективу кожного джерела спостереження.

Метою статті є розробка методу хронологічної реконструкції подій в ІКС для потреб кіберзахисту на основі узгодження локальних часових просторів.

Основна частина. Запропонований метод базується на поєднанні переваг вищезгаданих підходів, однак передбачає відмову від припущення про наявність єдиного глобального часу в ІКС та перехід до моделі множинних часових систем спостереження, що дає змогу відновлювати найбільш вірогідну послідовність подій в умовах часової відносності, коли часові дані різних підсистем можуть бути спотворені або неузгоджені. Його основу становить формування локальних часових просторів для кожного джерела подій в ІКС та подальше узгодження їх зав'язків, з урахуванням функціональних залежностей і логічних обмежень.

Під *локальним часовим простором* будемо розуміти власну часову систему відліку конкретного джерела або контексту фіксації подій в ІКС (агент, підсистема, сесія, процес), у межах якої порядок подій вважається внутрішньо узгодженим і спостерігається без обов'язкової відповідності зовнішнім часовим шкалам.

Для формування локальних часових просторів використовується ковзне вікно аналізу T, яке визначається параметрами моніторингу системи кіберзахисту. Вікно T охоплює останні події в ІКС, що надходять з різних джерел, і відповідає інтервалу часу, за який система кіберзахисту виконує агрегацію даних.

Вихідні дані:

$LS = \{L_1, L_2, \dots, L_K\}$ – множина локальних часових просторів (журналів подій) ІКС;

$E = \bigcup_{i=1}^{k} L_i -$ повна множина подій в ІКС за вікно часу T;

$\forall\, L_i \in LS$ – відома послідовність подій $\{e_{i1}, e_{i2}, \dots, e_{in}\}$ за вікно часу T;

$\forall\, e_{ij} \in L_i$ відомо:

локальна часова мітка $t_i(e_{ij})$;

атрибути події $a_i(e_{ij})$ – тип, процес/сесія/користувач, ідентифікатори поточного та батьківського процесу;

$D = \{(e_{ij}, e_{ij+1}) | e_{ij}, e_{ij+1} \in E, e_{ij} \to e_{ij+1}\}$ – множина обов'язкових функціональних залежностей між подіями вигляду:

"створення процесу → старт процесу";

"запит → відповідь";

"батьківський процес → процес нащадок";
"аутентифікація → виконання команди".
Необхідно: побудувати глобальну хронологію подій в ІКС за час Т, яка:
узгоджує локальні послідовності подій з LS;
враховує часову відносність подій (різні підсистеми мають різний час).
Обмеження і допущення:
часові мітки з різних підсистем не синхронізовані;
допускається відсутність деяких подій у журналах реєстрації.

Реалізація **методу хронологічної реконструкції подій в ІКС для потреб кіберзахисту на основі узгодження локальних часових просторів** передбачає виконання наступних кроків:

Крок 1. Ініціалізація локальних часових просторів

На даному кроці кожен журнал подій джерел ІКС формалізується як окремий локальний часовий простір $L_i \in LS$, у межах якого зафіксована послідовність подій $L_i = \{e_{i1}, e_{i1}, \dots, e_{in}\}$, вважається достовірною. Зазначене твердження базується на властивості внутрішньої причинної узгодженості процесів у межах одного джерела подій. Так, навіть якщо абсолютні часові мітки зазнають спотворення, відносний порядок подій журналу залишається достовірним, оскільки визначається фактичним порядком обробки запитів у черзі запису.

Метою кроку є перетворення фактичної послідовності подій L_i у формальну множину непорушних обмежень, які мають зберігатися під час побудови глобальної хронології подій. Для кожного L_i задаємо множину пар подій, які відображають внутрішній порядок їх фіксації (1).

$$SP_{L_i} = \{(e_{ij} \prec e_{ij+1}) | i = 1, \dots, n-1\}, \quad (1)$$

де $e_{ij} \prec e_{ij+1} - e_{ij}$ передує e_{ij+1}, $n-1$ – кількість пар подій L_i.

Сформована множина пар для кожного часового простору L_i є основою для недопущення ситуацій, коли подія e_{i5} з L_i виявиться у глобальному порядку подій раніше ніж подія e_{i2} з L_i при узгодженні множини локальних часових просторів LS.

Крок 2. Визначення опорних зв'язків між локальними просторами

На даному кроці здійснюється встановлення взаємозв'язків, які відображають функціональні залежності між подіями різних підсистем ІКС (виникнення однієї події зумовлює настання іншої), але в межах одного контексту (транзакції або сесії ІКС). Мета – визначення на основі виявлених функціональних залежностей таких пар подій локальних послідовностей, причинно-наслідковий зв'язок яких є незмінним незалежно від викривленнях у часових мітках.

На попередньому етапі для кожного L_i зафіксовано послідовність подій, де кожна подія описується вектором атрибутів (тип, часова мітка, номер користувача, процесу, сесії) (2).

$$A(e_{ij}) = \{a_1, a_2, \dots, a_m\}. \quad (2)$$

Для кожної пари локальних часових просторів L_p і L_q виконується співставлення подій на основі функції (3):

$$F_{sim}(e_{pi}, e_{qj}) = w_f S_f + w_a S_a + w_t S_t, \quad (3)$$

де S_f – функціональна сумісність згідно з правилами, що містить D; S_a – контекстна сумісність подій (атрибути подій); S_t – часова близькість; w_f, w_a, w_t – вагові коефіцієнти значущості кожної складової (w_f – [0.45-0.5], w_a – [0.35-0.4], w_t – [0.1-0.2]).

Пара подій вважається співставленою коректно, якщо $F_{sim}(e_{pi}, e_{qj}) \geq 0.7$ відповідно до загальноприйнятої концепції порогів подібності [12; 13]. Усі пари подій, що задовольняють наведеній умові, формують множину опорних міжпросторових зв'язків (4).

$$F_{hard} = \{(e_{pi} \prec e_{qj}) | F_{sim}(e_{pi}, e_{qj}) \geq 0.7\}, \quad (4)$$

тоді як усі пари подій, що не задовольняють умові (4), формують множину слабких зв'язків, представлену аналітичним виразом (5).

$$F_{soft} = \{(e_{pi} \prec e_{qj}) | F_{sim}(e_{pi}, e_{qj}) < 0.7\}. \quad (5)$$

Таким чином, множині F_{hard} відведена роль опорних зв'язків в послідовностях подій для подальшого забезпечення узгодження їх хронології між незалежними джерелами спостереження. Множина F_{soft} виконує стабілізуючу функцію у процесі узгодження хронології подій між незалежними джерелами у випадку дефіциту опорних зв'язків або неповного логування. На рисунку 1 схематично зображено визначені міжпросторові опорні зв'язки локальних часових просторів L_p і L_q.

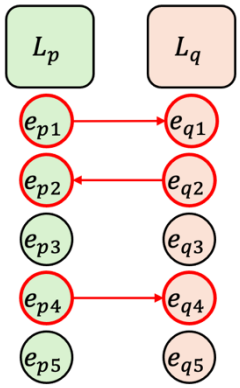

Рис. 1. Визначені опорні зв'язки між локальними часовими просторами L_p і L_q

Крок 3. Узгодження локальних часових просторів

З урахуванням часової відносності подій, визначеної раніше, узгодження локальних часових просторів полягає не у приведені всіх часових міток до єдиного абсолютного часу системи, а у взаємному вирівнюванні їхніх локальних шкал. Кожна підсистема ІКС фіксує події за власною часовою шкалою, тому метою цього кроку є встановлення кореляцій між такими просторами, а також компенсація відносних зсувів часу на основі отриманих на попередньому кроці опорних зв'язків F_{hard} і стабілізуючих зв'язків F_{soft}.

В умовах гетерогенних ІКС вибір єдиного еталонного локального простору для узгодження є некоректним, оскільки жоден з них не може вважатися апріорно достовірнішим за інші, до того ж, кожен з них може зазнати деструктивного впливу. Тому, узгодження часових просторів доцільно розглядати як задачу комбінаторної оптимізації, в якій необхідно знайти такі зсуви часу Δt_k для кожного локального часового простору L_k,, щоб мінімізувати кількість порушених опорних зв'язків між подіями різних L_k. Для кожного набору

$\Delta t = \{\Delta t_1, \Delta t_2, \dots, \Delta t_m\}$ виконується перевірка: чи збережено внутрішня послідовність подій у межах кожного L_k і скільки міжпросторових опорних зв'язків порушено.

Підбір індивідуальних зсувів часу Δt_k для кожного L_k здійснюється методом сіткового пошуку [14]. Цільова функція в такому випадку має вигляд (6):

$$\min_{\Delta t} C(\Delta t) = \sum_{(e_p, e_q) \in F_{hard}} \upsilon(e_p, e_q, \Delta t_p, \Delta t_q) + w_{soft} \sum_{(e_p, e_q) \in F_{soft}} \upsilon(e_p, e_q, \Delta t_p, \Delta t_q), \quad (6)$$

де $\upsilon(e_p, e_q, \Delta t_p, \Delta t_q) = \begin{cases} 1, \text{ якщо } t(e_p) + \Delta t_p > t(e_q) + \Delta t_q, \\ 0, \text{інакше.} \end{cases}$

w_{soft} – ваговий коефіцієнт впливу F_{soft}.

Після перевірки всіх варіантів сітки обирається оптимальна комбінація часових зсувів $\Delta t^* = arg \min_{\Delta t} C(\Delta t)$, що мінімізує кількість порушених обмежень. У випадку рівності кількості порушень опорних зв'язків перевага надається рішенню з меншими абсолютними зсувами часу. Використання множини слабких зв'язків F_{soft} дає змогу запобігти фрагментації послідовностей подій (м'яке збереження логіки навіть там, де причинно-наслідковий зв'язок не доведено).

Результатом узгодження є набір скоригованих часових міток $C(\Delta t)$, при яких максимально зберігається функціональний порядок подій між локальними часовими просторами.

На рисунку 2 проілюстровано узагальнену схему узгодження локальних часових просторів ІКС.

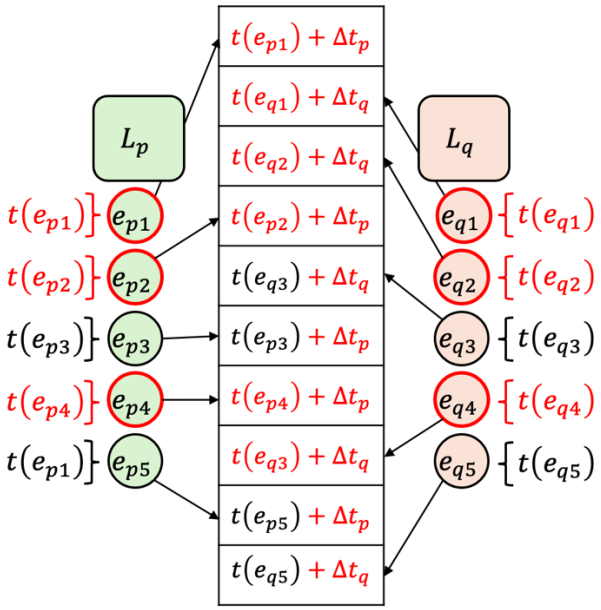

Рис. 2. Узагальнена схема узгодження локальних часових просторів L_p і L_q ІКС

Крок 4. Інтеграція в процес кіберзахисту

На завершальному кроці результати узгодження локальних часових просторів інтегруються в єдину інформаційну модель подій ІКС, сумісну з процесами аналітики та кореляції системи кіберзахисту.

На основі отриманих результатів на попередньому кроці формується узгоджена хронологія, що зберігає локальну послідовність подій кожного джерела спостереження, водночас забезпечуючи найбільш вірогідну послідовність подій в ІКС за ковзне вікно T (9).

$$H = \{e'_1, e'_2, \dots, e'_m\} \subseteq E. \tag{9}$$

Для кожного $e'_i \in H$ формується запис (10):

$$e'_i = \langle id_i, t_i, src_i, type_i, context_i, trust_i \rangle, \tag{10}$$

де t_i – скоригована часова мітка; src_i – джерело події; $type_i$ – тип подій (що відбулося); $context_i$ – контекст подій; $trust_i$ – показник довіри відповідно до значень F_{hard} і F_{soft}.

Рішення щодо кіберінцидентів в ІКС приймаються системою кіберзахисту, тоді як запропонований метод забезпечує коректність хронологічної послідовності подій для їх функціонування.

Експериментальне дослідження. Для оцінки запропонованого методу, щодо реконструкції хронології подій в ІКС для завдань кіберзахисту на основі узгодження локальних часових просторів, було згенеровано набір даних, що містить послідовності подій з таксономії технік кібератак [15].

Умови експерименту:

кількість технік кібератак – 30 (Execution, Persistence, Lateral Movement, Exfiltration, Command and Control, Credential Access, Privilege Escalation, Defense Evasion тощо);

кількість послідовностей подій – 100;

довжина кожної послідовності – 15 подій;

кількість журналів подій – 3;

кількість правил, що описують обов'язкові функціональні залежності – 18.

Для моделювання спотворень хронології подій кожній еталонній послідовності будо додано часові мітки. Події з еталонних послідовностей було випадковим чином розподілено між трьома журналами подій. У кожному журналі спотворено часові мітки (лінійний дрейф).

Після виконання етапів запропонованого методу засобами мови програмування Python було отримано реконструйовані глобальні послідовності подій. Оцінку якості реконструкції проведено шляхом порівняння відновленого порядку подій із еталонним порядком на основі Kendall Tau distance [16]:

кількість виявлених опорних пар подій – 8293;

середнє значення переставлених пар подій на послідовність ≈ 4;

точність реконструкції послідовностей подій – 96 %.

Висновки. У статті вирішується завдання реконструкції хронології подій в ІКС для потреб кіберзахисту на основі узгодження локальних часових просторів.

Запропоновано метод, який ґрунтується на відмові від припущення про єдиний глобальний час системи та передбачає реконструкцію локальних часових шкал підсистем ІКС з урахуванням функціональних залежностей між подіями. Передбачено формування множини локальних часових просторів із журналів подій, визначення опорних та стабілізуючих зв'язків між ними, пошук оптимальних часових зсувів та інтеграцію результатів у єдину хронологію подій ІКС.

Проведене експериментальне дослідження, із використанням згенерованих даних на основі технік кібератак MITRE ATT&CK, підтверджує ефективність запропонованого підходу – досягнуто точності реконструкції 96 %. Отримані результати свідчать, що метод забезпечує високу достовірність відтворення послідовностей подій за відсутності синхронізації годинників між підсистемами.

Перспективним напрямком подальших наукових досліджень є розробка методу самонавчання системи кіберзахисту на основі керованого онтологічного оновлення, який опиратиметься на коректну хронологію подій в ІКС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Субач І., Кубрак В., Микитюк А. Архітектура та функціональна модель перспективної проактивної інтелектуальної системи SIEM-системи для кіберзахисту об’єктів критичної інфраструктури. *Information Technology and Security.* 2019. № 7 (2). С. 208–215. URL: https://doi.org/10.20535/2411-1031.2019.7.2.190570.

2. Субач І. Ю., Власенко О. В., Архітектура інтелектуальної SIEM-системи для виявлення кіберінцидентів у базах даних інформаційно-комунікаційних систем військового призначення. *Системи і технології зв’язку, інформатизації та кібербезпеки*. 2023. Вип. 4. DOI: 10.58254/viti.4.2023.07.82.

3. Lamport L. Time, Clocks, and the Ordering of Events in a Distributed System. *Communications of the ACM*. 1978. Vol. 21, no. 7. P. 558–565. URL: https://lamport.azurewebsites.net/pubs/time-clocks.pdf.

4. Mattern F. Virtual Time and Global States of Distributed Systems. *Parallel and Distributed Algorithms.* North-Holland, 1989. P. 215–226. URL: https://homes.cs.washington.edu/~arvind/cs425/doc/mattern89virtual.pdf.

5. Allen J. F. Maintaining Knowledge about Temporal Intervals. *Communications of the ACM*. 1983. Vol. 26, no. 11. P. 832–843. URL: https://cse.unl.edu/~choueiry/Documents/Allen-CACM1983.pdf.

6. Snodgrass R. T. Temporal Databases. *IEEE Computer*. 1986. Vol. 19, no. 9. P. 35–42. URL: https://www2.cs.arizona.edu/~rts/pubs/EDC.pdf.

7. Akidau T., Bradshaw R., Chambers C., Chernyak S., Dimov D. et al. *The Dataflow Model: A Practical Approach to Balancing Correctness, Latency, and Cost in Massive-Scale, Unbounded, Out-of-Order Data Processing.* Proc. of the VLDB Endowment. 2015. Vol. 8, no. 12. P. 2188–2203. URL: https://static.googleusercontent.com/media/research.google.com/uk//pubs/archive/43864.pdf.

8. Breitinger F., Studiawan H., Hargreaves C. SoK: Timeline based event reconstruction for digital forensics: Terminology, methodology, and current challenges. *arXiv preprint* arXiv:2504.18131. 2025. URL: https://arxiv.org/abs/2504.18131.

9. Johan Olegård. *Tracking event causality for improved forensic analysis and logging sufficiency.* Forensic Science International: Digital Investigation, 2025. DOI: 10.1016/j.fdi.2025.09.012.

10. Loumachi F. Y., Ghanem M. C., Ferrag M. A. Advancing Cyber Incident Timeline Analysis Through Retrieval-Augmented Generation and Large Language Models. *Computers*. 2025. Vol. 14, no. 2. P. 67. URL: https://doi.org/10.3390/computers14020067.

11. Фесьоха В., Субач І. Концептуальна основа підвищення кіберстійкості інформаційно-комунікаційних систем в умовах еволюції кіберзагроз. *Кібербезпека: освіта, наука, техніка.* 2025. Vol. 4, no. 28. P. (–). DOI: 10.28925/2663-4023.2025.28.856. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/856.

12. Dos Santos J. B., Heuser C. A., Moreira V., Wives L. K. Automatic Threshold Estimation for Data Matching Applications. *Information Sciences.* 2011. Vol. 181. Pp. 3665–3688. URL: https://www.sciencedirect.com/science/article/pii/S0020025510002380.

13. Rekabsaz N., Lupu M., Hanbury A., Zuccon G. Exploration of a Threshold for Similarity Based on Uncertainty in Word Embedding. In: *Advances in Information Retrieval: 39th European Conference on IR Research (ECIR 2017), Aberdeen, UK, April 8–13, 2017. Lecture Notes in Computer Science*, Vol. 10193. Pp. 396–409. Springer, Cham. DOI: 10.1007/978-3-319-56608-5_31. URL: https://doi.org/10.1007/978-3-319-56608-5_31.

14. Ilemobayo J. A., Durodola O. I., Alade O., Awotunde O. J., Olanrewaju A. T., Falana O., Ogungbire A., Osinuga A., Ogunbiyi D., Ifeanyi A., Odezuligbo I. E., Edu O. E. “Hyperparameter Tuning in Machine Learning: A Comprehensive Review”. *Journal of Engineering Research and Reports.* 2024. Vol. 26, no. 6. P. 388–395. DOI: 10.9734/jerr/2024/v26i61188.

15. MITRE ATT&CK® Updates. *MITRE ATT&CK® – Updates.* 2025. URL: https://attack.mitre.org/resources/updates/.

16. Mercadier Y. *Kendall Tau Distance.* In: *distancia* 0.0.1 documentation. 2024. URL: https://distancia.readthedocs.io/en/latest/KendallTau.html#kendall-tau-distance.