УДК 004.056:004.75

МЕТОД ПРОГНОЗУВАННЯ КОМПРОМЕТАЦІЇ ВУЗЛІВ У СЕРЕДОВИЩІ EDGE ТА FOG ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Станіслава Кудренко, Олексій Німич, Ігор Макєєв

У статті запропоновано метод прогнозування компрометації вузлів у середовищі edge та fog для систем критичної інфраструктури. Актуальність дослідження зумовлена зростанням кількості кібератак на розподілені IoT-мережі, у яких порушення роботи окремих компонентів може призводити до втрати цілісності даних, зниження надійності вузлів та порушення функціонування інформаційної інфраструктури. Запропонований метод базується на аналізі поведінкових і мережевих характеристик компонентів edge/fog-середовища, формуванні вектора ознак, розрахунку показника аномальності, інтегрального ризику компрометації, рівня довіри та узагальненого показника небезпеки. Особливістю підходу є поєднання детекції аномалій із прогнозуванням станів, що дозволяє не лише виявляти поточні відхилення у поведінці вузлів, а й оцінювати ймовірність їх переходу до потенційно небезпечного стану. Використання елементів машинного навчання та нейронних мереж створює передумови для адаптації методу до динамічних умов функціонування розподілених систем. Запропонований підхід може бути використаний для підвищення рівня захисту даних, своєчасного виявлення аномальної поведінки та підтримки проактивних механізмів безпеки мереж IoT у системах критичної інфраструктури.

Ключові слова: безпека мереж IoT, кібератаки, надійність вузлів, критична інфраструктура, захист даних, детекція аномалій, машинне навчання, нейронні мережі, аномальна поведінка, цілісність даних, edge computing, fog computing, прогнозування станів, компрометація вузлів.

Вступ

Зростання кількості підключених пристроїв, сенсорів, контролерів та інтелектуальних модулів у сучасних інформаційних системах призводить до суттєвого збільшення обсягів даних, які необхідно обробляти, передавати та аналізувати в режимі, наближеному до реального часу. Особливо це стосується систем критичної інфраструктури, де затримка в обробленні інформації, втрата цілісності даних або зниження достовірності результатів аналізу може впливати на стабільність технологічних процесів, безпеку об'єктів та якість прийняття управлінських рішень. До таких систем належать енергетичні мережі, транспортні комплекси, промислові IoT-системи, логістичні платформи, системи моніторингу стану обладнання та інші розподілені середовища, у яких велика кількість компонентів взаємодіє між собою через мережеву інфраструктуру [3–5].

Для зменшення навантаження на центральні сервери та скорочення часу передавання даних дедалі ширше застосовуються технології **edge computing** та **fog computing**. Edge computing передбачає оброблення даних безпосередньо біля джерела їх виникнення або на периферійних обчислювальних компонентах. Fog computing, у свою чергу, формує проміжний рівень між периферійними пристроями та хмарною інфраструктурою, забезпечуючи попереднє оброблення, фільтрацію, агрегацію та маршрутизацію даних [3–5]. Така архітектура дозволяє зменшити затримки, підвищити оперативність реагування та ефективніше використовувати обчислювальні ресурси. Водночас розподілений характер edge/fog-середовищ ускладнює контроль за станом окремих елементів системи та створює додаткові ризики, пов'язані з порушенням цілісності, достовірності й захищеності даних [6, 7].

У межах цієї роботи під вузлом розподіленої edge/fog-системи будемо розуміти обчислювальний або комунікаційний компонент, який бере участь у прийманні, попередньому обробленні, передаванні або агрегації даних. У контексті критичної інфраструктури такими компонентами можуть бути edge-пристрої, fog-шлюзи, локальні контролери або проміжні обчислювальні елементи, що забезпечують взаємодію між периферійними пристроями та центральними сервісами. На відміну від звичайного сенсора, який переважно формує первинні вимірювання, такий компонент може впливати на маршрут передавання, якість попереднього оброблення, достовірність агрегованих даних і загальну узгодженість роботи системи.

Компрометованим у цій роботі вважається такий компонент edge/fog-середовища, нормальна поведінка якого була порушена внаслідок несанкціонованого доступу, шкідливого програмного впливу, зміни конфігурації, підміни даних або іншого деструктивного чинника. Небезпека

компрометації полягає в тому, що зовні елемент системи може залишатися працездатним, однак його дії вже не відповідають очікуваному профілю функціонування. Він може передавати викривлені значення, затримувати повідомлення, порушувати логіку маршрутизації, формувати некоректні результати попередньої обробки або створювати надмірне навантаження на суміжні компоненти. У системах критичної інфраструктури такі відхилення є особливо небезпечними, оскільки помилка на проміжному рівні оброблення даних може вплинути на подальші рішення, що приймаються автоматизованою системою керування [6–8].

З позиції безпеки мереж IoT компрометація окремого компонента не обмежується локальним порушенням його роботи. У розподіленому середовищі такий елемент може стати джерелом поширення спотворених даних, причиною зниження надійності вузлів, фактором порушення цілісності інформаційних потоків або точкою подальшого розвитку кібератаки. Унаслідок цього зростає ризик виникнення аномальної поведінки системи, коли окремі компоненти починають функціонувати неузгоджено, а результати оброблення даних втрачають необхідний рівень достовірності. Для критичної інфраструктури такі процеси є особливо небезпечними, оскільки вони можуть впливати на безперервність технологічних процесів, стабільність мережевої взаємодії та загальний рівень захисту даних [6, 7, 10].

Традиційні засоби захисту інформації та виявлення загроз часто орієнтовані на фіксацію вже наявного інциденту. Зокрема, сигнатурні методи дозволяють виявляти відомі типи атак або шкідливої активності за заздалегідь визначеними ознаками [8, 9]. Такі підходи залишаються важливими для побудови систем інформаційної безпеки, однак у динамічних edge/fog-середовищах їх можливостей може бути недостатньо. Це пояснюється тим, що нові або модифіковані кібератаки можуть не мати відомих сигнатур, а зміна поведінки скомпрометованого компонента може відбуватися поступово й не одразу проявлятися як очевидна загроза. Тому актуальним стає не лише виявлення факту компрометації, а й прогнозування ймовірності її виникнення на основі попередніх змін у поведінці компонентів системи.

Прогнозування станів у цьому контексті означає аналіз поточних і попередніх характеристик роботи елементів edge/fog-середовища з метою визначення ймовірності переходу до небезпечного або аномального стану. До таких характеристик можуть належати частота передавання повідомлень, затримки, кількість помилок, зміна обсягів трафіку, нетипові запити, відхилення від звичайного профілю поведінки, порушення цілісності даних або зниження узгодженості з іншими компонентами системи. Якщо такі зміни мають стійкий або наростаючий характер, вони можуть свідчити про підготовку атаки, початкову стадію компрометації або розвиток аномального процесу. Саме тому використання методів машинного навчання, нейронних мереж та аналізу аномальної поведінки є перспективним напрямом для побудови проактивних механізмів захисту розподілених IoT-систем [1, 2].

Аномальна поведінка компонента не завжди безпосередньо означає наявність кібератаки, оскільки вона може бути спричинена технічним збоєм, нестачею ресурсів, нестабільним каналом зв'язку або помилкою конфігурації. Проте для систем критичної інфраструктури важливо своєчасно виявляти навіть потенційно небезпечні відхилення, оскільки вони можуть бути першими ознаками майбутнього порушення. У цьому полягає відмінність прогнозування від звичайної детекції: детекція переважно відповідає на питання, чи вже відбулася небезпечна подія, тоді як прогнозування дозволяє оцінити, чи може така подія виникнути найближчим часом. Отже, прогнозування компрометації компонентів edge/fog-середовища дає змогу перейти від реактивної моделі захисту до проактивної, у якій система не лише реагує на загрози, а й заздалегідь визначає елементи з підвищеним ризиком.

Таким чином, *актуальним науково-прикладним завданням* є розроблення методу прогнозування компрометації вузлів у середовищі edge та fog для систем критичної інфраструктури. Такий метод має враховувати поведінкові характеристики компонентів, ознаки аномальної активності, параметри мережевої взаємодії, рівень надійності вузлів і можливі порушення цілісності даних. Його застосування дозволить підвищити ефективність раннього виявлення небезпечних станів, зменшити ризик поширення негативного впливу в розподіленій системі та забезпечити більш стійке функціонування інформаційної інфраструктури в умовах кібератак і кіберзагроз.

Метою даної роботи є розроблення методу прогнозування компрометації вузлів у середовищі edge та fog для об'єктів критичної інфраструктури на основі аналізу поведінкових характеристик, ознак аномальної активності та динаміки зміни станів компонентів розподіленої

системи. Запропонований підхід орієнтований на підвищення надійності вузлів, збереження цілісності даних, своєчасну детекцію потенційно небезпечних змін та підвищення рівня захищеності IoT-мереж, що функціонують у складі критичної інформаційної інфраструктури.

Метод прогнозування компрометації вузлів у середовищі edge та fog

Запропонований метод призначений для прогнозування ймовірності компрометації вузлів у розподіленому edge/fog-середовищі на основі аналізу поведінкових характеристик компонентів системи, параметрів мережевої взаємодії та ознак аномальної активності. Основна ідея методу полягає в тому, що компрометація вузла не завжди проявляється миттєво як явна атака. Часто перед цим спостерігаються поступові зміни в його поведінці: збільшення затримок, зростання кількості помилок, нетипова інтенсивність передавання повідомлень, порушення узгодженості з іншими вузлами або зміна структури мережевих взаємодій. Саме ці зміни можуть бути використані для раннього прогнозування небезпечного стану.

Нехай розподілена edge/fog-система складається з множини вузлів:

$$N = \{n_1, n_2, \dots, n_m\}, \qquad (1)$$

де N— множина вузлів системи, n_i— окремий вузол, m— загальна кількість вузлів у системі.

Для кожного вузла n_iу момент часу tформується вектор ознак, що характеризує його поточний стан:

$$X_i(t) = \{x_{i1}(t), x_{i2}(t), \dots, x_{ik}(t)\}, \qquad (2)$$

де $X_i(t)$— вектор поведінкових і мережевих ознак i-го вузла в момент часу t; $x_{ij}(t)$— значення j-ї ознаки; k— кількість ознак, що використовуються для аналізу.

До складу вектора $X_i(t)$можуть входити такі показники: частота передавання повідомлень, середня затримка, кількість помилок, обсяг переданого трафіку, частота повторних запитів, кількість відхилених або некоректних повідомлень, рівень узгодженості даних з іншими компонентами системи, а також інші параметри, що характеризують поведінку вузла. Таким чином, формула (2) дозволяє перейти від загального опису стану вузла до кількісного подання його поведінки.

Оскільки різні ознаки можуть мати різні одиниці вимірювання та діапазони значень, перед подальшим аналізом виконується нормалізація:

$$\hat{x}_{ij}(t) = \frac{x_{ij}(t) - x_j^{min}}{x_j^{max} - x_j^{min}}, \qquad (3)$$

де $\hat{x}_{ij}(t)$ — нормалізоване значення j-ї ознаки для i-го вузла; x_j^{min}та x_j^{max}— мінімальне та максимальне значення відповідної ознаки в навчальній або поточній вибірці.

Нормалізація за формулою (3) забезпечує приведення всіх ознак до єдиного масштабу, що дозволяє коректно порівнювати їх між собою та використовувати в єдиній моделі прогнозування.

Для оцінювання відхилення поточної поведінки вузла від нормального профілю вводиться показник аномальності:

$$A_i(t) = \sum_{j=1}^{k} w_j \cdot | \hat{x}_{ij}(t) - \bar{x}_{ij} |, \qquad (4)$$

де $A_i(t)$— показник аномальності поведінки i-го вузла в момент часу t; w_j— ваговий коефіцієнт важливості j-ї ознаки; $\bar{x}_{ij}$— еталонне або середнє значення відповідної ознаки для нормального режиму роботи.

Формула (4) дозволяє врахувати не лише факт відхилення певної ознаки від норми, а й важливість цієї ознаки для загальної оцінки стану вузла. Наприклад, для систем критичної інфраструктури більшу вагу можуть мати ознаки, пов'язані з цілісністю даних, затримкою повідомлень або нетиповим обсягом трафіку.

Оскільки для прогнозування важливо враховувати не лише поточний стан, а й динаміку змін, вводиться інтегральний показник ризику за часове вікно:

$$R_i(t) = \alpha A_i(t) + (1 - \alpha) R_i(t - 1), \qquad (5)$$

де $R_i(t)$— інтегральний ризик компрометації i-го вузла в момент часу t; $A_i(t)$— поточний показник аномальності, визначений за формулою (4); $R_i(t-1)$— значення ризику на попередньому кроці; α— коефіцієнт чутливості моделі, $0 < \alpha < 1$.

Формула (5) дозволяє врахувати накопичувальний характер небезпечних змін. Якщо вузол демонструє аномальну поведінку лише один раз, ризик може залишатися помірним. Якщо ж відхилення повторюються або посилюються, інтегральний показник $R_i(t)$поступово зростає, що є підставою для прогнозування можливої компрометації.

Для переходу від інтегрального ризику до ймовірнісної оцінки використовується функція прогнозування:

$$P_i(t + \Delta t) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 R_i(t) + \beta_2 A_i(t))}}, \qquad (6)$$

де $P_i(t+\Delta t)$— прогнозована ймовірність компрометації i-го вузла на інтервалі часу $t+\Delta t$; Δt— горизонт прогнозування; $\beta_0, \beta_1, \beta_2$— параметри моделі, які можуть бути визначені експериментально або під час навчання.

Формула (6) дає змогу отримати значення ймовірності в діапазоні від 0 до 1. Чим вищими є значення $R_i(t)$та $A_i(t)$, тим більшою є прогнозована ймовірність компрометації вузла. Такий підхід може бути реалізований як у вигляді логістичної моделі, так і як спрощений вихідний шар нейронної мережі.

Для прийняття рішення про потенційно небезпечний стан вузла використовується порогове правило:

$$S_i(t+\Delta t) = \begin{cases} 1, & \text{якщо } P_i(t+\Delta t) \geq P_{cr}, \\ 0, & \text{якщо } P_i(t+\Delta t) < P_{cr}, \end{cases} \quad (7)$$

де $S_i(t+\Delta t)$— прогнозований стан вузла; $S_i = 1$означає потенційно скомпрометований або небезпечний стан; $S_i = 0$означає нормальний або допустимий стан; P_{cr}— критичне порогове значення ймовірності.

Формула (7) дозволяє класифікувати вузли за рівнем ризику. Якщо прогнозована ймовірність перевищує заданий поріг P_{cr}, вузол позначається як такий, що потребує додаткової перевірки, обмеження доступу, перенаправлення трафіку або інших захисних дій.

Для врахування надійності вузла вводиться коефіцієнт довіри:

$$T_i(t) = 1 - R_i(t), \quad (8)$$

де $T_i(t)$— рівень довіри до i-го вузла в момент часу t; $R_i(t)$— інтегральний ризик компрометації, визначений за формулою (5).

З формули (8) випливає, що зі зростанням ризику компрометації рівень довіри до вузла зменшується. Такий коефіцієнт може бути використаний для адаптивного керування навантаженням, вибору маршруту передавання даних або обмеження участі небезпечного компонента в обробленні критичної інформації.

Узагальнений критерій небезпеки вузла можна подати у вигляді:

$$C_i(t) = \lambda_1 A_i(t) + \lambda_2 R_i(t) + \lambda_3 (1 - T_i(t)), \quad (9)$$

де $C_i(t)$— узагальнений показник небезпеки i-го вузла; $\lambda_1, \lambda_2, \lambda_3$— вагові коефіцієнти, що визначають значущість відповідних складових; $A_i(t)$— показник аномальності; $R_i(t)$— інтегральний ризик; $T_i(t)$— рівень довіри до вузла.

Формула (9) поєднує поточні аномальні прояви, накопичений ризик і зниження довіри до вузла. Це дозволяє не лише прогнозувати компрометацію, а й ранжувати компоненти системи за рівнем потенційної небезпеки.

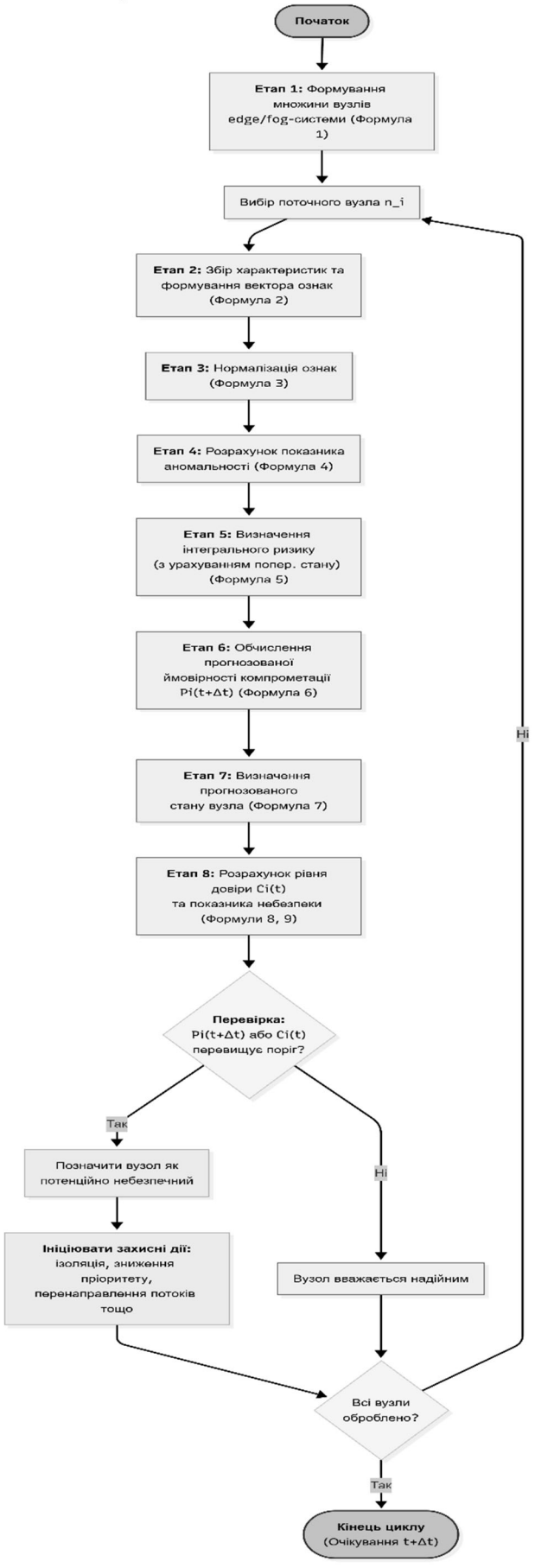

Рис. 1. Блок-схема методу прогнозування компрометації вузлів у середовищі edge та fog

На рис. 1 наведено блок-схему реалізації методу прогнозування компрометації вузлів у середовищі edge та fog. Запропонована схема відображає послідовність етапів аналізу стану вузлів розподіленої системи, починаючи з формування множини компонентів edge/fog-середовища та завершуючи прийняттям рішення щодо їх надійності або потенційної небезпеки.

На першому етапі формується множина вузлів edge/fog-системи відповідно до виразу (1). Після цього для кожного поточного вузла n_iвиконується послідовна процедура аналізу. Спочатку здійснюється збір його поведінкових і мережевих характеристик та формується вектор ознак згідно з формулою (2). До таких ознак можуть належати параметри трафіку, затримки передавання повідомлень, кількість помилок, частота нетипових запитів, показники узгодженості даних та інші характеристики, що відображають поточний стан компонента системи.

На наступному етапі виконується нормалізація ознак за формулою (3), що дозволяє привести різнорідні показники до єдиного масштабу. Після цього розраховується показник аномальності поведінки вузла за формулою (4). Цей показник відображає ступінь відхилення поточного стану вузла від очікуваного або еталонного профілю функціонування.

Далі визначається інтегральний ризик компрометації з урахуванням попереднього стану вузла за формулою (5). Такий підхід дозволяє врахувати не лише поточне відхилення, а й накопичувальну динаміку змін у поведінці компонента. На основі отриманого значення ризику та показника аномальності обчислюється прогнозована ймовірність компрометації $P_i(t + \Delta t)$згідно з формулою (6). Потім за пороговим правилом (7) визначається прогнозований стан вузла.

Окремо в схемі передбачено розрахунок рівня довіри $T_i(t)$та узагальненого показника небезпеки $C_i(t)$відповідно до формул (8) і (9). Ці показники використовуються для уточнення рішення щодо поточного стану компонента edge/fog-середовища. Якщо прогнозована ймовірність компрометації $P_i(t + \Delta t)$або показник небезпеки $C_i(t)$перевищує задане порогове значення, вузол позначається як потенційно небезпечний. У такому разі система може ініціювати захисні дії, зокрема ізоляцію вузла, зниження його пріоритету, обмеження участі в обробленні даних або перенаправлення інформаційних потоків через більш надійні компоненти.

Якщо порогове значення не перевищено, вузол вважається надійним, після чого здійснюється перехід до перевірки завершення оброблення всієї множини вузлів. Якщо залишаються необроблені елементи, цикл повторюється для наступного вузла. Після завершення аналізу всіх вузлів система переходить до очікування наступного часового інтервалу $t + \Delta t$, у межах якого процедура прогнозування може бути повторена.

Таким чином, наведена блок-схема демонструє циклічний характер запропонованого методу та його орієнтацію на проактивне виявлення потенційно небезпечних станів вузлів edge/fog-середовища. На відміну від реактивних підходів, які фіксують уже наявний інцидент, запропонована процедура дозволяє заздалегідь оцінювати ризик компрометації, визначати компоненти з підвищеним рівнем небезпеки та своєчасно ініціювати захисні дії в системах критичної інфраструктури..

Висновки

У статті запропоновано метод прогнозування компрометації вузлів у середовищі edge та fog для систем критичної інфраструктури. Розроблений підхід базується на аналізі поведінкових і мережевих характеристик компонентів розподіленої системи, розрахунку показника аномальності, інтегрального ризику компрометації, рівня довіри та узагальненого показника небезпеки. Це дозволяє не лише фіксувати факт появи аномальної поведінки, а й оцінювати ймовірність переходу вузла до потенційно небезпечного стану.

Запропонована формалізація методу забезпечує поетапне подання процесу прогнозування: від формування множини вузлів і вектора ознак до прийняття рішення за пороговим правилом. Такий підхід є зручним для використання в edge/fog-середовищах, оскільки враховує як поточні параметри функціонування компонентів, так і динаміку їх зміни в часі. Завдяки цьому метод може бути використаний як складова проактивної системи захисту даних у розподілених IoT-мережах критичної інфраструктури.

Особливістю запропонованого методу є поєднання детекції аномальної поведінки з прогнозуванням ризику компрометації. На відміну від реактивних підходів, які переважно орієнтовані на виявлення вже наявного інциденту, запропонована схема дозволяє

заздалегідь визначати компоненти з підвищеним рівнем небезпеки. Це створює передумови для своєчасного застосування захисних дій, зокрема ізоляції потенційно небезпечного вузла, зниження його пріоритету, обмеження участі в обробленні даних або перенаправлення інформаційних потоків через більш надійні компоненти.

Подальші дослідження доцільно спрямувати на проведення імітаційного моделювання роботи запропонованого методу для різних сценаріїв функціонування edge/fog-систем. Зокрема, перспективним є дослідження сценаріїв одиничної та множинної компрометації вузлів, поступового наростання аномальної активності, різної інтенсивності мережевого трафіку, зміни порогових значень, а також функціонування системи за умов обмежених обчислювальних ресурсів. Окремої уваги потребує порівняння ефективності запропонованого підходу з класичними методами детекції аномалій та оцінювання його впливу на своєчасність виявлення загроз, рівень хибних спрацювань і стійкість системи до кібератак.

Таким чином, запропонований метод може бути використаний як теоретична основа для побудови проактивних механізмів виявлення потенційно небезпечних станів у edge/fog-середовищах. Його застосування сприятиме підвищенню надійності вузлів, збереженню цілісності даних і посиленню захищеності інформаційної інфраструктури об'єктів критичного призначення.

Список літератури

[1] Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey // ACM Computing Surveys. 2009. DOI: https://doi.org/10.1145/1541880.1541882

[2] Mohammadi M., Al-Fuqaha A., Sorour S., Guizani M. Deep learning for IoT big data and streaming analytics: A survey // IEEE Communications Surveys & Tutorials. 2018. DOI: https://doi.org/10.1109/COMST.2018.2844341

[3] Satyanarayanan M. The emergence of edge computing // Computer. 2017. Vol. 50, No. 1. P. 30–39. DOI: https://doi.org/10.1109/MC.2017.9

[4] Bonomi F., Milito R., Zhu J., Addepalli S. Fog computing and its role in the Internet of Things // Proceedings of the MCC Workshop on Mobile Cloud Computing. 2012. DOI: https://doi.org/10.1145/2342509.2342513

[5] Buyya R., Srirama S. N. Fog and Edge Computing: Principles and Paradigms. Wiley, 2019.

[6] NIST. Security and Privacy Controls for Information Systems and Organizations. NIST SP 800-53 Rev. 5. 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[7] ENISA. Threat Landscape for the Internet of Things. 2020. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-the-internet-of-the-internet-of-things

[8] Khrashchevskyi R., Klobukov V., Kozlovskyi V., Akhramovych V., Lazarenko S. Method of calculating information protection from mutual influence of users in social networks // International Journal of Computer Network and Information Security. 2023. Vol. 15, No. 5. DOI: https://doi.org/10.5815/IJCNIS.2023.05.03

[9] Hilgurt S. Y., Davydenko A. M., Matovka T. V., Prygara M. P. Tools for analyzing signature-based hardware solutions for cyber security systems // Journal of Cyber Security and Mobility. 2023.

[10] Гільгурт С. Я. Методи та засоби створення реконфігуровних сигнатурних засобів захисту інформації комп'ютерних систем і мереж : дис. … д-ра техн. наук : 05.13.05 – комп'ютерні системи та компоненти. Київ, 2020.

METHOD FOR PREDICTING NODE COMPROMISE IN EDGE AND FOG ENVIRONMENTS FOR CRITICAL INFRASTRUCTURE

The paper proposes a method for predicting node compromise in edge and fog environments for critical infrastructure systems. The relevance of the study is determined by the increasing number of cyberattacks on distributed IoT networks, where disruption of individual components may lead to data integrity violations, reduced node reliability, and degradation of information infrastructure operation. The proposed method is based on the analysis of behavioral and network characteristics of edge/fog components, feature vector formation, anomaly score calculation, integrated compromise risk assessment, trust level estimation, and the use of a generalized danger indicator. A distinctive feature of the approach is the combination of anomaly detection with state prediction, which makes it possible not only to identify current deviations in node behavior but also to estimate the probability of their transition to a potentially dangerous state. The

use of machine learning and neural network elements provides the basis for adapting the method to dynamic operating conditions of distributed systems. The proposed approach can be used to improve data protection, support timely detection of anomalous behavior, and implement proactive IoT network security mechanisms in critical infrastructure systems.

Keywords: IoT network security, cyberattacks, node reliability, critical infrastructure, data protection, anomaly detection, machine learning, neural networks, anomalous behavior, data integrity, edge computing, fog computing, state prediction, node compromise.

Кудренко Станіслава Олексіївна, к.т.н., доцент, доцент кафедри технічного захисту інформації, Державний університет «Київський авіаційний інститут», м.Київ, Україна.

Kudrenko Stanislava, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Technical Information Protection, State University "Kyiv Aviation Institute", Kyiv, Ukraine., Kyiv, Ukraine.

E-mail:stanislava.kudrenko@npp.nau.edu.ua.

ORCID ID: 0000-0002-0759-3908

Німич Олексій Віталійович, аспірант кафедри кібербезпеки, Державний університет «Київський авіаційний інститут», м.Київ, Україна.

Oleksii Nimych, PhD student of the Department of Cybersecurity State university «Kyiv aviation institute», Kyiv, Ukraine.

E-mail: 5356349@stud.kai.edu.ua

ORCID ID: 0000-0003-1759-7088

Ігор Генрихович Макєєв, аспірант кафедри кібербезпеки, «Державний університет «Київський авіаційний інститут», м.Київ, Україна.

Ihor Makieiev, PhD student of the Department of Cybersecurity of the State university «Kyiv aviation institute», Kyiv, Ukraine.

E-mail: 8390988@stud.kai.edu.ua

ORCID ID: 0009-0009-8679-5