УДК 004.056.5:004.08
DOI: 10.31673/2409-7292.2024.040005

Чабан Б. В., Котенко А. М.

МОДЕЛЬ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ МАТЕРІАЛЬНО-РЕЧОВИМ КАНАЛОМ НА БАЗІ ЛАНЦЮГІВ МАРКОВА

Зростання обсягів конфіденційних даних, що обробляються в організаціях, і підвищенням ризику їх витоку через недосконаліть контролю фізичного доступу та використання технічних пристроїв обумовлює актуальність дослідження протидії витоку інформації матеріально-речовим каналом. Сучасні загрози пов'язані з маніпуляцією матеріальними носіями, мобільними пристроями, портативними накопичувачами, а також із викраденням інформації через друковані документи. Розвиток технологій ускладнює ідентифікацію таких каналів витоку, що вимагає вдосконалення методів їх виявлення, моніторингу та нейтралізації. У статті досліджується проблема 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. Крім того, автори досліджують концепцію багаторівневої системи захисту організації, яка враховує задіяні ресурси та навички співробітників служб захисту щодо протидії кібератакам. Наприкінці статті зроблено висновок, що запропонована концепція системи захисту організації буде ефективною проти витоку інформації матеріально-речовим каналом. Ефективна протидія сприятиме не лише збереженню інформаційної безпеки підприємств, але й забезпеченню довіри до організацій з боку партнерів, клієнтів та регуляторів.

Ключові слова: Кібербезпека, витік інформації, матеріально-речовий канал витоку, Марківський ланцюг, Марківська модель.

Вступ

З кожним днем питання кібербезпеки стають дедалі більш актуальними. Компанії вкладають значні кошти для захисту своїх комп'ютерних мереж від хакерів і вірусів, а також для захисту окремих комп'ютерів і приміщень від несанкціонованого доступу. Збільшення обсягу інформації, яка зберігається та обробляється в компанії, підвищує ризик викрадення матеріальних носіїв інформації (МНІ), що робить актуальною проблему протидії витоку інформації матеріально-речовим каналом [1].

Перелік МНІ є достатньо широким: паперові, оптичні, магнітні носії, біометричні пристрої та електронні сховища. Всі вони можуть бути викрадені зловмисником, якщо існують прогалини у системі захисту компанії. Захист МНІ від викрадення матеріально-речовим каналом традиційно відноситься до сфери технічного (фізичного) захисту інформації. Разом з тим, компанії вкрай неохоче діляться інформацією про проблеми внутрішньої безпеки, тому статистика таких атак та протидії їм з боку служб захисту є вкрай обмеженою. Відтак, основним методом дослідження проблеми протидії витоку інформації матеріально-речовим каналом є моделювання [2, 3].

Постановка проблеми дослідження

Традиційно моделювання загроз витоку інформації матеріально-речовим каналом зосереджується на поведінкових і психологічних методах, враховуючи особу потенційного порушника та прогнозуючи випадки можливого витоку [4]. Водночас самі по собі поведінкові моделі не дають уявлення про те, як має бути побудована ефективна система захисту від витоку інформації матеріально-речовим каналом. Такі моделі не враховують динаміку взаємодії потенційного порушника з системою безпеки організації. Зокрема, залишається незрозумілим, яким має бути розподіл ролей співробітників відповідно до їх кваліфікації та доступу до МНІ. Загроза витоку матеріально-речовим каналом – це динамічний процес, а отже, науковий інтерес становить зміна певних параметрів системи "організація – зловмисник" у часі. Логічно припустити, що реакції системи захисту організації повинні випереджати будь-якого потенційного зловмисника.

Аналіз публікацій

Марківські моделі є одними з найпоширеніших для моделювання динаміки взаємодії зловмисників із захистом організації. Так, у публікації [5] запропоновано побудувати

математичну модель протидії загрозам у системі захисту критичних інформаційних ресурсів організації за допомогою ланцюга Маркова. Такий підхід дає змогу визначати та моделювати параметри різних видів атак з акцентом на ймовірність збереження інформації без урахування часових параметрів захисту.

Публікація [6] пропонує метод виявлення атак шляхом виявлення аномалій на основі моделі ланцюга Маркова, яка представляє профіль переходу комп'ютерних подій у мережевій системі. Чим більше спостережувана активність користувача відрізняється від звичайної моделі ланцюга Маркова, тим більша ймовірність аномалії через атаку. У статті [7] предметом дослідження є побудова моделі на основі властивостей Марківських процесів, яка дозволяє детальніше вивчити процес, виконати аналіз та прогнозування розвитку кіберінциденту для прийняття управлінського рішення щодо подальших конструктивних дій. Автори [8] пропонують новий підхід до математичного моделювання системи управління кібербезпекою на судні, а саме використання теорії ланцюгів Маркова, оскільки кібератака на судно може статися в будь-який випадковий момент, і ця подія не завжди залежить від атак, які відбулися раніше.

Публікація [9] розглядає ланцюги Маркова для опису раніше невідомих уразливостей. Запропонований підхід, заснований на напівмарківському процесі, використовується для аналізу атак з будь-яким довільним типом розподілу часу переходу. В публікації [10] пропонується Марківська динамічна гра, яка може оцінити ефективність методів захисту проти зловмисника за допомогою штучного інтелекту в хмарній системі, в якій зловмисник використовує техніку штучного інтелекту, щоб розпочати розширену атаку, знаходячи найкоротший шлях атаки.

Моделювання системи "організація – зловмисник" може здійснюватися в різних аспектах. Аспект часу взаємодії в такій системі залишається недостатньо вивченим, тому що, незважаючи на очевидний факт, що захист повинен бути більш активним, ніж атака, проблема співвідношення часу реакції захисту до часу атаки ще не досліджена. У статті [11] на основі ланцюга Маркова автори пропонують базову модель взаємодії в системі "організація – інсайдер". У статті аналітично визначено співвідношення між часом інсайдерської атаки та часом, протягом якого система безпеки організації може її нейтралізувати.

Метою даної статті є дослідження фактору часу подолання загрози витоку інформації матеріально-речовим каналом та визначення основних часових параметрів системи захисту організації від такої загрози.

Модель захисту інформації від витоку матеріально-речовим каналом

Для подальших досліджень на основі [11] створимо типову модель у вигляді ланцюга Маркова з дискретними станами та безперервним часом (рис. 1). Ця модель описує діяльність потенційного зловмисника у вигляді послідовності станів 1, 2, 3, 4, 5, після яких він може досягти успіху (стан 5): 1 – нормальна робота організації; 2 – підготовка зловмисника до нападу; 3 – атака (викрадення носія інформації); 4 – знищення слідів викрадення; 5 – реалізація носія інформації.

Переходи з одного стану в інший визначаються як здатністю потенційного зловмисника виконувати певні дії в організації, так і діяльністю служб безпеки та функціонуванням технічних засобів захисту. Ланцюг переходів $1 \to 2 \to 3 \to 4 \to 5$ описує діяльність зловмисника для досягнення бажаної мети – викрадення та використання МНІ. Модель також передбачає ще два стани, які безпосередньо характеризують можливості системи захисту: 6 – перехоплення атаки службою безпеки; 7 – відмова зловмисника від проведення атаки (в тому числі і через складність подолання технічного (фізичного) захисту). Будемо вважати, що ці умови залежать виключно від характеристик служби безпеки (стан 6) і технічних засобів контролю (стан 7). Переходи $6 \leftarrow 2 \to 7$, $6 \leftarrow 3 \to 7$ і $6 \leftarrow 4 \to 7$ утворюють три рубежі захисту в організації і залежать лише від можливостей системи безпеки.

© 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.

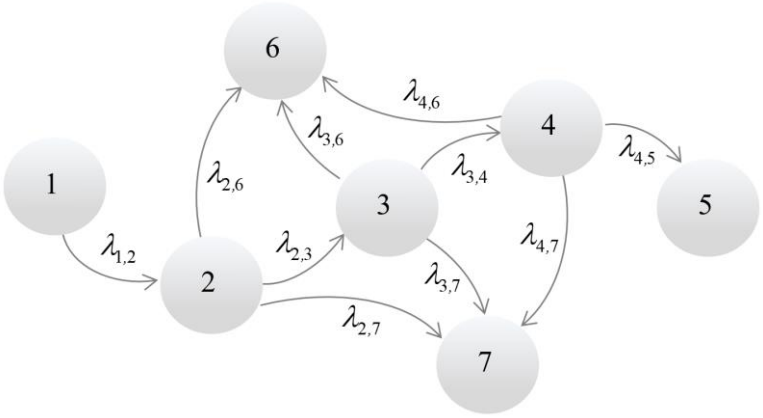


Рис. 1 Марківська модель системи захисту інформації від витоку матеріально-речовим каналом

Таким чином, переходячи зі стану 1 у стан 2, зловмисник має два варіанти: або піти далі до стану 3, реалізуючи власний план атаки, або бути перехопленим системою безпеки, потрапивши в стан 6, або відмовитися від подальших намірів – перехід до стану 7. Показники інтенсивності $\lambda_{i,j}, i, j = 1,...,7$ у цій моделі описують динаміку системи. Інтенсивність переходів є оберненою характеристикою середнього часу, витраченого на перехід до певного стану з попереднього

$$\lambda_{i,j} = \frac{1}{\bar{t}_{i,j}}, i, j = 1,...,7 . \tag{1}$$

Поведінку системи можна описати за допомогою диференційних рівнянь Колмогорова:

$$\begin{cases} \frac{\partial P_1(t)}{\partial t} = -\lambda_{1,2} P_1(t); \\ \frac{\partial P_2(t)}{\partial t} = \lambda_{1,2} P_1(t) - \lambda_{2,3} P_2(t) - \lambda_{2,6} P_2(t) - \lambda_{2,7} P_2(t); \\ \frac{\partial P_3(t)}{\partial t} = \lambda_{2,3} P_2(t) - \lambda_{3,4} P_3(t) - \lambda_{3,6} P_3(t) - \lambda_{3,7} P_3(t); \\ \frac{\partial P_4(t)}{\partial t} = \lambda_{3,4} P_3(t) - \lambda_{4,5} P_4(t) - \lambda_{4,6} P_4(t) - \lambda_{4,7} P_4(t); \\ \frac{\partial P_5(t)}{\partial t} = \lambda_{4,5} P_4(t); \\ \frac{\partial P_6(t)}{\partial t} = \lambda_{2,6} P_2(t) + \lambda_{3,6} P_3(t) + \lambda_{4,6} P_4(t); \\ \frac{\partial P_7(t)}{\partial t} = \lambda_{2,7} P_2(t) + \lambda_{3,7} P_3(t) + \lambda_{4,7} P_4(t). \end{cases} \tag{2}$$

Припустимо, що з самого початку система перебуває в стані нормальної роботи (стан 1), і тому початкові умови для диференціювання в момент часу $t = 0$ буде:

$$P_1(0) = 1;\ P_2(0) = P_3(0) = P_4(0) = P_5(0) = P_6(0) = P_7(0) = 0. \tag{3}$$

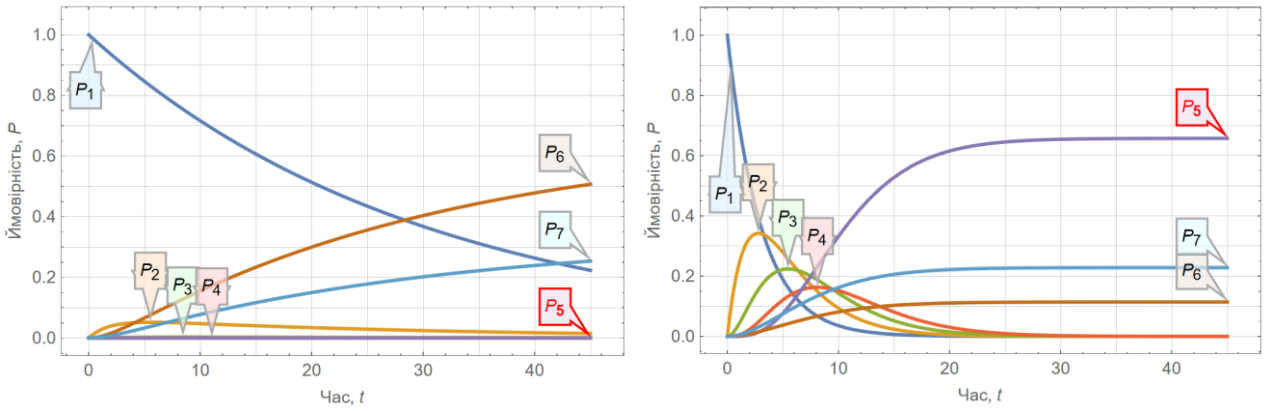
© Чабан Б. В., & Котенко А. М. (2024). Модель системи захисту інформації від витоку матеріально-речовим каналом на базі ланцюгів Маркова. Сучасний захист інформації, 4(60), 46–52. https://doi.org/10.31673/2409-7292.2024.040005.

Розглянемо для прикладу реалізацію моделі для двох варіантів при наступних початкових умовах:

1). У системі “організація – зловмисник” переважає захист. Служби захисту та обладнання для фізичного захисту в організації є більш потужними, ніж можливості зловмисника щодо здійснення атаки: $\lambda_{1,2}=\lambda_{2,3}=\lambda_{3,4}=\lambda_{4,5}=1/30$; $\lambda_{2,6}=\lambda_{3,6}=\lambda_{4,6}=1/3$; $\lambda_{2,7}=\lambda_{3,7}=\lambda_{4,7}=1/6$; $t_{max}=45$.

2). У системі “організація – зловмисник” переважає зловмисник. Можливості зловмисника щодо проникнення та викрадення МНІ є більш потужними, у порівнянні з можливостями служби захисту та обладнання для фізичного захисту: $\lambda_{1,2}=\lambda_{2,3}=\lambda_{3,4}=\lambda_{4,5}=1/3$; $\lambda_{2,6}=\lambda_{3,6}=\lambda_{4,6}=1/60$; $\lambda_{2,7}=\lambda_{3,7}=\lambda_{4,7}=1/30$; $t_{max}=45$.

В обох випадках реалізація системи рівнянь матиме наступний вигляд (рис. 2). Як бачимо, ймовірність перебування системи в стані 1 поступово зменшується (P_1). При цьому зростає ймовірність досягнення зловмисником своєї мети (P_5). Динаміка зміни цих станів залежить від інтенсивності переходів з одного стану до наступного. У першому випадку, при потужному захисті, ймовірність успішності атаки залишається вкрай низькою. У другому випадку, при слабкому захисті (коли час на реакцію системи захисту є значно більшим, ніж час зловмисної активності), ймовірність успішності атаки зростає суттєво. Ймовірності P_6 та P_7 описують роботу системи захисту.



а) б)

Рис. 2. Ймовірності станів системи “організація – зловмисник”:
а) потужний захист; б) слабкий захист

Для побудови ефективної системи захисту організації від витоку інформації матеріально речовим каналом необхідно мінімізувати ймовірність досягнення зловмисником своєї мети P_5. Параметрами керування в моделі є інтенсивності $\lambda_{i,j}, i,j=1,...,7$. Таким чином, підбираючи необхідне співвідношення параметрів інтенсивності, можна побудувати систему безпеки, в якій ймовірність успішної атаки зловмисника буде мінімальною. Оскільки інтенсивність – це обернена функція часу, то, відповідно, необхідно мінімізувати час реагування на атаку. Проблема створення ефективної системи захисту на основі балансу часу полягає в наступному: знайти оптимальні значення параметрів $\lambda_{i,j}$, які призводять до мінімізації ймовірності P_5 у полі стаціонарних розв’язків. Для цього розв’яжемо перше рівняння системи (2) з урахуванням $p_1(0)=1$ при початкових умовах (3):

$$p_1(t)=e^{-\lambda_{1,2}t}. \quad (4)$$

© 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.

Підставляючи (4) у друге рівняння системи (2) і розв'язуючи його за умови, що $p_2(0)=0$ отримуємо рівняння для P_2

$$p_2(t)=\frac{\lambda_{1,2}}{\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{1,2}}\left(e^{-\lambda_{1,2}t}-e^{-(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7})t}\right). \quad (5)$$

Оскільки функція (5) має розриви в точках, визначених виразом $\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{1,2}=0$ доцільно дослідити такі розриви. Визначивши ліміт функції (5) зверху та знизу, можна побачити

$$\begin{aligned}&\lim_{\lambda_{1,2}\to(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7})^{+}}\frac{\lambda_{1,2}}{\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{1,2}}\left(e^{-\lambda_{1,2}t}-e^{-(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7})t}\right)=\\&\lim_{\lambda_{1,2}\to(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7})^{-}}\frac{\lambda_{1,2}}{\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{1,2}}\left(e^{-\lambda_{1,2}t}-e^{-(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7})t}\right)=\\&=(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7})te^{-(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7})t}=\lambda_{1,2}te^{-\lambda_{1,2}t}\end{aligned} \quad (6)$$

З виразу (6), можна зробити висновок, що зазначені розриви є "усувними", що дає змогу визначити значення (5) у точках розривів як $p_2(t)=\lambda_{1,2}te^{-\lambda_{1,2}t}$. Використовуючи цей підхід, надалі будемо вважати, що похідні функції для $p_3(t),p_4(t),p_5(t)$ матимуть певні значення в точках розриву.

Як показано у [11], подальші обчислення пов'язані з громіздкими математичними операціями, і тому, щоб не втратити символи у формулах і забезпечити правильність написання виразів для подальших обчислень, необхідно використовувати систему символьних обчислень. Підставляючи отримані рівняння для ймовірностей у відповідні рівняння з виразу (2) і розв'язуючи їх за умови, що $p_i(0)=0$, можна отримати подальші рівняння для P_i (i=3,…,5). Такі рівняння мають велику кількість розривів, оскільки є багато точок, де знаменники в елементах функцій дорівнюють 0. Для таких точок можна використати підхід, наведений у формулах (6), щоб отримати розв'язки рівнянь в точках розриву.

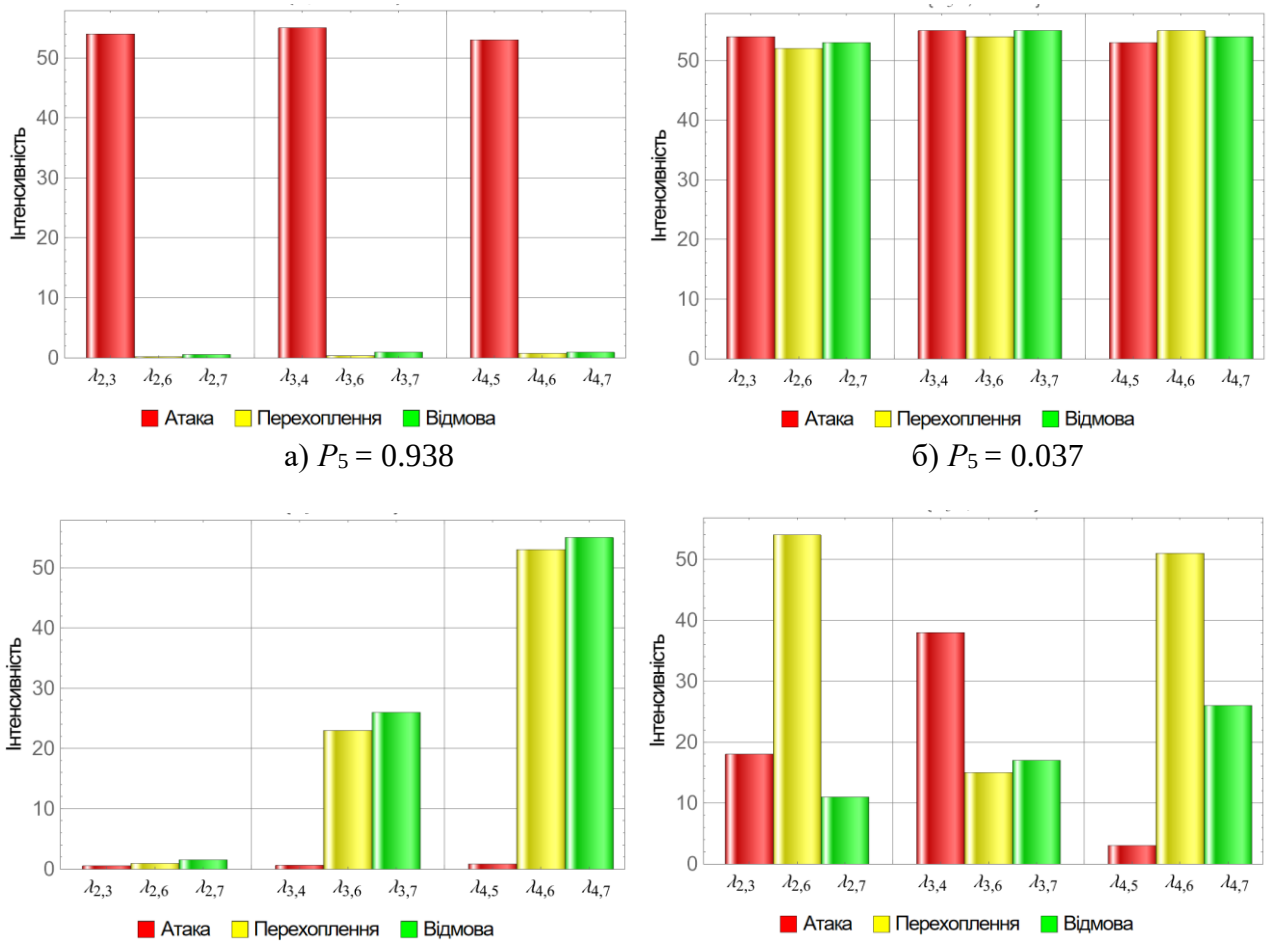
Функція $p_5(t)$ є цільовою функцією системи "організація – зловмисник". Для досягнення $p_5(t)\to 0$, необхідно знайти відповідні значення $\lambda_{i,j}$ на проміжку часу $t\to\infty$, оскільки нас цікавить робота системи в стаціонарному режимі. Слід зазначити, що аналітичний розв'язок оптимізаційної задачі $p_5(t)\to min$ є неможливим через те, що тоді необхідно буде накласти низку обмежень на більшість параметрів $\lambda_{i,j}$. У такому випадку для досягнення мети роботи більш доцільно змоделювати рівняння (7).

Апріорі ми можемо уявити, що для того щоб мінімізувати ймовірність $p_5(t)$, необхідно досягти певного співвідношення інтенсивностей. Зокрема, розглядаючи горизонтальну складову захисту на кожній лінії, можна виділити співвідношення інтенсивностей, яке можна сформулювати так:

$$\begin{cases}\lambda_{2,6}+\lambda_{2,7}>>\lambda_{2,3},\\ \lambda_{3,6}+\lambda_{3,7}>>\lambda_{3,4},\\ \lambda_{4,6}+\lambda_{4,7}>>\lambda_{4,5}.\end{cases} \quad (8)$$

© 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.

Суть нерівностей (8) полягає в тому, що для створення ефективної лінії захисту від зловмисника необхідно максимізувати інтенсивність переходів до станів 6 і 7 та мінімізувати перехід зловмисника до наступного стану атаки (ланцюжок $1\to2\to3\to4\to5$). Отже, візьмемо достатньо часу $t=500$ та $\lambda_{1,2}=1$ (оскільки існує лише один перехід від стану 1 до стану 2) як початкові умови для моделювання. Установка різних значень інтенсивності $\lambda_{i,j}$ і з урахуванням обмежень для підтвердження гіпотези (8) можна отримати відповідні значення $p_5(t)$. Результати моделювання для різних співвідношень інтенсивності $\lambda_{i,j}$ показані на рис. 3.



а) $P_5 = 0.938$ б) $P_5 = 0.037$

в) $P_5 = 0.000$ г) $P_5 = 0.004$

Рис. 3. Результати моделювання

На рис. 3а видно, що відсутність захисту дає максимальне значення успіху атаки. Атака може бути максимально успішною ($p_5\to1$) у випадку, коли інтенсивність нападу в десятки і сотні разів перевищує інтенсивність захисту. Поява належного захисту (рис. 3б) за тих же умов призводить до значного зниження успішності атаки. Як видно з рис. 3в і 3г, для випадкових значень інтенсивності атаки і інтенсивності захисту протягом значного періоду часу, ймовірність успіху атаки відносно незначна. Це пояснюється наявністю трьох ешелонів оборони і тим, що кількість оборонних переходів вдвічі більша за кількість наступальних.

Отже, як бачимо, основна перевага використання аналізу Маркова для оцінки часових параметрів системи захисту від витоку матеріально-речовим каналом полягає в тому, що таку атаку можна досить просто змоделювати. Однак така модель досить абстрактна і не може охопити всі нюанси атаки. У зв'язку з тим, що збільшення кількості станів і переходів

© 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.

призводить до збільшення числа рівнянь, ми змушені розглядати лише найосновніші стани і переходи, що дещо спрощує модель. Крім того, у розглянутому підході інтенсивності є змінними, незалежними від часу, хоча в реальному житті це не завжди так. Інший недолік обумовлений суттю Марківського процесу, який передбачає, що в будь-який момент часу ймовірність переходу системи в наступний стан у майбутньому залежить лише від стану, в якому система перебуває зараз, а всі попередні стани не враховуються. У реальному світі можуть бути ситуації, коли ймовірність переходу до наступного стану буде залежати від деякої комбінації попередніх станів. Також у цьому дослідженні основну увагу було зосереджено на граничному розподілі ймовірностей при $t \to \infty$, оскільки нас цікавить стан організації, який би забезпечував готовність системи захисту протистояти витоку інформації в будь-який момент. Всі ці недоліки обмежують можливості Марківської моделі для вивчення такого складного явища, як протидія витоку інформації матеріально-речовим каналом.

Висновки

Не зважаючи на велику кількість публікацій, присвячених протидії різного роду кібератакам, до цього часу розроблено лише обмежену кількість моделей для опису таких атак. Час є одним з найбільш впливових факторів, які впливають на ймовірність витоку інформації. Система безпеки організації, побудована на концепції збалансованого часу реакції захисту на дії потенційного зловмисника, є найбільш перспективною моделлю протидії загрозам. Організаціям необхідно досягти такого співвідношення часу між атакою та її ідентифікацією, щоб система безпеки випереджала будь-які можливі дії потенційного зловмисника. Напрямком подальших досліджень може бути широке коло питань визначення часових показників запропонованої моделі. Зокрема, повинні бути розроблені критерії та методи автоматизованої оцінки технічних та організаційних можливостей організації з метою підтримки необхідного балансу часу між захистом та потенційним нападом.

Перелік посилань

1. Матеріально-речові канали витоку інформації. (2024). https://ssbb.ua/poshuk-i-vyyavlennya-proslyshky/poshuk-zakladnykh-ustrojstv/materialno-veshestvennye-kanaly-utechki-informacii/

2. 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.

3. Котенко А. М. (2017) Запобігання витоку інформації з обмеженим доступом матеріально-речовим каналом за рахунок використання систем відеоспостереження. Сучасний захист інформації, № 1. 48–52.

4. 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.

5. Korniyenko, B.Y., Galata L. and Ladieva L.. (2019) Mathematical Model of Threats Resistance in the Critical Information Resources Protection System. International Conference on Intelligent Tutoring Systems [online]. https://ceur-ws.org/Vol-2577/paper23.pdf.

6. Nong, Y., Z. Yebin, and B. Connie. Robustness of the Markov-Chain Model for Cyber-Attack Detection. IEEE Transactions on Reliability, 2004, 53(1), pp. 116-123. https://doi.org/10.1109/TR.2004.823851.

7. Зайцева, Т. Марковські процеси в дослідженні ймовірності кібератак на морському судні / Т. Зайцева, Л. Кравцова, Н. Камінська // Information Technologies in Education: збірник наукових праць / голов. ред. О. В. Співаковський. – Херсон : ХДУ, 2022. – Вип. 3 (52). – С. 20-32.

8. Kaminska N., Kravtsova L., Kravtsov H. and Zaytseva T. Modeling ship cybersecurity using Markov chains: an educational approach. https://ceur-ws.org/Vol-3679/paper27.pdf

9. Gore, Ross & Padilla, José & Diallo, Saikou. (2017). Markov Chain modeling of cyber threats. Journal of Defense Modeling and Simulation. 14. 233-244. 10.1177/1548512916683451.

10. Hooman Alavizadeh, Julian Jang-Jaccard, Tansu Alpcan and Seyit A. Camtepe. A Markov Game Model for AI-based Cyber Security Attack Mitigation. https://arxiv.org/pdf/2107.09258

11. Savchenko, V., Savchenko, V., Dzyuba, T., Matsko, O., Novikova, I., Havryliuk, I., & Polovenko, V. (2024). Time Aspect of Insider Threat Mitigation. Advances in Military Technology, 19(1), 149-164. https://doi.org/10.3849/aimt.01830.

Надійшла 15.11.2024