КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1242
УДК 004.056:004.75:004.8

Шуклін Герман Вікторович
кандидат технічних наук, доцент
доцент кафедри інженерії програмного забезпечення в енергетиці
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID: 0000-0003-2507-384X
mathacadem-kiev@ukr.net

Шавловський Ярослав Сергійович
аспірант кафедри технічних систем кіберзахисту
Державний університет інформаційно-комунікаційних технологій, м. Київ, Україна
ORCID: 0009-0006-2725-5996
shavlovskyyaroslav@gmail.com

Пепа Юрій Володимирович
кандидат технічних наук, доцент
професор кафедри технічних систем кіберзахисту
Державний університет інформаційно-комунікаційних технологій, м. Київ, Україна
ORCID: 0000-0003-2073-1364
yurka14@ukr.net

Іванченко Євгенія Вікторівна
доктор технічних наук, професор
директор Навчально-наукового інституту кібербезпеки та захисту інформації
Державний університет інформаційно-комунікаційних технологій, м. Київ, Україна
ORCID: 0000-0003-3017-5752
evivancenko@gmail.com

МЕТОД АДАПТИВНОГО ОЦІНЮВАННЯ ЙМОВІРНОСТІ ВИТОКУ ІНФОРМАЦІЇ В МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ ДЛЯ МАШИННОГО НАВЧАННЯ

Анотація. У статті представлено формалізовану модель витоку інформації в мережах спеціального призначення (МСП) та розроблено метод адаптивного оцінювання ймовірності витоку інформації в таких мережах. Актуальність дослідження зумовлена зростанням кількості складних цільових кіберзагроз, використанням багаторівневих атак, прихованих каналів передавання даних, а також підвищенням ролі інсайдерських загроз у сучасних інформаційно-комунікаційних системах. Показано, що традиційні засоби захисту, орієнтовані переважно на безпеку периметра, сигнатурне виявлення та статичні політики доступу, не забезпечують належного рівня протидії витоку інформації в умовах динамічної зміни стану середовища функціонування МСП. У роботі запропоновано формалізацію МСП у вигляді сукупності вузлів, каналів передавання інформації та факторів ризику, які є підґрунтям виникнення витоку. Розроблений метод базується на інтеграції мережевих, хостових та контекстних індикаторів безпеки, нормуванні ознак, формуванні вектора факторів ризику, адаптивному оновленні вагових коефіцієнтів і визначенні інтегральної функції ризику з подальшим обчисленням ймовірності витоку інформації. Особливістю методу є можливість його застосування в реальному масштабі часу з урахуванням змін поведінки користувачів, режимів роботи мережі та рівня поточних загроз. Наведено приклад практичної реалізації запропонованого підходу, який демонструє послідовність обробки індикаторів безпеки, оцінювання ризику та прийняття рішень щодо реагування на інциденти. Отримані результати підтверджують, що застосування запропонованого методу дає змогу підвищити ефективність виявлення передумов витоку інформації, знизити ризик компрометації конфіденційних даних і забезпечити адаптацію системи захисту до нових типів загроз в умовах цілеспрямованої протидії.

Ключові слова: кібербезпека; витік інформації; мережі спеціального призначення; протидія витокам; модель загроз; адаптивна оцінка ризику.

ВСТУП

Як правило, МСП – це мережі, які обслуговують інформаційно-комунікаційні системи (ІКС) оборонних, правоохоронних об'єктів, об'єктів критичної інфраструктури, банківської сфери та інших чутливих сферах, де виставляються підвищені вимоги до конфіденційності, цілісності та доступності інформації. Витік інформації в таких мережах може призвести не тільки до економічних збитків, але й до загроз національній безпеці. Сучасні методи захисту інформації значною мірою спираються на сигнатурні засоби виявлення, статичні політики доступу та ізольовані механізми запобігання витокам (DLP). Однак наявність стійких загроз, які породжують цільові атаки, інсайдерських загроз і прихованих каналів передачі даних демонструє обмеженість зазначених підходів. У зв'язку з цим виникає необхідність розробки нових методів протидії витоку інформації, орієнтованих на комплексний і адаптивний аналіз процесів функціонування МСП.

Постановка проблеми. У МСП, що використовуються в системах оборонного, правоохоронного, банківського та іншого критично важливого призначення, витік інформації становить суттєву загрозу для безпеки даних і стабільності функціонування ІКС. Традиційні засоби захисту, орієнтовані переважно на сигнатурне виявлення, контроль периметра та статичні політики доступу, не забезпечують належної ефективності в умовах багаторівневих атак, інсайдерських загроз і використання прихованих каналів передавання даних.

У зв'язку з цим виникає потреба у розробленні формалізованого методу, який давав би змогу комплексно враховувати мережеві, хостові та контекстні індикатори безпеки, адаптивно оцінювати ймовірність витоку інформації та своєчасно виявляти передумови реалізації загроз у реальному масштабі часу. Саме розв'язання цієї проблеми є необхідною умовою підвищення ефективності протидії витоку інформації в МСП.

Аналіз досліджень і публікацій. В роботі [1] розглянуто застосування методів глибокого навчання для виявлення інсайдерських загроз. Автори акцентують увагу на тому, що традиційні сигнатурні методи недостатньо ефективні для виявлення легітимних користувачів, дії яких поступово набувають аномального або шкідливого характеру. Вони обґрунтували доцільність використання моделей машинного навчання для аналізу поведінкових ознак користувачів, журналів подій, активності доступу до файлів і мережевих взаємодій. Водночас у зазначеному дослідженні основну увагу приділено загальним підходам до виявлення інсайдерів, тоді як питання адаптивного оцінювання ймовірності витоку інформації в МСП залишається недостатньо розкритим. Автори роботи [2] узагальнили сучасні підходи до протидії інсайдерським загрозам. Дослідники вказали, що інсайдерська загроза є однією з найскладніших для формалізації, оскільки вона може реалізовуватися через поєднання технічних, організаційних і поведінкових факторів. Також підкреслено необхідність комплексного аналізу подій безпеки, контексту діяльності користувача, рівня доступу та характеру операцій з інформаційними ресурсами.

Досліджуються поведінкові підходи до виявлення інсайдерських загроз у роботі [3], де значну увагу приділено аналізу дій користувачів, часових характеристик активності, нетипових звернень до ресурсів, змін у шаблонах доступу та інших поведінкових індикаторів. Такий підхід є важливим для побудови систем адаптивного оцінювання, оскільки в МСП небезпечними можуть бути не лише явно заборонені дії, а й формально дозволені операції, що виконуються в нетипових умовах або у нетиповій послідовності. Разом із тим поведінкові моделі потребують доповнення мережевими, хостовими та контекстними індикаторами, оскільки ізольований аналіз поведінки користувача не завжди дозволяє повноцінно встановити факт підготовки або реалізації витоку інформації. Робота [4] присвячена управлінню ризиками інсайдерських атак з урахуванням готовності до цифрової криміналістики. Ефективна система кіберзахисту має не лише виявляти інциденти, а й забезпечувати накопичення доказової інформації, придатної для подальшого аналізу. Такий підхід є особливо важливим для МСП, де необхідно забезпечувати трасованість подій, збереження журналів доступу, контроль дій користувачів та можливість подальшої реконструкції інциденту.

Окремий напрям сучасних досліджень пов'язаний із виявленням витоку даних через мережеві канали, зокрема DNS-тунелювання та DNS over HTTPS. Так, в [5] автори запропонували легковаговий гібридний підхід до виявлення екс-фільтрації даних через DNS із використанням методів машинного навчання. Однак такий підхід переважно орієнтований на один тип каналу витоку і не охоплює повною мірою хостові та поведінкові фактори. В той же час в [6] розглянуто систему виявлення витоку даних через DNS-тунелювання в реальному масштабі часу. У цій роботі важливим є акцент на оперативність виявлення, оскільки для захищених МСП критичним є не лише факт виявлення загрози, а й швидкість реагування на неї. Зазначений підхід підтверджує доцільність використання потокових даних і автоматизованого аналізу мережевої активності. Разом із тим у контексті МСП необхідним є розширення

такого підходу шляхом урахування рівня критичності вузлів, режиму функціонування мережі, прав користувачів і поточного рівня загроз. Автори [7] досліджували виявлення екс-фільтрації даних через DNS та HTTPS. Показано, що шифрування DNS-запитів ускладнює традиційний аналіз мережевого трафіку та знижує ефективність класичних засобів контролю периметра. Це свідчить про необхідність переходу від суто сигнатурного аналізу до аналізу непрямих ознак, статистичних характеристик, поведінкових патернів і динамічних змін у мережевій активності.

Вчені у [8] систематизують сучасні підходи до аналітики кібербезпеки в корпоративному середовищі. Автори підкреслюють значення інтеграції різнорідних джерел даних, зокрема журналів подій, мережевих потоків, поведінкових ознак, даних кінцевих пристроїв і контекстної інформації. Саме такий інтеграційний підхід є методологічно близьким до задачі адаптивного оцінювання ймовірності витоку інформації, оскільки дає змогу перейти від аналізу окремих подій до комплексного оцінювання стану безпеки системи.

Проте в більшості робіт цього напряму недостатньо формалізовано механізм перетворення різнорідних індикаторів у єдину інтегральну функцію ризику.

Відмітимо роботу [9], у якій розглядаються питання математичного моделювання керування процесами інформаційної безпеки в системі державного регулювання кібернетичною безпекою фондового ринку. Цінним є формалізація процесів управління інформаційною безпекою та використання математичних моделей для опису складних кібернетичних процесів. Результати підтверджують доцільність застосування формалізованих моделей для оцінювання стану захищеності інформаційних систем. Водночас специфіка МСП, а також питання адаптивного оновлення параметрів оцінювання ризику витоку інформації потребують окремого розгляду. Дослідження [10] присвячене динамічному виявленню та класифікації критичних об’єктів уваги в умовах кризових подій. Важливим є сам принцип динамічного аналізу об’єктів, стан яких змінюється під впливом зовнішніх і внутрішніх факторів. Такий підхід може бути використаний як концептуальна основа для побудови систем, що не лише фіксують події безпеки, а й визначають їхню критичність, пріоритетність і потенційний вплив на функціонування захищеної МСП.

Проведений аналіз джерел свідчить, що наявні дослідження достатньо ґрунтовно розкривають окремі аспекти проблеми: виявлення інсайдерських загроз, аналіз поведінкових аномалій, протидію DNS екс-фільтрації, використання машинного навчання в кібербезпеці, управління ризиками та математичне моделювання процесів інформаційної безпеки. Проте більшість існуючих підходів має фрагментарний характер і, як правило, орієнтована або на окремий клас загроз, або на конкретний канал витоку, або на певний рівень захисту – мережевий, хостовий чи організаційний.

Існуючі підходи до запобігання витоку інформації можна умовно розділити на три групи:

1. Методи захисту периметру: брандмауери, проксі, ведення журналу, перевірка пакетів з відслідковуванням стану, аудит, тестування на проникнення, аналіз вразливостей;
2. Хост: автентифікація, антивіруси, брандмауери, IDS, IPS, паролі, хешування, ведення журналу, аудит, тестування на проникнення, аналіз вразливостей;
3. Організаційно-адміністративні методи: шифрування, контроль доступу, резервне копіювання, тестування на проникнення, аналіз вразливостей.

Для МСП зазначені методи застосовуються в умовах жорстких обмежень щодо сумісності, обчислювальних ресурсів і допустимих змін архітектури мережі. Крім того, більшість існуючих рішень не враховує динамічний характер загроз і можливість комбінування різних каналів витоку інформації (мережевих, електромагнітних, логічних). Отже, актуальним науковим завданням є розробка формалізованого підходу, що дозволяє:

- описувати процес витоку інформації як багатофакторний і динамічний;
- враховувати особливості функціонування МСП;
- адаптивно оцінювати ймовірність витоку інформації в реальному масштабі часу.

Мета статті – розробка методу підвищення протидії витоку інформації в МСП на основі формалізованого моделювання процесів витоку та адаптивної оцінки ризиків.

Задачі дослідження:

1. Провести аналіз існуючих методів і моделей виявлення та оцінювання ризику витоку інформації в МСП, визначити їхні переваги, обмеження та обґрунтувати необхідність застосування саме адаптивного підходу з урахуванням мережевих, хостових і контекстних індикаторів безпеки;
2. Розробити метод адаптивного оцінювання ймовірності витоку інформації в МСП на основі формалізованої моделі, системи факторів ризику та механізму оновлення вагових коефіцієнтів, а також оцінити його ефективність на прикладі практичного сценарію функціонування мережі.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Математична модель методу. Модель витоку інформації в МСП будемо формалізувати в представлення цих мереж у вигляді системи S, елементами якої є три множини:

$$S = \langle X, Y, Z \rangle \tag{1}$$

де $X = \{x_i\}$; $i = \overline{1,N}$ – множина вузлів МСП; $Y = \{y_j\}$; $j = \overline{1,m}$ – множина каналів передачі інформації, включаючи і скриті; $Z = \{z_l\}$; $l = \overline{1,K}$ – множина факторів, які є підгрунтям витоку інформації.

До факторів, які є підгрунтям витоку інформації, будемо відносити:

- уразливість програмного забезпечення, яке обслуговує МСП;
- параметри мережевих протоколів, які забезпечують функціонування МСП;
- параметри, які характеризують поведінку користувачів;
- режими роботи МСП;
- рівень загрози витоку інформації.

Процес витоку інформації є стохастичним, який характеризується визначенням ймовірності $P_{вит}(t)$, яку в загальному випадку будемо представляти наступним чином

$$P_{вит}(t) = f\left[x_i, y_j, z_l(t)\right] \tag{2}$$

На основі формалізації (1) розробимо метод адаптивної оцінки ймовірності (2), який буде включати в себе шість послідовних етапів для створення методики машинного навчання виявленню і запобіганню загроз МСП. Розіб'ємо його на етапи.

Етап 1. Метою цього етапу є отримання даних спостереження, які характеризують передумови витоку інформації.

Для отримання на виході ідентифікаторів безпеки на вхід системи поступає інформація щодо мережі (NetFlow/IPFIX, L7-логи шлюзів, DNS/HTTP(S)/SMTP, VPN, проксі, IDS/IPS); інформація щодо хостів (EDR/AV подія, Sysmon/аудит операційної системи, логи додатків, робота з файлами/USB/печаткою); ідентифікаційні дані (AD/LDAP, автентифікація користувачів та їх привілеї, MFA) і контекстні дані (режим роботи МСП, рівень загроз, чергування та зміни авторизованих користувачів, класифікація даних та вузлів). Після здійснення обробки вхідних даних (об'єктами є вузли, користувачі, канали прийому і передачі інформації) на вихід надходить множина первинних індикаторів $C = \{c_i, i = \overline{1,n}\}$ за об'єктами та часовими вікнами.

Етап 2. Метою другого етапу є перетворення ознак, які мають різні розмірності у факторі ризику $f_i(t) \in [0,1]$; $i = \overline{1,k}$.

Вхідними даними є множина $C = \{c_i, i = \overline{1,n}\}$ і першим кроком здійснюється фільтрація шуму. Після цього здійснюється нормування елементів множини C за наступним правилом

$$\overline{c_i} = \frac{c_i - c_{\min}}{c_{\max} - c_{\min}} \tag{3}$$

Після здійснення нормування за формулою (3) формується вихідний вектор $F(t)$ факторів ризику

$$F(t) = \|f_i\|_{1xk} \tag{4}$$

Етап 3. Метою третього етапу є побудова закону змін вагових коефіцієнтів, що є адаптивним процесом оцінюванням ймовірності.

Вхідними даними є вектор (4) за яким визначаються початкові ваги $w_i(t=0)$; $i = \overline{1,k}$. Оновлення ваг здійснюється за наступною рівністю

$$w_i(t+\tau) = \frac{w_i(t) + \lambda_i \mu_i(t)}{\sum_{i=1}^{k}\left[w_i(t) + \lambda_i \mu_i(t)\right]} \tag{5}$$

де $\mu_i(t)$ – внесок фактору $f_i(t)$, що є координатою вектору (4), на момент часу t у виявлення витоку інформації, або передумов для витоку; λ_i – швидкість адаптації при наявності i-го фактору, значення якої належить відрізку $[-1;1]$.

Вихідними даними є вектор $W(t)$, координатами якого є адаптовані ваги $w_i(t)$

$$W(t)=\|w_i\|_{1xk}, \qquad \sum_{i=1}^{k} w_i = 1, \quad \forall i=\overline{1,k} \text{ при } w_i(t)\geq 0 \tag{6}$$

Етап 4. Метою четвертого етапу є визначення інтегральної оцінки функції ризику $R_{вит}(t)$ витоку інформації в МСП, та взаємозв'язку цієї функції з ймовірністю.

Вхідними даними на цьому етапі є вектори (4) і (6). Тоді, інтегральна функція ризику витоку інформації в МПС має наступне представлення

$$R_{вит}(t)=F(t)\cdot\left[W(t)\right]^T \tag{7}$$

де $[\bullet]^T$ – операція транспонування матриці.

Очевидно, що з умов (3) і (6) випливає, що $R_{вит}(t)\in[0;1]$.

Особливістю функції (7) є те, що для кожного моменту часу t і довільного проміжку часу τ в режимі реального часу повинна виконуватись умова чутливості, яка математично має наступне представлення

$$\lim_{\tau\to 0}\frac{R_{вит}(t+\tau)-R_{вит}(t)}{f_i(t+\tau)-f_i(t)}=w_i(t) \tag{8}$$

На перший погляд представлення (8) визначає похідну функції $R_{вит}(t)$ від $f_i(t)$. Однак в реальних умовах це не зовсім так. Справа в тому, що необхідною умовою існування похідної функції є її неперервність. Однак, в реальних умовах функції (4), (6), а значить і (7) приймають дискретні значення і їх неперервне представлення, як правило, здійснюється за допомогою регресійного і коваріаційного аналізів. Але, не зважаючи на дискретну чи неперервну природу цих функцій, зв'язок між факторами ризику, ваговими коефіцієнтами і інтегральною оцінкою функції ризику повинен завжди задовольняти умові (8).

Одним з інструментів автоматизації виявлення факторів загроз в сучасних ІКС [11], включаючи МСП, є нейронні мережі. Як відомо, нейрони не реагують миттєво, а пригнічують вхідний сигнал до тих пір, поки він не досягне певного значення, яке стане імпульсом для генерації вихідного сигналу. Так як за вхідним сигналом необхідно згенерувати вихідний сигнал, то функція, яка це реалізовує є функцією активації $G_{act}(t)$. Саме ця функція визначає взаємозв'язок між ймовірністю (2) і функцією ризику (7) у вигляді рівності

$$P_{вит}(t)=G_{act}\left\{\sum_{k=1}^{\infty}\alpha_k\cdot\left[R_{вит}(t)\right]^k\right\} \tag{9}$$

В рамках досліджень в якості спрощення і наочності, здійснимо лінеарізацію функції (9) і представимо її у наступному вигляді

$$G_{act}=P_{вит}(t)\cdot G_{act}\left\{\alpha_0+\alpha_1 R_{вит}(t)\right\} \tag{10}$$

де коефіцієнти α_0 і α_1 визначаються за допомогою лінії регресії на основі спостережень інцидентів (експертні оцінки), які виникають при функціонуванні МСП.

В якості функції активації будемо розглядати S-функцію, яка має наступне представлення

$$G_{act}(t)=\frac{1}{1+e^{-\gamma\cdot t}} \tag{11}$$

де $\gamma=\alpha_0+\alpha_1 R_{вит}(t)$ – показник згладжування, який залежить від коефіцієнтів α_0 і α_1.

З представлень (10) і (11), маємо

$$P_{вит}(t) = \frac{1}{1+e^{-[\alpha_0+\alpha_1 K_{вит}(t)]\cdot t}} \quad (12)$$

Вихідними даними цього етапу є функція ризику витоку інформації (7) і ймовірність витоку інформації (12) в МПС.

Етап 5. Метою п'ятого етапу є перетворення оцінок (7) і (12) в реалізацію захисту МПС від витоку інформації.

Вхідними даними на цьому етапі є аналітичні представлення (7) і (12), критична значимість вузла x_i. Значення виразів (7) і (12) відрізняються, якщо цей вузол звичайний і якщо він містить таємні данні. Виходячи з цього, приймаються відповідні рішення.

Етап 6. Метою шостого етапу є забезпечення адаптації у часі.

Вхідними даними є результат досліджень, які були здійснені на попередньому етапі в рамках виявлення підтверджених і хибних інцидентів.

Вихідними даними цього етапу є оновлені параметри даного методу і підвищення їх точності.

На рис. 1 представлено загальну логічну схему реалізації всіх шести етапів запропонованого методу.

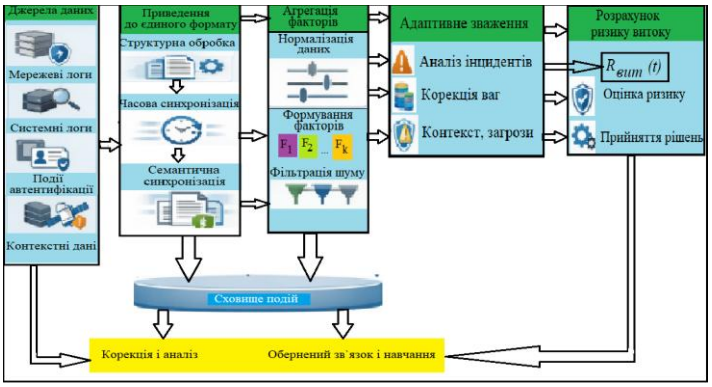

Рис. 1. Логічна схема адаптивної оцінки ймовірності витоку інформації в МСП

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Приклад практичної реалізації запропонованого методу. Наведемо приклад, який демонструє чисельні розрахунки запропонованого методу. Робоча станція оператора має доступ до чутливих файлів. Протягом спостереження вікна є ознаки несанкціонованого виводу конфіденційної інформації з МСП в зовнішнє середовище (exfiltration): масове читання файлів, архівування, зростання зовнішнього трафіку, не зрозумілі DNS-запити і вхід вночі.

Нехай поточний момент часу $t = 09:00$ тривалість спостереження у вікні складає 90 хвилин. Тоді, маємо часовий інтервал $\tau = [07:30;\ 09:00]$. Представимо алгоритм:

Етап 1. Процес збору індикаторів безпеки.

В табл. 1 представлено результат збору індикаторів.

Таблиця 1

Результати збору індикаторів

Інформація щодо мережі			
Вихідний трафік у зовнішній сегмент	Відповідь DNS-сервера, щодо не існування домену	Відповідь DNS-сервера, щодо унікальності домену	Кількість з'єднань у зовнішні сегменти
$c_1^{(м)} = 640$ Мб $c_{\min} = 0$ Мб $c_{\max} = 800$ Мб	$c_2^{(м)} = 120$ $c_{\min} = 0$ $c_{\max} = 150$	$c_3^{(м)} = 48$ $c_{\min} = 0$ $c_{\max} = 60$	$c_4^{(м)} = 210$ $c_{\min} = 0$ $c_{\max} = 300$
Інформація щодо хостів			
Кількість читань файлів з каталогу «Таємно»	Кількість копіювань на локальні часові каталоги	Обсяг створення архіву	Запис на USB (заборонено)

Продовження таблиці 1

$c_1^{(хост)} = 390$ Мб $c_{\min} = 0$ Мб $c_{\max} = 400$ Мб	95	$c_2^{(хост)} = 190$ Мб $c_{\min} = 0$ Мб $c_{\max} = 200$ Мб	0
Ідентифікаційні данні			
Час входу користувача в систему	Кількість подій перевищення привілеїв	Режим загроз	
03 : 20 $c_1^{(I)} = 1$ (приймає значення 0 або 1)	$c_2^{(I)} = 1$ $c_{\min} = 0$ $c_{\max} = 2$	$c_3^{(I)} = 0.8$ штатний показник: 0.3 підвищений показник: 0.8 високий показник: 1	

З табл. 1 виділяємо три множини: $C^{(M)} = \left\{c_1^{(м)}, c_2^{(м)}, c_3^{(м)}, c_4^{(м)}\right\}$; $C^{(хост)} = \left\{c_1^{(хост)}, c_2^{(хост)}\right\}$; $C^{(I)} = \left\{c_1^{(I)}, c_2^{(I)}, c_3^{(I)}\right\}$. Етап 1 завершено.

Етап 2. Процес перетворення елементів множин $C^{(M)}$, $C^{(хост)}$ і $C^{(I)}$ у фактори ризику $f_i(t) \in [0;1];\ i = \overline{1,k}$.

Розглянемо п'ять факторів ($k = 5$):

$f_1(t)$ – несанкціонований вивід інформації з МСП у зовнішнє середовище;

$f_2(t)$ – аномальна файлова активність;

$f_3(t)$ – несанкціонована автентифікація (витік інформації);

$f_4(t)$ – наявність скритих каналів зв'язку;

$f_5(t)$ – режим загроз.

Здійснюємо нормування елементів множин $C^{(M)}$, $C^{(хост)}$ і $C^{(хост)}$ за формулою (3):

$$C^{(M)}:\ \overline{c_1^{(м)}} = \frac{640}{800} = 0{,}8; \qquad \overline{c_2^{(м)}} = \frac{120}{150} = 0{,}8; \qquad \overline{c_3^{(м)}} = \frac{48}{60} = 0{,}8;$$

$$\overline{c_4^{(м)}} = \frac{210}{300} = 0{,}7; \qquad C^{(хост)}:\ \overline{c_1^{(хост)}} = \frac{390}{400} = 0{,}975; \qquad \overline{c_2^{(хост)}} = \frac{190}{200} = 0{,}95;$$

$$C^{(I)}:\ \overline{c_1^{(I)}} = 1; \qquad \overline{c_2^{(I)}} = \frac{1}{2} = 0.5; \qquad \overline{c_3^{(I)}} = 0.8.$$

Тепер визначимо вектор (4). В нашому прикладі $F = \left\| f_1(t); f_2(t); f_3(t); f_4(t); f_5(t) \right\|$. Маємо:

$$f_1(t) = \frac{\overline{c_1^{(м)}} + \overline{c_4^{(м)}}}{2} = 0.75; \qquad f_2(t) = \frac{\overline{c_1^{(хост)}} + \overline{c_2^{(хост)}}}{2} = 0.9625; \qquad f_3(t) = \frac{\overline{c_1^{(I)}} + \overline{c_2^{(I)}}}{2} = 0.75;$$

$$f_4(t) = \frac{\overline{c_2^{(м)}} + \overline{c_3^{(м)}}}{2} = 0.8; \qquad f_5(t) = \overline{c_3^{(I)}} = 0.8.$$

Отже, вектор факторів (4) має наступний вид $F = \left\| 0.75; 0.9625; 0.75; 0.8; 0.8 \right\|$. Етап 2 завершено.

Етап 3. Побудова змін вагових коефіцієнтів.

Нехай початкові значення ваг факторів ризику в МСП на основі експертних оцінок мали наступні значення: $w_1(t=0) = 0.25$; $w_2(t=0) = 0.25$; $w_3(t=0) = 0.2$; $w_4(t=0) = 0.15$; $w_5(t=0) = 0.15$. Перевірка:

$$\sum_{i=1}^{5} w_i(t=0) = 0.25 + 0.25 + 0.2 + 0.15 + 0.15 = 1,$$

тоді, знаменник рівності (5) прийме вид:

$$(0.25+0.75\lambda_1)+(0.25+0.9625\lambda_2)+(0.2+0.75\lambda_3)+(0.15+0.8\lambda_4)+(0.15+0.8\lambda_5)=$$
$$=0.75\lambda_1+0.9625\lambda_2+0.75\lambda_3+0.8\cdot(\lambda_4+\lambda_5)+1.$$

Тепер здійснимо оновлення ваг згідно (5). Маємо:

$$w_1(t=09:00)=\frac{0.75\lambda_1+0.25}{0.75\lambda_1+0.9625\lambda_2+0.75\lambda_3+0.8\cdot(\lambda_4+\lambda_5)+1};$$

$$w_2(t=09:00)=\frac{0.9625\lambda_2+0.25}{0.75\lambda_1+0.9625\lambda_2+0.75\lambda_3+0.8\cdot(\lambda_4+\lambda_5)+1};$$

$$w_3(t=09:00)=\frac{0.75\lambda_3+0.2}{0.75\lambda_1+0.9625\lambda_2+0.75\lambda_3+0.8\cdot(\lambda_4+\lambda_5)+1};$$

$$w_4(t=09:00)=\frac{0.8\lambda_4+0.15}{0.75\lambda_1+0.9625\lambda_2+0.75\lambda_3+0.8\cdot(\lambda_4+\lambda_5)+1};$$

$$w_5(t=09:00)=\frac{0.8\lambda_5+0.15}{0.75\lambda_1+0.9625\lambda_2+0.75\lambda_3+0.8\cdot(\lambda_4+\lambda_5)+1}.$$

Так як в ситуації, яка розглядається, режим загрози підвищений $\left(c_3^{(I)}=0.8\right)$, то ваги $w_4(t=09:00)$ і $w_5(t=09:00)$ необхідно збільшити, а ваги $w_1(t=09:00)$ і $w_2(t=09:00)$ можна зменшити, залишивши без змін лише вагу $w_3(t=09:00)$ і при цьому щоб виконувалась умова нормування $\sum_{i=1}^{5}w_i(t=09:00)=1$.

Таким чином, маємо наступну систему

$$\begin{cases} w_1(t=09:00)<0.25; \\ w_2(t=09:00)<0.25; \\ w_3(t=09:00)=0.2; \\ w_4(t=09:00)>0.15; \\ w_5(t=09:00)>0.15; \\ \sum_{i=1}^{5}w_i(t=09:00)=1. \end{cases}$$

В результаті отримаємо нові значення вагових коефіцієнтів. В нашому випадку:

$$w_1(t=09:00)=0.23; \quad w_2(t=09:00)=0.22; \quad w_3(t=09:00)=0.2;$$
$$w_4(t=09:00)=0.18; \quad w_5(t=09:00)=0.17.$$

В результаті, вектор ваг (6) має вид $W=\|0.23;0.22;0.2;0.18;0.17\|$. Етап 3 завершено.

Етап 4. Визначаємо значення інтегральної оцінки функції ризику (7). В нашому прикладі

$$W^T=\begin{Vmatrix}0.23\\0.22\\0.2\\0.18\\0.17\end{Vmatrix} \text{ і } R_{вит}=F\cdot W^T=0.81425.$$

Таким чином, $R_{вит}(t=09:00)=0.81425$. Етап 4 завершено.

Використовуючи формулу (12) обчислимо значення $P_{вит}(t=09:00)$. Згідно за результатами історії інцидентів, було встановлено, що $\alpha_0=-2$ і $\alpha_1=5$, тоді

$$P_{вит}(t = 09:00) = \frac{1}{1 + e^{-(-2+5\cdot 0.81425)}} \approx 0.89 \cdot$$

Етап 5. Прийняття рішень. В табл. 2 представлено пороги політики захисту МСП.

Таблиця 2

Пороги політики захисту МСП і отримане значення $P_{вит}$

Порогове значення	Отримане значення	Дії
$P_{вит} < 0.3$	–	Здійснюється спостереження без прийняття якихось дій
$0.3 \le P_{вит} < 0.6$	–	Здійснюється посилений моніторинг
$P_{вит} \ge 0.6$	$P_{вит} = 0.89$	Здійснюється реакція: аналіз інциденту, блокування каналу, тощо

Виходячи з даних, які представлено в табл. 2, необхідно здійснити наступні заходи: обмежити з'єднання робочої станції із зовнішнім середовищем, заблокувати запуск архіваторів на робочій станції, підсилити автоматичну реєстрацію подій функціонування МСП і ініціювати процес розслідування з боку відповідальних осіб.

Етап 6. Припустимо, що при розслідуванні виявилось, що відбувся витік інформації. Це означає, що було підтвердження факторів $f_1(t)$, $f_3(t)$ і $f_4(t)$. Задаймо значення внеску кожного з факторів $\mu_i(t)$ і відповідну йому швидкість адаптації λ_i. В табл. 3 представлено ці значення.

Таблиця 3

Нові значення вкладу факторів і відповідні швидкості адаптації

Фактор / Внесок	f_1	f_2	f_3	f_4	f_5
μ_i	0.2	0.01	0.3	0.25	0.02
λ_i	0.5	0.3	0.6	0.55	0.2

Використовуючи данні табл. 3, здійснимо оновлення ваг за формулою (5). Спочатку обчислимо знаменники формули (5) і якщо їх сума не буде дорівнювати одиниці, то здійснимо нормування. Маємо:

$$w_1^* = 0.23 + 0.2 \cdot 0.5 = 0.33; \quad w_2^* = 0.22 + 0.01 \cdot 0.3 = 0.223; \quad w_3^* = 0.2 + 0.3 \cdot 0.6 = 0.38,$$

$$w_4^* = 0.18 + 0.25 \cdot 0.55 = 0.3175; \quad w_5^* = 0.17 + 0.02 \cdot 0.2 = 0.174.$$

Здійснюємо перевірку:

$$0.33 + 0.223 + 0.38 + 0.3175 + 0.174 = 1.4245.$$

Зробивши нормування, отримаємо оновлені ваги:

$$w_1(9:00 + \tau) = \frac{0.33}{1.4245} = 0.23; \quad w_2(9:00 + \tau) = \frac{0.223}{1.4245} = 0.16;$$

$$w_4(9:00 + \tau) = \frac{0.3175}{1.4245} = 0.22; \quad w_1(9:00 + \tau) = \frac{0.174}{1.4245} = 0.12 \cdot$$

В результаті ми отримали наступну інтерпретацію: так як вага фактору f_1 не змінилась, то можна зробити висновок, що контроль щодо несанкціонованого виводу інформації з МСП у зовнішнє середовище не змінився. Так як ваговий коефіцієнт w_3 з 0.2 до 0.27, то необхідно провести аудит автентифікації користувачів і змінити паролі доступу до відповідної інформації. І, нарешті, ваговий коефіцієнт w_4 збільшився від значення 0.18 до значення 0.22, що означає наявність скритого каналу. В цьому і полягає процесадаптації – процес машинного навчання на інцидентах, які з'являються в реальному режимі часу.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В роботі вперше представлено формалізовану модель витоку інформації в МСП, що враховує сукупність технічних, програмних і поведінкових факторів. Розроблено метод адаптивної оцінки ймовірності витоку інформації в них на основі інтеграції мережевих, хостових і контекстних індикаторів безпеки. Отримані результати підтверджують перевагу адаптивних методів протидії витоку інформації в МСП над статистичними методами, які базуються на обробці емпіричних даних попередніх періодів спостереження. У функціонуванні МСП в режимі реального часу важливим є миттєва реакція на інциденти і висока швидкість адаптації в протидії їм. Тому представлені результати мають практичне значення для забезпечення захисту інформації в МСП і є підґрунтям для створення алгоритмів машинного навчання для моніторингу подій, які відбуваються в інформаційних системах, які обслуговують МСП.

В подальшому слід вдосконалювати запропонований метод шляхом використання більш складних моделей машинного навчання для автоматичного налаштування вагових коефіцієнтів факторів ризику та підвищення точності оцінювання ймовірності витоку інформації. Доцільним також буде розширення переліку індикаторів безпеки за рахунок урахування нових типів прихованих каналів, поведінкових аномалій користувачів і міжмережевих взаємодій у реальному часі. Окремим напрямом подальших досліджень є експериментальна перевірка методу на реальних наборах даних функціонування МСП та оцінювання його ефективності в умовах цілеспрямованих кібератак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges, and opportunities. *Computers & Security*, *104*, 102221. https://doi.org/10.1016/j.cose.2021.102221
2. Inayat, U., Farzan, M., Mahmood, S., Zia, M. F., Hussain, S., & Pallonetto, F. (2024). Insider threat mitigation: Systematic literature review. *Ain Shams Engineering Journal*, *15*(12), 103068. https://doi.org/10.1016/j.asej.2024.103068
3. Kamatchi, K., & Uma, E. (2025). Insights into user behavioral-based insider threat detection: Systematic review. *International Journal of Information Security*, *24*(2). https://doi.org/10.1007/s10207-025-01002-6
4. Daubner, L., Macak, M., Matulevičius, R., Buhnova, B., Maksović, S., & Pitner, T. (2023). Addressing insider attacks via forensic-ready risk management. *Journal of Information Security and Applications*, *73*, 103433. https://doi.org/10.1016/j.jisa.2023.103433
5. Mahdavifar, S., Salem, A. H., Victor, P., Razavi, A. H., Garzón, M., Hellberg, N., & Lashkari, A. H. (2021). Lightweight hybrid detection of data exfiltration using DNS based on machine learning. In *Proceedings of the 11th International Conference on Communication and Network Security (ICCNS 2021)* (pp. 80-86). https://doi.org/10.1145/3507509.3507520
6. Abualghanam, O., Alazzam, H., Elshqeirat, B., Qatawneh, M., & Almaiah, M. A. (2023). Real-time detection system for data exfiltration over DNS tunneling using machine learning. *Electronics*, *12*(6), 1467. https://doi.org/10.3390/electronics12061467
7. Zhan, M., Li, Y., Yu, G., Li, B., & Wang, W. (2022). Detecting DNS over HTTPS-based data exfiltration. *Computer Networks*, *209*, 108919. https://doi.org/10.1016/j.comnet.2022.108919
8. Le, T. D., Le-Dinh, T., & Uwizeyemungu, S. (2025). Cybersecurity analytics for the enterprise environment: A systematic literature review. *Electronics*, *14*(11), 2252. https://doi.org/10.3390/electronics14112252
9. Shuklin, H. V., & Barabash, O. V. (2018). Mathematical modeling of information security process management in the system of state regulation of stock market cybersecurity. *Control, Navigation and Communication Systems*, *4*(50). https://doi.org/10.26906/SUNZ.2018.4.091
10. Lande, D., & Danyk, Y. (2025). Dynamic detection and classification of critical attention objects under crisis events. *Theoretical and Applied Cybersecurity*, *7*(3). https://doi.org/10.20535/tacs.2664-29132025.3.347370
11. Ponochovnyi, P. M., & Pepa, Y. V. (2025). System for implementing server protection considering anomalies in packets. *Ukrainian Information Security Research Journal*, *26*(2). https://doi.org/10.18372/2410-7840.26.20018

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Herman Shuklin
Candidate of Technical Sciences, Associate Professor
Associate Professor at the Department of Software Engineering in Energy
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: 0000-0003-2507-384X
mathacadem-kiev@ukr.net

Yaroslav Shavlovskyi
Postgraduate of Department of Technical Cybersecurity Systems
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0006-2725-5996
shavlovskyyaroslav@gmail.com

Yurii Pepa
Candidate of Technical Sciences, Associate Professor
Professor at the Department of Technical Cybersecurity Systems
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-2073-1364
yurka14@ukr.net

Yevheniia Ivanchenko
Doctor of Technical Sciences, Professor
Director of the Educational and Scientific Institute of Cybersecurity and Information Protection
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-3017-5752
evivancenko@gmail.com

A METHOD FOR ADAPTIVE ESTIMATION OF THE PROBABILITY OF INFORMATION LEAKAGE IN SPECIAL-PURPOSE NETWORKS FOR MACHINE LEARNING

Abstract. This article presents a formalized model of information leakage in special-purpose networks (SPN) and develops a method for adaptive estimation of the probability of information leakage in such networks. The relevance of the research is driven by the growing number of sophisticated targeted cyber threats, the use of multi-layered attacks and covert data transmission channels, as well as the increasing role of insider threats in modern information and communication systems. It is shown that traditional protection measures, focused primarily on perimeter security, signature-based detection, and static access policies, do not provide an adequate level of protection against information leakage in the context of dynamic changes in the operating environment of SPNs. This paper proposes a formalization of the SPN as a set of nodes, information transmission channels, and risk factors that underlie the occurrence of leaks. The developed method is based on the integration of network, host, and contextual security indicators, the normalization of features, the formation of a risk factor vector, the adaptive updating of weight coefficients, and the determination of an integral risk function, followed by the calculation of the probability of information leakage. A key feature of the method is its ability to be applied in real time, taking into account changes in user behavior, network operating modes, and the current threat level. An example of the practical implementation of the proposed approach is provided, demonstrating the sequence of processing security indicators, risk assessment, and decision-making regarding incident response. The results confirm that applying the proposed method improves the effectiveness of detecting precursors to information leaks, reduces the risk of compromising confidential data, and ensures that the protection system adapts to new types of threats in the context of targeted countermeasures.

Keywords: cybersecurity; information leakage; special-purpose networks; countering leaks; threat model; adaptive risk assessment.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges, and opportunities. *Computers & Security, 104*, 102221. https://doi.org/10.1016/j.cose.2021.102221
2. Inayat, U., Farzan, M., Mahmood, S., Zia, M. F., Hussain, S., & Pallonetto, F. (2024). Insider threat mitigation: Systematic literature review. *Ain Shams Engineering Journal, 15*(12), 103068. https://doi.org/10.1016/j.asej.2024.103068
3. Kamatchi, K., & Uma, E. (2025). Insights into user behavioral-based insider threat detection: Systematic review. *International Journal of Information Security, 24*(2). https://doi.org/10.1007/s10207-025-01002-6
4. Daubner, L., Macak, M., Matulevičius, R., Buhnova, B., Maksović, S., & Pitner, T. (2023). Addressing insider attacks via forensic-ready risk management. *Journal of Information Security and Applications, 73*, 103433. https://doi.org/10.1016/j.jisa.2023.103433
5. Mahdavifar, S., Salem, A. H., Victor, P., Razavi, A. H., Garzón, M., Hellberg, N., & Lashkari, A. H. (2021). Lightweight hybrid detection of data exfiltration using DNS based on machine learning. In *Proceedings of the 11th International Conference on Communication and Network Security (ICCNS 2021)* (pp. 80-86). https://doi.org/10.1145/3507509.3507520
6. Abualghanam, O., Alazzam, H., Elshqeirat, B., Qatawneh, M., & Almaiah, M. A. (2023). Real-time detection system for data exfiltration over DNS tunneling using machine learning. *Electronics, 12*(6), 1467. https://doi.org/10.3390/electronics12061467
7. Zhan, M., Li, Y., Yu, G., Li, B., & Wang, W. (2022). Detecting DNS over HTTPS-based data exfiltration. *Computer Networks, 209*, 108919. https://doi.org/10.1016/j.comnet.2022.108919
8. Le, T. D., Le-Dinh, T., & Uwizeyemungu, S. (2025). Cybersecurity analytics for the enterprise environment: A systematic literature review. *Electronics, 14*(11), 2252. https://doi.org/10.3390/electronics14112252
9. Shuklin, H. V., & Barabash, O. V. (2018). Mathematical modeling of information security process management in the system of state regulation of stock market cybersecurity. *Control, Navigation and Communication Systems, 4*(50). https://doi.org/10.26906/SUNZ.2018.4.091
10. Lande, D., & Danyk, Y. (2025). Dynamic detection and classification of critical attention objects under crisis events. *Theoretical and Applied Cybersecurity, 7*(3). https://doi.org/10.20535/tacs.2664-29132025.3.347370
11. Ponochovnyi, P. M., & Pepa, Y. V. (2025). System for implementing server protection considering anomalies in packets. *Ukrainian Information Security Research Journal, 26*(2). https://doi.org/10.18372/2410-7840.26.20018

Отримано редакцією журналу / Received: 26.02.26
Прорецензовано / Revised: 10.03.26
Схвалено до друку / Accepted: 25.06.26