УДК 004.056.5:004.08
DOI: 10.31673/2409-7292.2025.011016

Чабан Б. В.

МОДЕЛЬ ПРОТИДІЇ ВИТОКУ ІНФОРМАЦІЇ МАТЕРІАЛЬНО-РЕЧОВИМ КАНАЛОМ

На сьогоднішній день промислове шпигунство стало основним засобом здобування інформації про нові технології та технічні рішення у сфері виробництва. Разом з тим, компанії, зазвичай, неохоче діляться інформацією про проблеми внутрішньої безпеки, що призводить до необхідності дослідження проблеми протидії витоку інформації матеріально-речовим каналом шляхом моделювання. У статті розглядається проблема протидії витоку інформації матеріально-речовим каналом шляхом побудови деталізованої моделі протидії. Стаття є продовженням попередньої публікації щодо Марківської моделі багаторівневої системи захисту організації з урахуванням задіяних ресурсів та навичок співробітників. У даній роботі запропоновано ігровий підхід до побудови аналітичного співвідношення між часом атаки та часом, протягом якого система безпеки організації може її нейтралізувати. Побудовано систему диференційних рівнянь, яка описує ймовірності перебування об'єкта інформаційної діяльності в кожному зі станів з урахуванням інтенсивностей нападу та захисту і дає можливість узагальнено визначати співвідношення між такими інтенсивностями. Здійснено оптимізацію моделі за критерієм мінімуму ймовірності успіху атаки, що викликає необхідність максимізувати інтенсивність захисту або мінімізувати інтенсивність нападу на об'єкт. Зроблено висновок щодо необхідності багатократного перевищення інтенсивності захисту над нападом з урахуванням відповідних вагових коефіцієнтів для кожної зі складових цільової функції. Окреслено напрям подальших досліджень щодо методів визначення інтенсивностей нападу та захисту для матеріально-речового каналу витоку інформації з урахуванням особливостей організації.

Ключові слова: Кібербезпека, витік інформації, технічний канал витоку інформації, матеріально-речовий канал витоку, теорія ігор, ігрова модель, оптимізація.

Вступ

Технологічний розвиток суспільства призводить до того, що промислове шпигунство стає чи не основним засобом здобування інформації. З урахуванням глобалізації інформаційно-комунікаційних технологій, воно поступово переходить у нову якість, набуваючи ознак кіберпромислового шпигунства. За даними досліджень [1] на сьогоднішній день втрати від кіберзлочинності сягають 0,8 відсотка світового ВВП, або 600 млрд. дол. на рік. У цьому процесі значною залишається частка крадіжки інформації матеріально-речовим каналом, де у якості носія інформації використовуються матеріальні речовини, вироби, елементи пристроїв, схем тощо. Протидія витоку інформації матеріально-речовим каналом традиційно є сферою відповідальності системи внутрішньої безпеки компанії, але компанії, зазвичай, неохоче діляться інформацією про проблеми внутрішньої безпеки, тому статистика та методи протидії таким атакам є вкрай обмеженими. Відтак, основним методом дослідження проблеми протидії витоку інформації матеріально-речовим каналом є моделювання [2, 3].

Загальна постановка проблеми

Зазвичай моделювання загроз витоку інформації через матеріально-речові канали ґрунтується на психологічних та поведінкових підходах, які фокусуються на аналізі особистості ймовірного порушника та прогнозуванні можливих випадків компрометації даних. Однак подібні моделі не дозволяють визначити, яким чином слід організовувати ефективну систему захисту від витоків через матеріально-речові канали. Вони не враховують особливості взаємодії потенційного зловмисника із системою безпеки підприємства. Витік даних через матеріально-речові канали є динамічним процесом, що розгортається за певними закономірностями. Тому важливим напрямом дослідження є вивчення змін параметрів системи "організація – зловмисник" у часовому вимірі. Також, логічно припустити, що заходи інформаційної безпеки мають випереджати дії потенційного зловмисника, забезпечуючи проактивний захист.

Аналіз публікацій

Побудові науково-методичного апарату дослідження технічних каналів витоку інформації присвячено багато публікацій як в Україні, так і за кордоном. Так, у [4] було

проведено аналіз різних підходів до визначення сутності терміну “витік інформації” та здійснена класифікація технічних каналів витоку інформації. Вивчено сутність процесу формування технічних каналів витоку інформації та висвітлено різноманітні методи захисту інформації від такого витоку. Більш глибоко процеси утворення технічних каналів витоку інформації досліджуються у [5]. У роботі здійснено аналіз особливостей фізичного середовища поширення інформаційних сигналів, а також здійснено детальний аналіз фізичних процесів, які лежать в основі функціонування різноманітних технічних каналів витоку конфіденційної інформації.

У [6] розроблено унікальну методику оптимізації кількості засобів блокування каналів витоку інформації на основі поєднання кроків: аналізу особливостей об’єкта інформаційної діяльності та розроблення моделі загроз; розроблення моделі комплексу технічного захисту інформації від витоку технічними каналами; оцінювання характеристик систем постановки завад і розрахунку їх оптимальної кількості. У статті [7] запропоновано складові частини кількісної моделі технічного каналу витоку інформації, що дозволяють проводити врахування факторів, які впливають на співвідношення сигнал/шум сигналу, що сприймається апаратурою розвідки.

Достатньо глибокий аналіз підходів щодо моделювання загроз витоку інформації технічними каналами наведено у [8]. Зокрема, розглянуто сигнатурні, статистичні методи, приховані марковські моделі, метод опорних векторів, сплайни багатовимірної адаптивної регресії, методи кластеризації, байєсовські мережі. Також, розглядаються методи природних обчислень, такі як штучні нейронні та імунні мережі, генетичні алгоритми, методи нечіткої логіки, експертні системи, теорія графів та теорія фракталів, теорія ігор. Автори показують, що кожен з розглянутих методів має свої переваги та недоліки і на теперішній час ще не розроблено ідеальної системи протидії вторгненням, яка б не вимагала вдосконалень, тому розробка та пошук ефективних математичних методів триває.

Значна кількість моделей, які пов’язують часові та ймовірнісні параметри, базується на Марківських підходах. Аналіз таких підходів та розробка власного методу були нами запропоновані у [9]. У статті було визначено співвідношення між часом атаки та часом її нейтралізації. Крім того, було досліджено концепцію багаторівневої системи захисту організації з урахуванням задіяних ресурсів та навичок співробітників. Наприкінці статті зроблено висновок про ефективність запропонованої концепції системи захисту організації від витоку інформації матеріально-речовим каналом.

Моделювання системи “організація – зловмисник” може здійснюватися на основі різних підходів, хоча насправді зміст моделі зводиться до взаємодії двох акторів: нападника та захисту. Таким чином, в основу дослідження можна покласти ігрові підходи, які започатковані зокрема у [10]. Як і раніше, нас цікавить аналітичне співвідношення між часом атаки та часом, протягом якого система безпеки організації може її нейтралізувати.

Метою даної статті є подальше удосконалення моделі взаємодії “організація – зловмисник” з визначенням оптимального співвідношення інтенсивностей захисту та нападу з урахуванням вартості гри.

Модель протидії витоку інформації матеріально-речовим каналом

Загальна модель, запропонована нами в [9], вводить співвідношення між швидкістю нападу на об’єкт інформаційної діяльності (ОІД) та швидкістю реагування захисту ОІД при намаганні зловмисника заволодіти матеріальним носієм інформації (МНІ). В той же час, абстракція цієї моделі не дає можливості досліджувати особливості утворення матеріально-речового каналу витоку інформації: структуру самого ОІД, та структуру системи його охорони, які визначають оптимальні показники системи захисту. Для більш детального розгляду доцільно розглянути ОІД у складі: 1) система контролю та управління доступом (СКУД); 2) служба безпеки та охорони організації (СБО); 3) сховище МНІ; 4) комплекс засобів обробки інформації (КЗОІ).

© Чабан Б. В. (2025). Модель протидії витоку інформації матеріально-речовим каналом. Сучасний захист інформації, 1(61), 277–284.
https://doi.org/10.31673/2409-7292.2025.011016.

Припустимо, що у поточний момент часу ОІД перебуває в одному з типових станів, які позначимо:

S_0 – робота ОІД у штатному режимі (S_1 – штатне функціонування СКУД; S_2 – безперервний зв'язок з СБО; S_3 – штатна робота сховища МНІ; S_4 – надійна робота КЗОІ);

F_0 – витік інформації матеріально-речовим каналом (F_1 – відмова СКУД; F_2 – відмова зв'язку з СБО; F_3 – компрометація сховища МНІ; F_4 – порушення нормальної роботи КЗОІ).

Під час атаки ОІД змінює свої стани з відповідними ймовірностями протягом деякого часу *T*, що дорівнює тривалості інтервалу нападу на ОІД $t \in [0,T]$. На рис. 1 наведено модель процесу нападу-захисту ОІД.

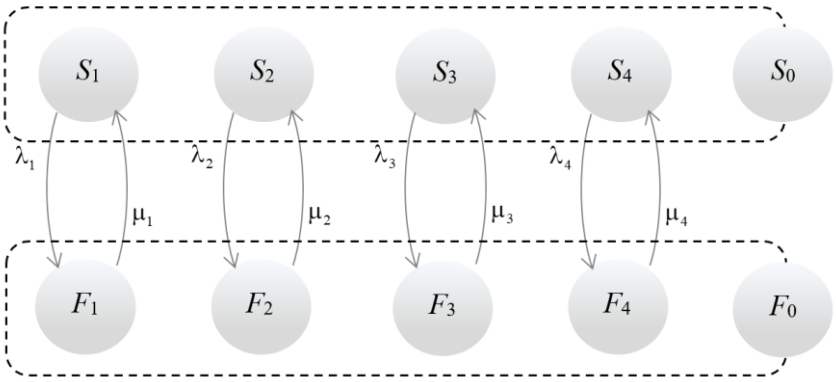


Рис. 1. Модель процесу нападу-захисту ОІД

У вузлах графа вказано стани елементів ОІД, а над стрілками переходів зі стану в стан наведено інтенсивності потоків нападу λ_i та захисту μ_j. Нормальна та безвідмовна робота ОІД S_0 передбачає повну функціональність ОІД – одночасне перебування системи в станах $S_1 ... S_4$, які будемо вважати незалежними. Компрометація ОІД F_0, за будь-якою зі складових, відповідно, є подією, що настає при виникненні хоча б однієї з незалежних відмов $F_1 ... F_4$. Таким чином, ймовірності станів S_0 та F_0 можна подати як:

$$\begin{cases} P_{S_0}(t) = \prod_{i=1}^{4} P_{S_i}(t); \\ P_{F_0}(t) = 1 - \prod_{i=1}^{4} \left(1 - P_{F_i}(t)\right). \end{cases} \tag{1}$$

Система диференціальних рівнянь щодо *i*-ї функціональності ОІД буде мати вигляд:

$$\begin{cases} \dfrac{dP_{S_i}(t)}{dt} = -\lambda_i P_{S_i}(t) + \mu_i P_{F_i}(t); \\ \dfrac{dP_{F_i}(t)}{dt} = \lambda_i P_{F_i}(t) - \mu_i P_{F_i}(t); \end{cases} \quad i = \overline{1,4}. \tag{2}$$

Ймовірності станів ОІД утворюють повну групу подій і тому до системи (2) необхідно застосувати умову нормування:

© Чабан Б. В. (2025). Модель протидії витоку інформації матеріально-речовим каналом. Сучасний захист інформації, 1(61), 277–284.
https://doi.org/10.31673/2409-7292.2025.011016.

$$P_{S_i}(t)+P_{F_i}(t)=1,\ \ i=\overline{1,4}. \tag{3}$$

Процеси нападу та захисту на ОІД слід доповнити (2) рівняннями (1) та (3), в результаті чого можна сформувати математичну модель процесу витоку інформації матеріально-речовим каналом:

$$\begin{cases} \dfrac{dP_{S_i}(t)}{dt}=-\lambda_i P_{S_i}(t)+\mu_i P_{F_i}(t); \\ \dfrac{dP_{F_i}(t)}{dt}=\lambda_i P_{F_i}(t)-\mu_i P_{F_i}(t); \\ P_{S_0}(t)=\prod\limits_{i=1}^{4} P_{S_i}(t); \\ P_{F_0}(t)=1-\prod\limits_{i=1}^{4}\left(1-P_{F_i}(t)\right); \\ P_{S_i}(t)=1-P_{F_i}(t); \\ i=\overline{1,4}. \end{cases} \tag{4}$$

Для системи (4) визначимо також початкові умови:

$$\begin{cases} P_{S_i}(0)=1; \\ P_{F_i}(0)=0; \\ P_{S_0}(0)=\prod\limits_{i=1}^{4} P_{S_i}(0); \\ P_{F_0}(0)=1-\prod\limits_{i=1}^{4}\left(1-P_{F_i}(0)\right). \end{cases} \tag{5}$$

Система рівнянь (4) описує ймовірності перебування ОІД в кожному стані під час нападу з урахуванням інтенсивностей нападу та захисту. Припустивши, що стратегії обох сторін λ_i та μ_i є постійними величинами, динаміка зміни основних ймовірностей може бути описана, як на рис. 2.

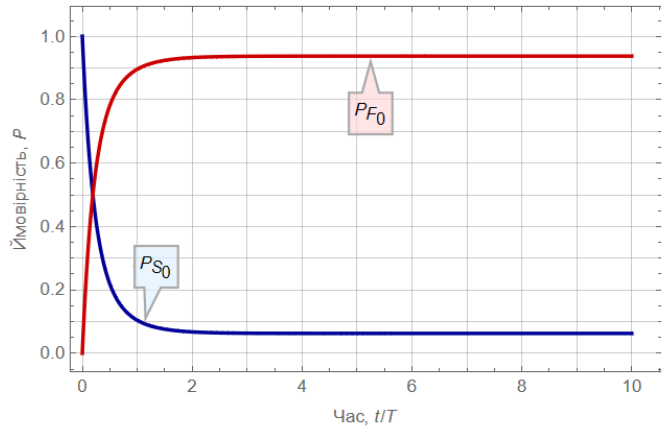


Рис. 2. Динаміка моделі нападу-захисту ОІД

Ймовірності стаціонарного стану системи (4) можуть бути знайдені з умови:

$$\frac{dP_{S_i}(t)}{dt} = \frac{dP_{F_i}(t)}{dt} = 0. \tag{6}$$

Якщо розв'язати систему рівнянь

$$\begin{cases} -\lambda_i P_{S_i} + \mu_i P_{F_i} = 0; \\ \lambda_i P_{S_i} - \mu_i P_{F_i} = 0; \\ P_{S_i} + P_{F_i} = 1; \\ P_{S_0} = P_{S_i}^4; \\ P_{F_0} = 1 - \left(1 - P_{F_i}\right)^4, \end{cases} \tag{7}$$

відносно P_{S_i}, P_{F_i}, P_{S_0}, P_{F_0}, то можна отримати:

$$P_{S_i} = \frac{\mu_i}{\lambda_i + \mu_i};\ P_{F_i} = \frac{\lambda_i}{\lambda_i + \mu_i};\ P_{S_0} = \frac{\mu_i^4}{\left(\lambda_i + \mu_i\right)^4};\ P_{F_0} = \frac{\lambda_i\left(\lambda_i^3 + 4\lambda_i^2\mu_i + 6\lambda_i\mu_i^2 + 4\mu_i^3\right)}{\left(\lambda_i + \mu_i\right)^4}. \tag{8}$$

Якщо у якості основного критерію обрати ймовірність успіху атаки P_{F_0}, яка залежить від λ_i та μ_i, то стає очевидно, що для мінімізації P_{F_0} необхідно максимізувати μ_i або мінімізувати λ_i. Зважаючи на те, що ресурси організації завжди обмежені, для пошуку оптимального співвідношення λ_i та μ_i цільову функцію можна визначити у вигляді

$$F = w_1 P_{F_0} + w_2 C_\mu + w_3 C_\lambda, \tag{9}$$

де: w_1, w_2, w_3 – вагові коефіцієнти ймовірності компрометації, витрат на захист та витрат на напад відповідно;

C_μ – вартість заходів захисту, пропорційна μ_i;

C_λ – вартість атаки, пропорційна λ_i.

Вагові коефіцієнти w_1, w_2, w_3 визначають пріоритетність компонентів цільової функції. При цьому їх абсолютні значення не впливають на математичну розв'язуваність задачі, якщо кожна компонента виражена в узгоджених одиницях вимірювання. Важливо лише щоб вагові коефіцієнти зберігали пропорційність між собою.

Підставивши P_{F_0} з (8) у (9) та з урахуванням пропорційності $C_\mu \sim \mu_i$ та $C_\lambda \sim \lambda_i$ отримаємо вираз для цільової функції:

$$F = w_1 \frac{\lambda_i\left(\lambda_i^3 + 4\lambda_i^2\mu_i + 6\lambda_i\mu_i^2 + 4\mu_i^3\right)}{\left(\lambda_i + \mu_i\right)^4} + w_2\mu_i + w_3\lambda_i, i = \overline{1,4}. \tag{10}$$

https://doi.org/10.31673/2409-7292.2025.011016.

Взявши окремі похідні функції (10) та прирівнявши їх до нуля ($\frac{\partial F}{\partial \lambda_i}=0$ та $\frac{\partial F}{\partial \mu_i}=0$) отримаємо вирази для визначення оптимальних значень інтенсивностей:

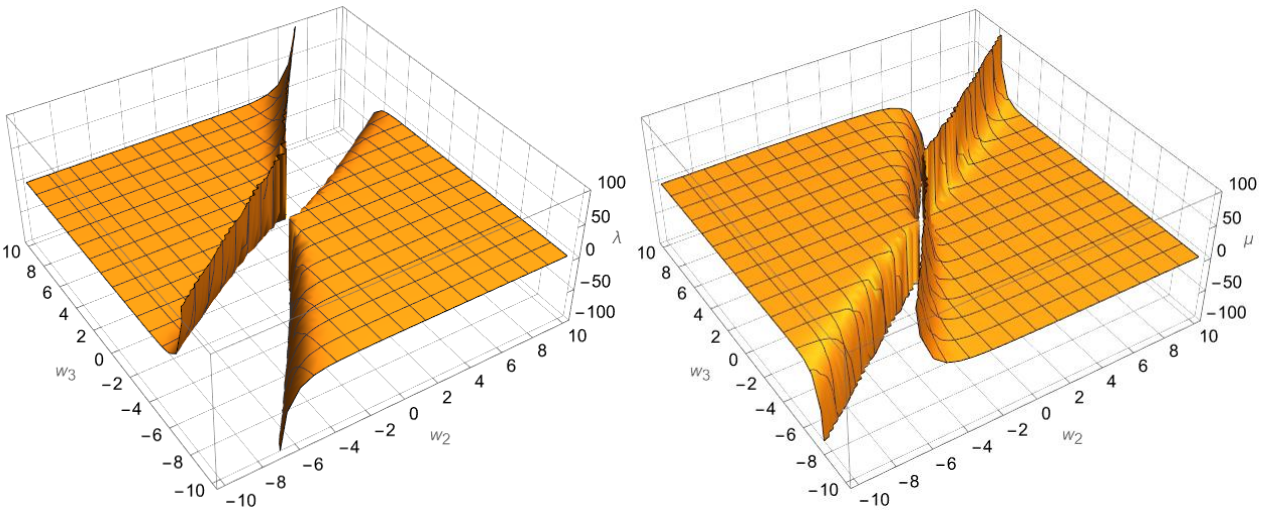
$$\lambda_{\text{Опт}}=-\frac{4w_1w_2w_3^3}{\left(w_2-w_3\right)^5};\ \mu_{\text{Опт}}=-\frac{4w_1w_3^4}{\left(-w_2+w_3\right)^5}. \tag{11}$$

Для виразів (11) важливим елементом є необхідність врахування області визначення. Задавши $w_1=1$, отримуємо:

$$\left(w_2\geq 0\right)\wedge\left\{\left(w_3<-w_2\right)\vee\left(-w_2<w_3<0\right)\right\}. \tag{12}$$

Як бачимо, w_2 лежить в області додатних значень, в той час, як w_3 перебуває в області від'ємних. Така позиція вагових коефіцієнтів вказує на те, що в цільовій функції (10) вони діють по різному. При загальній стратегії $F\to\min$, $w_2\geq 0$ означає, що нам необхідно мінімізувати витрати на захист, а $w_2<0$ – максимізацію витрат зловмисника на напад.

Графічно області визначення w_2, w_3 відносно λ_i та μ_i можуть бути зображені, як вказано на рис. 3.



а) б)

Рис. 3. Область визначення: а) λ_i; б) μ_i

Для перевірки оптимальності (11) оберемо у якості вагових коефіцієнтів $w_1=1$, $w_2=1$ і $w_3=-5$. Вибір саме таких значень w_2 і w_3 обгрунтуємо тим, що нам набагато важливіше примусити зловмисника рахуватися з витратами, аніж рахувати власні витрати чи зважати на ймовірність успіху атаки.

Підставивши ці значення у (11), отримаємо:

$$\lambda_{\text{Опт}}=0.064;\ \mu_{\text{Опт}}=0.321;\ F=0.518;\ P_1=0.51. \tag{13}$$

© Чабан Б. В. (2025). Модель протидії витоку інформації матеріально-речовим каналом. Сучасний захист інформації, 1(61), 277–284.
https://doi.org/10.31673/2409-7292.2025.011016.

Співвідношення $\frac{\mu_{\text{Опт}}}{\lambda_{\text{Опт}}} = \frac{0.321}{0.064} = 5.02$, що означає необхідність п’ятикратного перевищення інтенсивності захисту над інтенсивністю нападу. Заради справедливості необхідно сказати, що це співвідношення буде пропорційним співвідношенню $\frac{w_2}{w_3}$, яке встановлюється самим дослідником при формуванні цільової функції (10). Разом з тим, навіть при такому перевищенні захисту над нападом, як бачимо, ймовірність успіху атаки P_1=0.51 є достатньо високою.

Загальний вигляд цільової функції наведено на рис. 4.

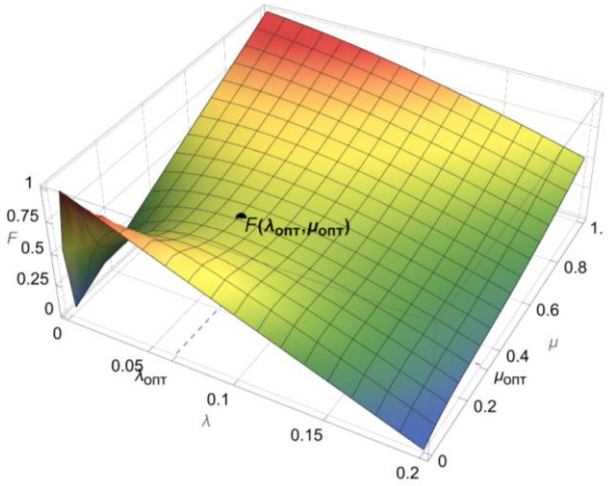


Рис. 4. Загальний вигляд цільової функції (10)
при $w_1 = 1,\ w_2 = 1,\ w_3 = -5$

Як бачимо, функція досягає свого оптимального значення в сідловій точці

$$\max_{\lambda_i} \min_{\mu_j} F\left(t, P_{F_0}(t), \lambda_i, \mu_j\right). \tag{14}$$

При цьому необхідно враховувати також обмеження на ресурси нападу та захисту:

$$\begin{cases} \lambda_{i\min} \le \lambda_i \le \lambda_{i\max}; \\ \mu_{j\min} \le \mu_j \le \mu_{j\max}, \end{cases} \tag{15}$$

де $\lambda_{i\min}$, $\mu_{j\min}$ та $\lambda_{i\max}$, $\mu_{j\max}$ – мінімальні та максимальні значення інтенсивностей потоків нападу та захисту. Тобто, ресурси як захисту так і нападу завжди обмежені і сторони будуть намагатися максимізувати витрати супротивника при мінімізації власних витрат.

Запропонована модель протидії витоку інформації матеріально-речовим каналом базується на ігровому підході, що дозволяє аналітично оцінювати співвідношення між часом атаки та можливостями системи безпеки щодо її нейтралізації. Використання системи диференційних рівнянь для опису ймовірностей перебування об’єкта в різних станах дозволяє не лише прогнозувати розвиток загрози в реальному часі, а й визначати оптимальні параметри реагування. Порівняльний аналіз показує, що традиційні підходи, засновані виключно на статичних моделях ризиків, не забезпечують достатньої гнучкості для адаптації до змінних умов загрози, тоді як запропонована модель дозволяє оперативно коригувати стратегію

© Чабан Б. В. (2025). Модель протидії витоку інформації матеріально-речовим каналом. Сучасний захист інформації, 1(61), 277–284.
https://doi.org/10.31673/2409-7292.2025.011016.

захисту. Оптимізація моделі за критерієм мінімізації ймовірності успіху атаки підтвердила необхідність багатократного перевищення інтенсивності захисту над інтенсивністю нападу. Визначення відповідних вагових коефіцієнтів для різних компонентів цільової функції дозволяє гнучко адаптувати модель під специфічні умови кожної організації. Це, своєю чергою, дає змогу більш ефективно розподіляти ресурси, підвищуючи загальну ефективність системи безпеки без надмірного збільшення витрат. Практичне застосування моделі продемонструвало, що її використання дозволяє суттєво знизити ризики витоку інформації, навіть за наявності активних атакувальних дій з боку зловмисників..

Висновки

Моделювання матеріально-речового каналу витоку інформації викликає низку труднощів через складність формалізації окремих процесів, які складають тактики та процедури нападу і відповідні їм технології захисту. Існуючі підходи мають свої переваги та недоліки і на теперішній час ще не розроблено ідеальної моделі системи протидії витоку матеріально-речовим каналом. Система диференційних рівнянь, яка описує ймовірності перебування об’єкта інформаційної діяльності в кожному зі станів з урахуванням інтенсивностей нападу та захисту дає можливість узагальнено визначати співвідношення між такими інтенсивностями. Оптимізація моделі за критерієм мінімуму ймовірності успіху атаки викликає необхідність максимізувати інтенсивність захисту або мінімізувати інтенсивність нападу на об’єкт. Введення відповідних вагових коефіцієнтів для кожної зі складових цільової функції призводить до висновку щодо багатократного перевищення інтенсивності захисту над нападом. Напрямом подальших досліджень може бути широке коло питань щодо методів визначення інтенсивностей нападу та захисту для матеріально-речового каналу витоку інформації з урахуванням особливостей організації.

Перелік посилань

1. Корнілова, І. (2024). Кіберпромислове шпигунство: сутність та наслідки. Економічний простір, (190), 248-253. https://doi.org/10.32782/2224-6282/190-45

2. Котенко, А. М. (2017) Запобігання витоку інформації з обмеженим доступом матеріально-речовим каналом за рахунок використання систем відеоспостереження. Сучасний захист інформації, № 1. 48–52. https://journals.dut.edu.ua/index.php/dataprotect/article/view/1411/1344

3. Іванченко, С. О., Гавриленко, О. В., Липський, О. А., Шевцов, А. С. (2016). Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. К.: КПІ. 104 с. https://ela.kpi.ua/server/api/core/bitstreams/930d9270-2cb1-4c62-a4ce-ab5404d9b90f/content

4. Horlichenko, S. (2023). Peculiarities of the formation of technical channels of information leakage from modern x-rays // Ukrainian Scientific Journal of Information Security. vol. 29, issue 2, pp. 80-87. https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/17872/25175

5. Попович, Н. І. (2015). Фізичні основи утворення технічних каналів витоку інформації. Науковий вісник Ужгородського університету: серія: Фізика. Вип. 37, 154–160. https://dspace.uzhnu.edu.ua/jspui/handle/lib/15861

6. Гуменюк, І., Костерев, Д., Шейгас, В. (2025). Методика оптимізації кількості засобів блокування каналів витоку акустичної інформації на об'єкті інформаційної діяльності. Ukrainian Scientific Journal of Information Security. 30. 289-296. https://doi.org/10.18372/2225-5036.30.19241

7. Воронов, В., Заболотний, В., & Лиско, В. (2020). Accounting for the interference component in the technical channel of information leakage of spurious electromagnetic radiation in the video path with diversity reception. Radiotekhnika, 3(202), 99–105. https://doi.org/10.30837/rt.2020.3.202.10

8. Лисенко, Н. О., Мазуренко, В. Б., Федоровіч, А. І., Астахов, Д. С., Стаценко, В. І. (2021). Огляд математичних методів у системах виявлення та попередження кіберзагроз. Актуальні проблеми автоматизації та інформаційних технологій. Том 25. 91–102. https://doi.org/10.15421/432110

9. Чабан, Б. В., & Котенко, А. М. (2024). Модель системи захисту інформації від витоку матеріально-речовим каналом на базі ланцюгів Маркова. Сучасний захист інформації, 4(60), 46–52. https://doi.org/10.31673/2409-7292.2024.040005

10. Voronko, I. (2021). Differential-Game Model of Information Protection for Computer Systems of Transport Infrastructure. Transport Systems and Technologies, (38), 201–212. https://doi.org/10.32703/2617-9040-2021-38-198-19

Надійшла 25.02.2025