УДК 004.056.5:004.08 DOI 10.31673/2412-4338.2025.022437

Чабан Богдан Валентинович
Державний університет інформаційно-комунікаційних технологій, м. Київ
ORCID 0009-0004-8815-7295

МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ МАТЕРІАЛЬНО-РЕЧОВИМ КАНАЛОМ ІЗ ЗАДАНИМИ ПАРАМЕТРАМИ ЗАХИЩЕНОСТІ

Анотація: *У статті досліджено проблему витоку інформації матеріально-речовим каналом. Такі загрози можуть виникати внаслідок навмисних дій зловмисників або ненавмисних витоків, пов'язаних із людським фактором, технічними особливостями носіїв інформації та недосконалістю організаційних заходів безпеки. Показано, що дослідженню матеріально-речового каналу витоку інформації у світовій науковій літературі присвячено не надто багато публікацій. Існуючі методи побудови ефективних систем захисту мають бути адаптовані шляхом визначення припустимих параметрів кількості спроб проникнення зловмисника на об'єкт інформаційної діяльності та припустимого часу, який може бути відведено на таке проникнення. У статті обгрунтувано теоретичні основи побудови системи захисту інформації від витоку матеріально речовим каналом. Автором запропоновано метод захисту інформації від витоку матеріально-речовим каналом із заданими параметрами захищеності, який враховує кількість припустимих спроб проникнення та час, який необхідно витратити зловмиснику для проникнення на об'єкт для заволодіння зразком технологій чи документом. У розробленій моделі збільшення параметра захищеності об'єкта призводить до зниження ймовірності проникнення. Метод базується на визначенні лінії ймовірності проникнення і дозволяє не тільки проектувати ефективні системи захисту, але й керувати самим процесом проникнення за збігом чи відхиленням інцидентів безпеки, що відбулися, від лінії проникнення. Моделювання такого підходу дозволяє передбачити, в якому напрямку йде проектований процес проникнення на об'єкт, та здійснювати його аналіз. Зроблено висновок про те, що подальші дослідження щодо побудови ефективних систем захисту інформації від витоку матеріально-речовим каналом можуть бути зосереджені на методах визначення ймовірностей проникнення та показників захищеності систем захисту з урахуванням особливостей конкретних організацій.*

Ключові слова*: кібербезпека, захист інформації, витік інформації, технічний канал витоку інформації, матеріально-речовий канал витоку інформації, ймовірність проникнення.*

Chaban Bohdan
State University of Information and Communication Technologies, Kyiv
ORCID 0009-0004-8815-7295

METHOD FOR PROTECTING INFORMATION FROM LEAKAGE THROUGH PHYSICAL CHANNELS WITH SPECIFIED SECURITY PARAMETERS

Abstract: *The article studies the problem of information leakage through the material channel. Such threats can arise as a result of intentional actions of attackers or unintentional leaks associated with the human factor, technical features of information carriers and imperfection of organizational security measures. It is shown that not too many publications are devoted to the study of the material channel of information leakage in the world scientific literature. Existing methods for building effective protection systems should be adapted by determining the permissible parameters of the number of attempts by an attacker to penetrate the object of information activity and the permissible time that can be allocated for such penetration. The article substantiates the theoretical foundations of building a system for protecting information from leakage through the material channel. The author proposes a method for protecting information from leakage through the material channel with specified security parameters, which takes into account the number of permissible penetration attempts and the time that an attacker needs to spend to penetrate the object to seize a technology sample or document. In the developed model, increasing the security parameter of the object leads to a decrease in the probability of penetration. The method is based on determining the line of probability of penetration and allows not only to design effective protection systems, but also to control the penetration*

process itself by the coincidence or deviation of the security incidents that have occurred from the line of penetration. Modeling such an approach allows you to predict the direction in which the designed process of penetration into the object is going, and to analyze it. It is concluded that further research on the construction of effective information protection systems against leakage through a material channel can be focused on methods for determining the probabilities of penetration and indicators of the security of protection systems, taking into account the characteristics of specific organizations.

Keywords: *cybersecurity, information protection, information leakage, technical information leakage channel, material information leakage channel, probability of penetration.*

1. Вступ

В умовах зростаючої кількості загроз інформаційній безпеці особливо актуальною є проблема захисту інформації від витоку через матеріально-речові канали. Такі загрози можуть виникати внаслідок навмисних дій зловмисників або ненавмисних витоків, пов'язаних із людським фактором, технічними особливостями носіїв інформації та недосконалістю організаційних заходів безпеки. Більшість традиційних підходів до забезпечення інформаційної безпеки зосереджені на цифрових загрозах, що створює прогалину в дослідженні методів протидії витоку даних через матеріальні (фізичні) носії інформації. Розробка методу захисту з урахуванням заданих параметрів захищеності дозволить створити ефективну систему безпеки, адаптовану до конкретних умов функціонування організації [1].

2. Аналіз літературних даних і постановка проблеми

Дослідженню матеріально-речового каналу витоку інформації у світовій науковій літературі присвячено не надто багато публікацій. До більш визначних слід віднести роботу [2], де розглядаються методи адміністрування фізичного доступу в складних середовищах на основі використання тривимірних інформаційних моделей будівель та алгоритмів пошуку шляху проникнення. У статті [3] автори описують основний набір функцій, які повинна мати система контролю фізичного доступу, у формі шаблонів, що полегшує проєктувальникам можливість створення ефективних систем контролю доступу. В публікації [4] автори характеризують системи фізичного доступу через моделі фізичного простору та різні рівні політик, а також процеси удосконалення та реалізації політик. У статті [5] автор досліджує існуючі технічні канали витоку інформації з об'єктів інформаційної діяльності (ОІД), джерела та причини витоку інформації матеріально-речовим каналом, акцентуючи увагу на системах відеоконтролю. Публікація [6] досліджує проблему протидії витоку інформації матеріально-речовим каналом шляхом створення збалансованої за часом системи безпеки в організації. Автори пропонують базову модель взаємодії в системі "організація – зловмисник" на основі ланцюга Маркова з дискретними станами та неперервним часом. У статті аналітично визначено співвідношення між часом атаки та часом, протягом якого система безпеки організації може її нейтралізувати.

Декілька публікацій присвячені побудові оптимальних систем технічного захисту інформації. Так, у [7] отримана функція технічного захисту, що залежить від параметрів напрямку процесу злому і визначає ймовірнісну надійність технічного захисту в напрямку злому. З функції напряму процесу злому отримано вираз взаємної залежності спроб та часу злому захисту. У [8] авторами пропонується метод розрахунку ймовірності злому технічного захисту інформації у часі. Цей вираз підпорядковується закону геометричного розподілу ймовірностей, дозволяє враховувати статистичні чи сертифікаційні дані у дослідженнях із захищеності інформації. У статті [9] наведено математичну модель процесу злому технічного захисту інформації з урахуванням інвестицій у захист інформації, коефіцієнта ефективності захисту і напрямку злому на основі розподілу Пуассона. Публікація [10] висвітлює результати досліджень фізичного процесу злому для послідовного дворівневого захисту інформації з ймовірнісною надійністю. В роботі запропоновано спосіб визначення ймовірності злому дворівневої системи захисту що дає можливість визначати реальну надійність системи захисту для будь-якого напрямку злому.

Не зважаючи на перспективність розглянутих підходів, вони мають бути адаптовані для використання у системах захисту, пов'язаних з матеріально-речовим каналом витоку

інформації. Зокрема, потребують визначення припустимі параметри кількості спроб проникнення зловмисника на об'єкт інформаційної діяльності та припустимий час, який може бути відведено на таке проникнення.

3. Мета і задачі дослідження

Метою статті є розробка методу проектування системи захисту інформації на об'єкті інформаційної діяльності із заданими припустимими параметрами проникнення в системі протидії витоку інформації матеріально-речовим каналом.

Для досягнення поставленої мети потребують вирішення такі завдання:

– обгрунтування теоретичних основ побудови системи захисту інформації від витоку матеріально речовим каналом;

– моделювання залежностей заданих параметрів захищеності ОІД;

– розробка алгоритму проектування системи захисту інформації від витоку матеріально-речовим каналом**.**

4. Теоретичні основи побудови системи захисту інформації від витоку матеріально-речовим каналом.

Як було показано у [7 – 10] ключовими параметрами для створення ефективної системи захисту інформації (СЗІ) можуть бути: 1) кількість спроб проникнення, і 2) час, який необхідно витратити зловмиснику для проникнення на ОІД. При цьому ймовірність захищеності ОІД $p_0(t)$ та ймовірність проникнення на ОІД $p(t)$ у часі можуть бути описані виразами:

$$p_0(t)=\frac{f(t)}{f(t)+t},\ p(t)=\frac{t}{f(t)+t}, \tag{1}$$

де: t – поточний час; $f(t)$ – довільна функція, що залежить від часу і має розмірність часу (математичне очікування захищеності ОІД).

Якщо обрати, що ймовірність проникнення на ОІД не залежить від результатів попередніх спроб, то, вважатимемо, що ймовірність проникнення залишається сталою. Такий розподіл спроб проникнення на ОІД підпорядковуватиметься геометричному закону [8], і тому ймовірність події проникнення на m-й спробі може бути записана як:

$$P_m(t)=\left[p_0(t)\right]^{m-1}\cdot p(t)=\left[\frac{f(t)}{f(t)+t}\right]^{m-1}\cdot\frac{t}{f(t)+t}. \tag{2}$$

Щоб відшукати розподіл максимумів ймовірностей проникнення $P_m(t)$ визначимо ймовірність m-ї спроби проникнення у часі, прирівнявши нулю першу похідну виразу (2):

$$\frac{\partial P_m(t)}{\partial t}=\left[f(t)+t\cdot(m-1)\cdot\frac{\partial f(t)}{\partial t}-t\cdot m\cdot\frac{f(t)}{f(t)+t}\cdot\left(\frac{\partial f(t)}{\partial t}+1\right)\right]\times\frac{f^{m-2}(t)}{\left(f(t)+t\right)^m}=0. \tag{3}$$

Вираз $\frac{f^{m-2}(t)}{\left(f(t)+t\right)^m}\neq 0$, тому що $f(t)>0$ і $t\geq 0$. Скоротивши на цей вираз і прирівнявши нулю значення квадратних дужках в рівнянні (3), після перетворень отримаємо

$$f(t)-t\cdot m\cdot\frac{f(t)}{f(t)+t}=\left[t\cdot m\cdot\frac{f(t)}{f(t)+t}-t\cdot(m-1)\right]\cdot\frac{\partial f(t)}{\partial t}, \tag{4}$$

$$f(t)\cdot\left[f(t)-(m-1)\cdot t\right]=t\cdot\left[f(t)-(m-1)\cdot t\right]\cdot\frac{\partial f(t)}{\partial t}. \tag{5}$$

З (5) знайдемо одне з його рішень, прирівнявши нулю вираз у квадратних дужках:

$$f(t)=(m-1)\cdot t. \tag{6}$$

Друге рішення (5) можна знайти, скоротивши обидві частини на вираз в дужках

$$\frac{\partial f(t)}{\partial t}=\frac{f(t)}{t},\ \text{або}\ \frac{\partial f(t)}{f(t)}=\frac{\partial t}{t}. \tag{7}$$

Інтегруючи а потім потенціюючи вираз (7) можна отримати друге рішення рівняння (5):

$$lg\left[f(t)\right] = lg\left[t\right] + const, \tag{8}$$

$$f(t) = t \cdot const. \tag{9}$$

З (9) і (6) слідує, що вони будуть рівними при $m-1 = const$. Вираз (6) визначає зв'язок між спробами проникнення *m* і часом цієї спроби *t*. Друга похідна розподілу ймовірностей проникнення (2) за часом дає максимум у точці, що визначається виразом (6). Щільність ймовірності проникнення на *m*-й спробі у часі може бути записана як

$$P_m(t) = \left[\left(\frac{f(t)}{f(t)+t}\right)^{m-1} \cdot \left(\frac{t}{f(t)+t}\right)\right]^{\gamma}, \tag{10}$$

де $f(t)$ – параметр, який визначає захисні властивості СЗІ; *t* – поточна координата часу; *m* – поточна спроба проникнення на ОІД; γ – ефективність проектованого захисту.

Залежність $P_m(t)$ наведено на рис. 1, з якого видно, що збільшення $\gamma \to 1$ призводить до зниження $P_m(t) \to 0$. Як було зазначено у [11], якщо проникнення на цьому чи інших аналогічних об'єктах відбулося, то завжди $\gamma < 1$. При $\gamma = 1$ проникнення можливе лише при $m \to \infty$, а при $\gamma > 1$ проникнення взагалі неможливе і захищеність ОІД гарантується.

Максимум ймовірності проникнення в часі може бути отриманий з рівняння (10) шляхом заміни ступеня $m-1$ рішенням (6), яке визначає максимум ймовірності в точці $m-1$.

$$P(t) = \left[\left(\frac{f(t)}{f(t)+t}\right)^{\frac{f(t)}{t}} \cdot \left(\frac{t}{f(t)+t}\right)\right]^{\gamma}. \tag{11}$$

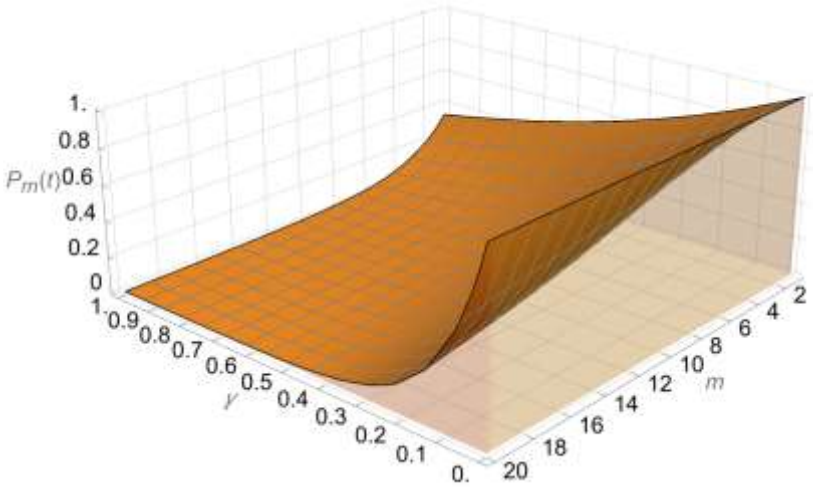

Рис. 1. Залежність $P_m(t)$ від кількості спроб m та ефективності проектованого захисту γ при $f(t) = 20$, $t = 10$

Визначимо $f(t)$ через час *t*, враховуючи (6) та вихідні дані: початкові $m_1 = 1$; $t_1 = 0$ і необхідні при проектуванні системи ТЗІ m_2 і t_2 шляхом апроксимації таким чином, щоб $f(t)$ приймала відповідні значення при вибраних вихідних даних

$$f(t) = \left[(m_1 - 1) + \frac{m_2 - m_1}{t_2 - t_1} \cdot (t - t_1)\right] \cdot t, \tag{12}$$

де $\omega = \frac{m_2 - m_1}{t_2 - t_1}$ – середня частота спроб проникнення.

Якщо у вираз (12) підставити вихідні дані часу t_1 і t_2, то $f(t)$ дасть значення, відповідні спробам проникнення m_1 і m_2. З іншого боку, аналогічним чином знаходиться $f(m)$ через спроби проникнення $m-1$ з урахуванням початкових даних

$$f(m) = \left[t_1 + \frac{t_2 - t_1}{m_2 - m_1} \cdot (m - m_1) \right] \cdot (m-1). \quad (13)$$

Використовуючи вирази (12) і (13) можна побудувати поверхню, яка одночасно задовольнятиме спробам проникнення та часу проникнення проектованої СЗІ:

$$f(m,t) = \sqrt{f(t) \cdot f(m)}. \quad (14)$$

Як було показано у [11], якщо побудувати поверхні для виразів (12), (13) та (14), то можна показати, що проектований процес проникнення на ОІД відбуватиметься за загальною лінією перетину всіх цих поверхонь. Реальний процес проникнення на ОІД відбуватиметься по лінії перетину поверхонь, на якій виконується умова $f(t) = f(m)$. Час спроби проникнення можна визначити через середню частоту та кількість спроб проникнення з (12) і (13):

$$t(m) = \frac{\sqrt{A^2 + \frac{4}{\omega} \cdot f(m)} - A}{2}, \text{ або } m(t) = \frac{\sqrt{B^2 + 4 \cdot \omega \cdot f(t)} - B}{2} + 1 \quad (15)$$

де $A = t_1 + \frac{m_1 - 1}{\omega}$ та $B = \omega \cdot t_1 - (m_1 - 1)$.

5. Модель залежності параметрів захищеності об'єкта інформаційної діяльності.

Ймовірність проникнення на ОІД на *m*-й спробі може бути визначена за допомогою:

$$P(m) = \frac{1}{m}, \text{ або } P(m) = P(t) = \frac{1}{m(t)}. \quad (16)$$

За допомогою виразів (12) – (16) можна провести процес проектування СЗІ. Поверхні ймовірностей проникнення можуть бути побудовані за допомогою виразу для максимумів

$$P(m,t) = \left[\left(\frac{f(m)}{f(m)+t} \right)^{\frac{f(m)}{t}} \cdot \left(\frac{t}{f(m)+t} \right) \right]^{\gamma}, \quad (17)$$

та виразів припустимої ймовірності (15), і тієї ж ймовірності, вираженої через час (16). В результаті розв'язання рівності щодо γ після перетворень отримаємо:

$$\gamma_m = \frac{t(m) lg(m)}{lg\left[\frac{f(m)+t(m)}{f(m)} \right]^{f(m)} + lg\left[\frac{f(m)+t(m)}{t(m)} \right]^{t(m)}}, \quad \gamma_t = \frac{t\, lg\left[m(t) \right]}{lg\left[\frac{f(t)+t}{f(t)} \right]^{f(t)} + lg\left[\frac{f(t)+t}{t} \right]^{t}}. \quad (18)$$

Якщо відомі лише $m_{пр}$ та $t_{пр}$, то можна визначити необхідну ефективність захисту, підставивши ці параметри у (18). Залежність параметра γ від $m_{пр}$ та $t_{пр}$ наведено на рис. 2.

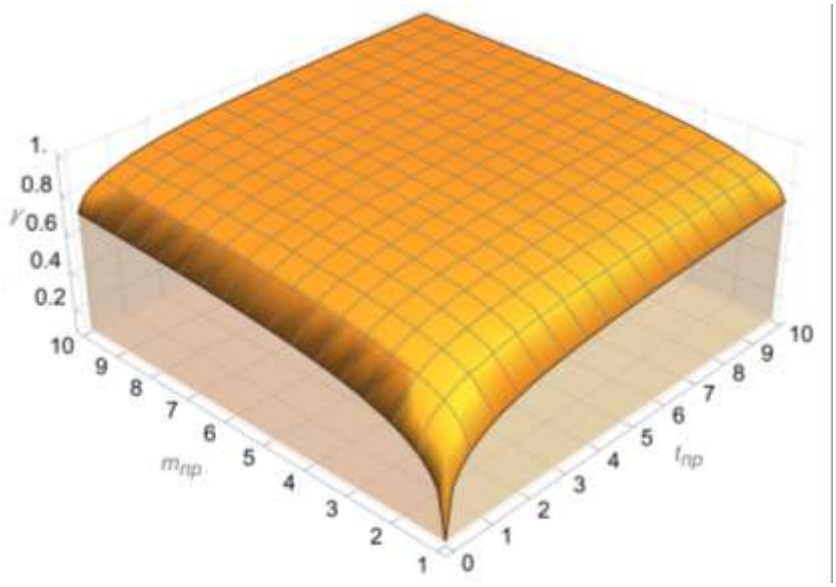

Рис. 2. Залежність ефективності захисту γ від $m_{пр}$ та $t_{пр}$ при $m_1 = 1$, $t_1 = 0$, $m_2 = 2$, $t_2 = 1$

Як видно з рис. 2, якщо зловмисник може собі дозволити декілька спроб на проникнення і має достатньо часу на реалізацію таких спроб, то, чим більше спроб $m_{пр}$ та часу $t_{пр}$ є у його розпорядженні, тим більшим має бути параметр захищеності об'єкта γ щоб не допустити проникнення. Як вже зазначалося, теоретично, при $\gamma = 1$ проникнення можливе лише при $m_{пр} \to \infty$, або $t_{пр} \to \infty$, а при $\gamma > 1$ проникнення взагалі неможливе і захищеність ОІД гарантується. Моделювання (11), (16) та (17) з урахуванням (15) та вихідних даних $m_1 = 1$, $t_1 = 0$, $m_{пр} = m_2 = m = 9$, а також $\gamma = 0.7$, дозволяє отримати поверхні максимумів ймовірностей проникнення (рис. 3).

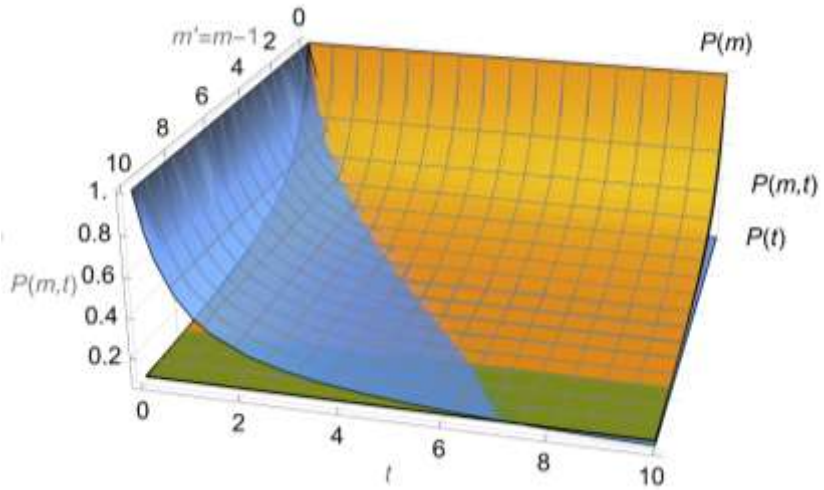

Рис. 3. Поверхні ймовірностей проникнення при $m_1 = 1$, $t_1 = 0$, $m_2 = 9$, $t_2 = 6$, $\gamma = 0.7$

По лінії перетину поверхонь $P(m)$ і $P(t)$ буде здійснюватися процес проникнення на ОІД, який визначається обраними вихідними даними. Поверхня $P(m,t)$, отримана за допомогою (16) із заміною $f(m)$ на $f(m,t)$. При проектуванні СЗІ точка перетину всіх поверхонь дає необхідну спробу проникнення. Лінія ймовірності проникнення дозволить не тільки проектувати СЗІ, але й досліджувати і керувати самим процесом проникнення за збігом

або відхиленням подій проникнення, що відбулися, від лінії проникнення. Із результатів рис. 3 видно, що при вихідних проектованих параметрах та ефективності СЗІ $\gamma = 0.7$ проникнення відбудеться у часі при $t = 6$ на $m = 8$ спробі.

6. Алгоритм проектування системи захисту інформації від витоку матеріально-речовим каналом.

Враховуючи вищенаведений підхід алгоритм проектування системи захисту інформації від витоку матеріально-речовим каналом з заданими показниками захищеності можна подати наступним чином:

1. За початковими вихідними даними задається чи обчислюється середня частота спроб проникнення на ОІД.

2. За формулами (12) – (14) визначаються значення виразів $f(m)$, $f(t)$, $f(m,t)$, які відповідають за ймовірнісні властивості проектованої СЗІ.

3. За вихідними даними з допомогою виразів (18) розраховується проектована ефективність СЗІ.

4. Будуються поверхні ймовірностей проникнення за формулами (11), (16), (17), як наведено на рис. 3.

5. За перетином поверхонь визначається напрям проектованого процесу проникнення і зона допуску спроб і часу проникнення (на рис. 3 – область світлого кольору).

Таким чином, визначення виду функцій $f(m)$, $f(t)$, $f(m,t)$ з параметрами, властивими конкретній проектованій СЗІ, через спроби *m* і час *t* проникнень зловмисника на ОІД, що враховують початкові $m_1 = 1$, $t_1 = 0$ та необхідні для проектування СЗІ m_2 і t_2. За допомогою цих вихідних даних та отриманих функцій можна обчислити частоту спроб проникнення, а надійність СЗІ – через частоту спроб проникнення і одного з проектованих параметрів спроб проникнення *m*, або часу спроб проникнення *t*, або тільки через проектовані параметри $m_{пр}$ і $t_{пр}$. Також, за допомогою функцій $f(m)$, $f(t)$, $f(m,t)$ можна передбачити, в якому напрямку йде проектований процес проникнення на ОІД.

7. Висновки

Стрімкий розвиток технологій призводить до того, що в умовах зростаючої кількості загроз інформаційній безпеці особливо актуальною є проблема захисту інформації від витоку через матеріально-речові канали. На сьогоднішній день зловмисникам вже недостатньо просто мати лише інформацію про нові технології, вони прагнуть заволодіти також і результатами передових розробок, що робить проблему їх захисту вкрай актуальною.

Запропонований метод захисту інформації від витоку матеріально-речовим каналом із заданими параметрами захищеності враховує кількість припустимих спроб проникнення та час, який необхідно витратити зловмиснику для проникнення на об’єкт для заволодіння зразком технологій чи документом. У розробленій моделі збільшення параметра захищеності об’єкта призводить до зниження ймовірності проникнення. Визначення лінії ймовірності проникнення дозволяє не тільки проектувати ефективні системи захисту, але й керувати самим процесом проникнення за збігом чи відхиленням інцидентів безпеки, що відбулися, від лінії проникнення.

Подальші дослідження щодо побудови ефективних систем захисту інформації від витоку матеріально-речовим каналом можуть бути зосереджені на методах визначення ймовірностей проникнення та показників захищеності систем захисту з урахуванням особливостей конкретних організацій.

Список використаної літератури

1. Матеріально-речові канали витоку інформації. https://ssbb.ua/poshuk-i-vyyavlennya-proslyshky/poshuk-zakladnykh-ustrojstv/materialno-veshestvennye-kanaly-utechki-informacii/

2. Skandhakumar, N., Salim, F., Reid, J., Dawson, Ed. (2012). Physical Access Control Administration Using Building Information Models. 236-250. https://doi.org/10.1007/978-3-642-35362-8_19

3. Fernández, E., Ballesteros, J., Desouza-Doucet, A., Larrondo Petrie, M. (2007). Security Patterns for Physical Access Control Systems. 4602. 259-274. https://doi.org/10.1007/978-3-540-73538-0_19

4. Masoumzadeh A., Hans van der Laan, and Dercksen A. (2022). BlueSky: Physical Access Control: Characteristics, Challenges, and Research Opportunities. In Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies (SACMAT '22). Association for Computing Machinery, New York, NY, USA, 163-172. https://doi.org/10.1145/3532105.3535019

5. 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

6. 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

7. Журиленко, Б.Є., Ніколаєва, Н.К. (2018). Імовірна надійність технічного захисту інформації в залежності від напрямки злому. Захист інформації, том 20, № 3, 174-180. https://doi.org/10.18372/2410-7840.20.13073

8. Журиленко, Б.Є., Ніколаєва, Н.К., Пелих, Н.С. (2012). Оцінка стійкості технічного захисту інформації у часі. Захист інформації, том 14, № 1 (54), 12-19. https://doi.org/10.18372/2410-7840.14.2071

9. Журиленко, Б., Ніколаєв, К., Рябова, Л. (2021). Математична модель фізичного процесу зламу технічного захисту інформації. Захист інформації, том 23, № 3, 167-176. https://doi.org/10.18372/2410-7840.23.16405

10. Журиленко, Б., Ніколаєв, К. (2020). Послідовний дворівневий захист інформації з імовірнісний надійністю. Захист інформації, том 22, № 1, 21-26. https://doi.org/10.18372/2410-7840.22.14660

11. Журиленко, Б. (2014). Метод проектування одиничної системи технічного захисту інформації з імовірнісною надійністю та заданими параметрами злому. Захист інформації, том 20, № 1, 26-42. https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/6572/7343