УДК 519.226:004.056.53
DOI: 10.31673/2409-7292.2023.030404

Кожухівський А. Д., Коровайченко Ю. Ю.

МЕТОДИКА ПРОГНОЗУВАННЯ ЙМОВІРНОСТІ ІНСАЙДЕРСЬКОЇ АТАКИ НА ОСНОВІ АНАЛІЗУ БАЙЄСІВСЬКИХ МЕРЕЖ

Небезпека інсайдерської загрози є достатньо високою для будь-якого підприємства. Для прогнозування можливих атак інсайдерів необхідно знати структуру підприємства, ролі персоналу та політики безпеки, які застосовуються. Зважаючи на стохастичний характер системи широкого використання набули методи прогнозування на основі Байєсівського оцінювання. У статті розроблено модель прогнозування внутрішньої загрози на основі Байєсівської мережі, яка включає опис різних станів у вигляді графа мережевих атак, а також алгоритм виведення для розрахунку ймовірності ризику інсайдерської загрози. Для формування методики використовуються поняття «елементарна атака», як мінімальний набір операцій, необхідних зловмиснику для переходу від одного ресурсу до наступного та «доказ вторгнення», як сукупність серії дій, записаних зловмисником з одного ресурсу на інший ресурс і які можна відслідкувати за допомогою log-журналу. Для вимірювання масштабу вторгнення використовується «достовірність доказу вторгнення», як ймовірність того, що доказ вторгнення, визначений на множині операцій, охоплює елементарну атаку. Для перевірки достовірності запропонованої методики прогнозування інсайдерської атаки було проведено моделювання методом Монте-Карло, де змінні визначалися за допомогою генератора випадкових чисел. За результатами моделювання встановлено, що зі збільшенням числа випробувань та початкової ймовірності проникнення до ресурсу (окремого вузла мережі) загальна кількість проникнень збільшується, також збільшується і загальна ймовірність проникнення до вузла. Разом з тим, результат майже не залежить від поточного кроку випробувань і загальна ймовірність залишається сталою. Мережева структура внутрішньої загрози, яка описана в Байєсівською моделлю, може бути використана для обчислення загальної вірогідності інсайдерських атак.

Ключові слова: інсайдер, інсайдерська атака, Байєсівська мережа, Байесівське оцінювання, проникнення, прогнозування.

Вступ

Небезпека інсайдерської загрози є достатньо високою для будь-якого підприємства. На теперішній час існує достатньо широкий арсенал протидії інсайдерам, як у технічній площині, так і у соціальній та психологічній. Важливим елементом протидії інсайдерам є прогнозування такого типу атак. Для прогнозування можливих атак інсайдерів необхідно знати структуру підприємства, ролі персоналу та політики безпеки, які застосовуються.

Постановка проблеми

Арсенал методів прогнозування, які застосовуються у кібербезпеці, є достатньо широким. У той же час, для визначення поведінки інсайдера більш популярними та практичними є методи моделювання. Зважаючи на стохастичний характер системи широкого використання набули методи прогнозування на основі Байєсівського оцінювання.

Байєсівська мережа – це графова модель, яка використовується для опису залежних взаємозв’язків між випадковими величинами та застосовується для вирішення проблем невизначеності. Вона широко застосовується для аналізу, прогнозування та оцінювання ймовірностей. За визначенням Байєсівської мережі побудова моделі на її основі має включати два аспекти: 1) у якісному аспекті вона використовує спрямований ациклічний граф для відображення взаємозалежних та незалежних відносин між різними вузлами, що є мережевою структурою моделі; 2) у кількісному аспекті вона використовує умовний розподіл ймовірностей для опису залежного відношення одного (дочірнього) вузла до іншого (батьківського) вузла, що є параметром моделі.

Аналіз дотичних джерел

У роботі [1] наведено приклад Байєсівської мережі на основі поточної моделі графа безпеки, обґрунтовано підхід до моделювання за допомогою семантики атаки та показано на основі експериментальних досліджень, що отримана Байєсівська мережа нечутлива до збурень параметрів. У роботі [2] представлено підхід до аналізу, заснований на формалізмі Байєсівських мереж і сценаріях реальних загроз. Він дозволяє проводити аналіз, орієнтований

© Кожухівський, А. Д., & Коровайченко, Ю. Ю. (2023). Методика прогнозування ймовірності інсайдерської атаки на основі аналізу Байєсівських мереж. Сучасний захист інформації, 4(56), 33–41. https://doi.org/10.31673/2409-7292.2023.030404.

на планування заходів безпеки та моніторинг, а також на прогнозування суперницької поведінки користувачів. У роботі [3] розроблено гнучкий підхід, для реалізації моделі Факторного аналізу інформаційних ризиків за допомогою Байєсівських мереж. Щоб оцінити продуктивність моделі, автори використовують метод Монте-Карло, таким чином уникаючи відповідної неточності, яка може бути внесена. У статті [4] розроблено систематичну кількісну процедуру на основі підходу Байєсівської мережі для розрахунку ймовірності успіху атак на фізичну безпеку, враховуючи як превентивні, так і пом'якшувальні стратегії втручання в безпеку.

Стаття [5] пропонує модель ризиків кібербезпеки, заснована на Байєсівській мережі, для комплексної оцінки кібербезпеки ядерних установок. Запропонована модель дає змогу оцінювати як процедурні, так і технічні аспекти кібербезпеки, які пов'язані з дотриманням нормативних вказівок та системної архітектури відповідно. Дві моделі об'єднані в єдину модель, яка називається моделлю ризиків кібербезпеки, щоб кібербезпеку можна було оцінити одночасно з процедурної та технічної точок зору. Публікація [6] показує кількісну структуру, яка містить: Байєсівську мережу, яка охоплює кілька сценаріїв атак і, таким чином, дозволяє краще оцінити вразливості; і модель багатоцільової оптимізації, побудована на основі зазначеної мережі, яка явно представляє численні виміри потенційних наслідків успішних кібератак. Структура використовує ширшу перспективу, ніж стандартний аналіз витрат і вигод, і дозволяє формулювати більш тонкі цілі безпеки. Запропоновано обчислювально ефективний алгоритм, який визначає набір оптимальних за Парето портфелів заходів безпеки, які одночасно мінімізують різні типи очікуваних наслідків кібератак, задовольняючи при цьому бюджетні та інші обмеження. У статті [7] було розроблено та проаналізовано різні сценарії, щоб визначити критичні змінні, чутливі до кібервідмовостійкості інтелектуальної мережевої системи. Результати цих аналізів свідчать про те, що загальна кіберстійкість системи залежить від стану визначених факторів, і більше уваги слід приділяти розробці контрзаходів проти вразливості домену доступу. Дослідження також показує ефективність Байєсівської мережі для оцінки та підвищення загальної кіберстійкості системи інтелектуальної мережі.

Найбільш близькою для вирішення проблеми є публікація [8], де показано, що важливим інструментом для аналізу безпеки є граф мережевих атак а технологія автоматичного формування графу мережевих атак є проблемою, яку досліджують експерти в країні та за кордоном, і на сьогодні вона вже досягла хороших результатів. Байєсова мережа – це перевірена теоретична модель для вирішення оцінки та прогнозування ризику невизначеності, а також досконалий метод моделювання.

Мета роботи полягає у розробці такої моделі прогнозування внутрішньої загрози на основі Байєсівської мережі, яка б включала опис різних станів у вигляді графа мережевих атак, а також алгоритм виведення для розрахунку ймовірності ризику інсайдерської загрози.

Викладення основного матеріалу

Для загального формулювання структури моделі необхідно дати визначення *операції*. Мережева атака складається з різних наборів команд або дій, а сукупність різних команд або дій, сформованих будь-якими методами, називається *операцією*.

Крім того, для подальшого розгляду необхідним є також визначення *елементарної атаки.* Для цього можна скористатися сигнатурним методом, який описує прогнозування інсайдерської загрози. Перед тим, як користувачі використовують інформаційну систему, вони повинні подавати свої наміри відповідно до певної форми у вигляді списку <тема, рух, об'єкт, період>. Тобто, користувач повинен зробити завчасну заявку щодо дій у системі, які він має намір зробити. Легальний набір операцій (MOS) у внутрішній мережі віображається у вигляді атрибутів <рух, об'єкт> плану, який подали користувачі.

У процесі атаки серія операцій між двома ресурсами (включаючи всі види замовлень та операцій) відповідає підмножині MOS–Sub-MOS і називається *елементарною атакою*.

© Кожухівський, А. Д., & Коровайченко, Ю. Ю. (2023). Методика прогнозування ймовірності інсайдерської атаки на основі аналізу Байєсівських мереж. Сучасний захист інформації, 4(56), 33–41. https://doi.org/10.31673/2409-7292.2023.030404.

Елементарна атака – це мінімальний набір операцій, необхідних зловмиснику для переходу від одного ресурсу до наступного.

Ще одним поняттям, яке необхідно ввести для подальшого розгляду, є визначення доказу вторгнення. *Доказ вторгнення* – це сукупність серії дій, записаних зловмисником з одного ресурсу на інший ресурс і які можна відслідкувати за допомогою log-журналу. Доказ вторгнення – це також набір, що складається з множини операцій з певним порядком. Різні операції та різний порядок дають різні докази вторгнення. *Достовірність доказу вторгнення* використовується для вимірювання масштабу вторгнення. Достовірність доказу вторгнення – це ймовірність того, що доказ вторгнення, визначений на множині операцій, охоплює елементарну атаку. Тут «охоплення» означає, що відповідно до послідовності операцій у множині елементарної атаки, кількість операцій в множині доказів вторгнення та у атаці однакова.

Припустимо, що атака складається з множини операцій m_i, дорівнює $\{m_1, m_2, m_3, m_4\}$ і порядок операцій складає $m_1 \rightarrow m_2 \rightarrow m_3 \rightarrow m_4$. Таким чином, охоплення доказів вторгнення $\{m_1, m_5, m_6, m_2, m_7\}$ дорівнює 2, а достовірність становить 0.5; охоплення доказів вторгнення $\{m_5, m_6, m_7, m_8\}$ дорівнює 0, і достовірність також дорівнює 0. Охоплення доказів вторгнення $\{m_2, m_1, m_5, m_6\}$ дорівнює 1, а достовірність 0.25.

Для зручності пояснення, якщо припустити, що кількість операцій в елементарній атаці дорівнює n, то, коли кількість доказів вторгнення менша за n, справа називається недостатньо доказовою (слабо доказовою); коли загальна кількість доказів вторгнення дорівнює n, цей випадок називається достатньо доказовим. Рис. 1 – приклад, що демонструє взаємозв'язок між операцією, елементарною атакою та доказами вторгнення. v_1 і v_2 – два вузли ресурсів, а o_1 і o_2 – два докази вторгнення, взаємозв'язок показано на рис. 1: коли V_1 зайнятий, зловмисник може зайняти V_2 через докази вторгнення o_1 або o_2.

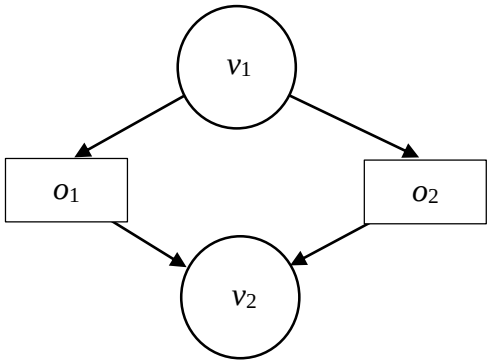

Рис. 1. Зв'язок між операціями та доказами вторгнення

Нехай загальна множина операцій $M=\{m_i \mid i=1,2,3\ldots,n\}$, і, якщо зловмисник хоче зайняти вузол ресурсу v_2 з вузла ресурсу v_1, йому необхідно здійснити чотири операції, наприклад, $m_2 \rightarrow m_4 \rightarrow m_5 \rightarrow m_7$, стрілка показує послідовність чотирьох операцій у елементарній атаці $\{m_2, m_4, m_5, m_7\}$. Відповідно, коли число операцій менше чотирьох або послідовність цих чотирьох операцій відрізняється, вони не можуть бути елементарною атакою.

Докази вторгнення – це поєднання різних операцій, виявлених службою безпеки. Для наведеного прикладу, коли доказ вторгнення $o_1=\{m_1, m_2, m_3, m_4, m_6\}$, охоплення доказу вторгнення дорівнює 2, що є недостатнім доказом і не може свідчити про атаку. Якщо ж взяти у якості доказу вторгнення $o_1=\{m_1, m_2, m_3, m_4, m_5, m_6, m_7\}$, а множина доказу вторгнення буде підмножиною елементарної атаки, то тоді охоплення буде становити 4, що буде достатнім доказом успішного досягнення зловмисником вузла v_2.

Мережевий граф атаки. Для того, щоб описати різні можливі шляхи атаки та її характеристики, необхідно визаначити мережевий граф атаки (NAG – Network Attack Graph),

© Кожухівський, А. Д., & Коровайченко, Ю. Ю. (2023). Методика прогнозування ймовірності інсайдерської атаки на основі аналізу Байєсівських мереж. Сучасний захист інформації, 4(56), 33–41. https://doi.org/10.31673/2409-7292.2023.030404.

щоб показати взаємозв'язок різних позицій на шляху атаки. Визначення мережевого графа атаки виглядає наступним чином: $NAG=(V, V_0, G, O, E, P)$, де:

V – множина вузлів ресурсів, і $V = \{v_i \mid i = 1,2\ldots,N\}$, v_i – це окремий вузол, який використовується для опису ресурсу, який зловмисник зайняв у процесі атаки, і його значення має значення *True* або *False*. Коли зловмисник успішно зайняв ресурс v_i його значення дорівнює *True*, у протилежному випадку – *False*;

V_0 – множина ресурсів, які зловмисник зайняв у початковому стані. V_0 є підмножиною V. На мережевому графі атаки це набір початкових вузлів.

G – множина цільових вузлів, які зловмисник хоче остаточно досягти.

O – множина вузлів, що свідчать про вторгнення (доказів вторгнення), який означає множину серій операцій, коли зловмисник зайняв певні ресурси. $O = \{o_i \mid i=1,2...,n\}$, o_i – це вузол єдиного доказу вторгнення і його значенням є достовірність доказу вторгнення, яка коливається у межах [0, 1]. Коли достовірність доказів вторгнення менше 1, це свідчить про те, що немає достатніх доказів щодо вторгнення, і наступний вузол ресурсу зловмисником не зайнятий; коли достовірність доказів вторгнення становить 1, це свідчить про те, що є достатні докази вторгнення, і наступний вузол ресурсу вже зайнятий.

E – множина спрямованих ребер, асоційованих з усіма видами вузлів. $E=(E_1 \cup E_2)$, в якому $E_1 \subseteq V \times O$, $E_2 \subseteq O \times V$. E_1 представляє умову, що лише деякі ресурси, які зайняв зловмисник, можуть мати докази вторгнення; E_2 показує, що зловмисник може мати деякі ресурси впливу на докази вторгнення.

P – умовний розподіл ймовірності кожного вузла на мережевому графі атак. $P=(P_1 \cup P_2)$, P_1 – умовний розподіл вірогідності вузлів доказів вторгнення, а P_2 – розподіл ймовірності умов ресурсних вузлів. Взагалі, $Pre(x)$ – це множина батьківських вузлів X, а $Con(x)$ – набір дочірніх вузлів вузлів X. Для повноти мережевого графу атак слід враховувати оператори AND та OR між різними вузлами. Існують різні оператори AND та OR між різними вузлами $Pre(x)$, і між різними вузлами $Pre(v_i)$, зокрема:

оператор AND між різними вузлами $Pre(o_i)$ показує, що як тільки зловмисник одночасно займає декілька ресурсів, він може здійснити подальшу атаку, додати нові докази вторгнення та зайняти більше ресурсів;

оператор OR між різними вузлами $Pre(o_i)$ показує, що доки зловмисник займає будь-який ресурс, він може здійснити подальшу атаку, додати нові докази вторгнення та зайняти більше ресурсів;

оператор AND між різними вузлами $Pre(v_i)$ показує, що якщо зловмисник хоче досягти наступного вузла ресурсу, він повинен заповнити всі докази вторгнення кожного батьківського вузла;

оператор OR між різними вузлами $Pre(v_i)$ показує, якщо зловмисник заповнив докази вторгнення будь-якого батьківського вузла, зловмисник може зайняти вузол ресурсу.

Згідно з наведеними вище визначеннями, мережевий граф атаки може мати вигляд, показаний на рис. 2:

спрямовані ребра представляють взаємозв'язок між ресурсами, якими володіє зловмисник, та доказами вторгнення, а основна структура мережевого графа атаки формується з урахуванням усіх видів ситуацій. v_1, v_2 і v_3 – початкові вузли, v_7 – цільовий вузол. Є три способи, якщо зловмисник хоче зайняти v_7 (символ ∧ це оператор AND між різними вузлами):

1. $(v_1 \wedge v_2) \rightarrow o_1 \rightarrow v_4 \rightarrow o_3 \rightarrow v_7$;
2. $v_3 \rightarrow o_2 \rightarrow v_5 \rightarrow o_3 \rightarrow v_7$;
3. $((v_1 \wedge v_2 \rightarrow o_1) \wedge (v_3 \rightarrow o_2)) \rightarrow v_6 \rightarrow o_4 \rightarrow v_7$.

Для більш чіткого взаємозв'язку між вузлами у мережевому графі атаки вводиться відношення порядку шляхів між вузлами, що є процесом формування шляху атаки.

По-перше, слід знайти частковий порядок мережевого графа атаки. Тут вводиться поняття *вхідного ступеня* та *вихідного ступеня* вузла. У спрямованому графі кількість ребер,

© Кожухівський, А. Д., & Коровайченко, Ю. Ю. (2023). Методика прогнозування ймовірності інсайдерської атаки на основі аналізу Байєсівських мереж. Сучасний захист інформації, 4(56), 33–41. https://doi.org/10.31673/2409-7292.2023.030404.

що прямують до вузла, називається вхідним ступенем вузла, а кількість ребер, що виходять із вузла, – вихідним ступенем вузла. Наприклад, на рис. 2, вхідний ступінь o_1 дорівнює 2, вихідний ступінь дорівнює 2, вхідний ступінь v_1 дорівнює 0, вихідний ступінь дорівнює 1. В процесі оцінки відношення часткового порядку між вузлами, вибір шляху буде зроблений відповідно до вхідного та вихідного ступенів вузла: спочатку виявлення вузла m із значенням вхідного ступеня дорівнює 0, потім обрізання спрямованих ребер, пов'язаних з вузлом m, якщо спрямовані ребра асоціюються з іншим вузлом n, записується відношення часткового порядку $<m, n>$ між вузлом m і вузлом n. Таким чином, як було зазначено вище, усі відношення часткового порядку між вузлами на мережевому графі атак можна визначити. У частково впорядкованій множині видаляють спрямовані дуги, які будуть обрізані.

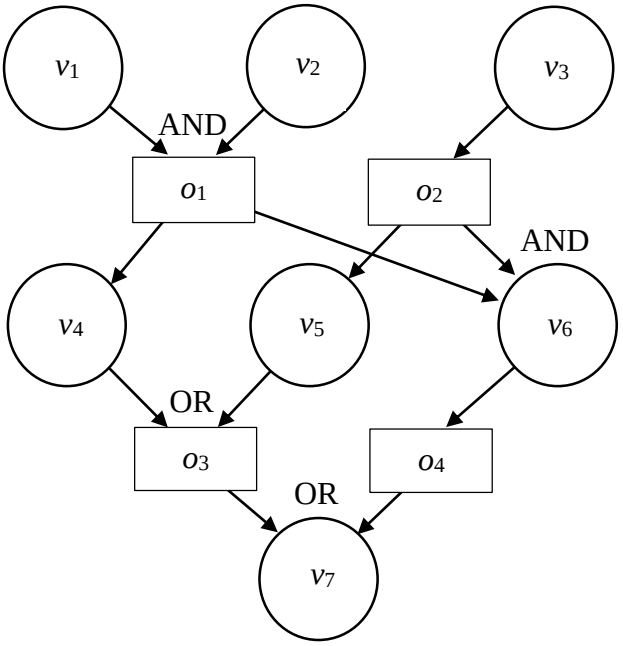

Рис. 2. Мережевий граф атаки

Частково упорядковані множини (*POS*) між вузлами без оператора AND можуть бути одержані у вигляді:

POS_1={<v_1,o_1>,<o_1,v_4>,<v_4,o_3>,<o_3,v_7>}	POS_2= {<v_2,o_1>,<o_1,v_4>,<v_4,o_3>,<o_3,v_7>}
POS_3={<v_1,o_1>,<o_1,v_6>,<v_6,o_4>,<o_4,v_7>}	POS_4= {<v_2,o_1>,<o_1,v_6>,<v_6,o_4>,<o_4,v_7>}
POS_5={<v_3,o_2>,<o_2,v_5>,<v_5,o_3>,<o_3,v_7>}	POS_6= {<v_3,o_2>,<o_2,v_6>,<v_6,o_4>,<o_4,v_7>}

На графі між v_1 і v_2, а також між o_1 і o_2 є оператор AND, який представляє ситуацію, коли обидва вузли зайняті зловмисником і може бути сформоване відношення часткового порядку з наступним вузлом. Отже, вдосконалена множина часткових порядків утворює множину послідовностей шляхів, а множина послідовностей шляхів мережевого графа атак може бути показана наступним чином:

$STEP_1$= {<{v_1,v_2},o_1>,<o_1,v_4>,<v_4,o_3>,<o_3,v_7>};

$STEP_2$= {<{<{v_1,v_2},o_1>,<v_3,o_2>},v_6>,<v_6,o_4>,<o_4,v_7>};

$STEP_3$= {<v_3,o_2>,< o_2,v_5>,<v_5,o_3>,<o_3,v_7>}.

Якщо порівняти $STEP_1$, $STEP_2$ і $STEP_3$ з трьома шляхами на вищезгаданому мережевому графі атак, можна побачити, що лінія відношення порядку узгоджується з можливим шляхом атаки.

© Кожухівський, А. Д., & Коровайченко, Ю. Ю. (2023). Методика прогнозування ймовірності інсайдерської атаки на основі аналізу Байєсівських мереж. Сучасний захист інформації, 4(56), 33–41. https://doi.org/10.31673/2409-7292.2023.030404.

Розрахунок мережевої Байєсівської моделі

Розглянемо окрему операцію, яка полягає у послідовній вибірці вузлів у мережевому графі атаки відповідно до відношення часткового порядку. У процесі вибірки, якщо змінна є змінною інформації доказу, яка вже відома, то вибірка шляхом розподілу $p(X)$ і встановлення результату вибірки як змінної доказів спостереження. Якщо вибіркова змінна не є змінною доказів, то вибірка шляхом розподілу $p(X|\pi(X))$, а результат вибірки є значенням вибірки. Алгоритм, зважений за вірогідністю, не витрачає жодної вибірки, і кожен результат вибірки доказової змінної відповідає значенню змінної доказу апостеріорного розподілу ймовірності, так що кожна вибірка повинна відігравати свою роль.

Формула розрахунку апостеріорної ймовірності:

$$P(Q=q/E=e)\approx\frac{\sum P(E=e/Q=q)}{\sum P(E=e)}, \tag{1}$$

де $\sum P(E=e/Q=q)$ – сума ймовірностей $E=e$ за умови, що $Q=q$;

$\sum P(E=e)$ – сума ймовірностей $E=e$.

Через оператори AND та OR між вузлами у Байєсівському мережевому графі атак порядок топології буде впливати на вузли при обчисленні зваженої ймовірності, тому пропонуються вдосконалені алгоритми 1 та 2 обчислення зваженої ймовірності.

Алгоритм 1: Визначення зважених ймовірностей (*NAG*, *m*, *E*, *e*, *Q*, *q*)

На основі Байєсівського графу мережевих атак, відомих значень змінних доказів, апостеріорний розподіл ймовірності атаки може бути знайдений наступним чином.

Вхідні дані: Байєсівський мережевий граф атаки (NAG), зразок *m*, змінна доказу *E*, значення доказової змінної *e*, змінна запиту *Q*, значення змінної запиту *q*.

Результат: апроксимація $p(Q=q|E=e)$

1. $A\leftarrow$STEP(*NAG*,*D*);
2. $\omega_e\leftarrow 0$; $\omega_{q,e}\leftarrow 0$;
3. for (i=1 to m)
4. $D_i\leftarrow 0$;
5. for (для всіх X з A)
6. if ($X\in E$)
7. $x\leftarrow$ спостережуване значення з X;
8. else
9. $x\leftarrow$ результат вибірки $P(X|\pi(X))$;
10. end if
11. end for
12. $D_i\leftarrow D_i\cup\{X=x\}$;
13. $\omega_i\leftarrow\prod_{X\in E} P(X|\pi(X))|D_i$
14. $\omega_e\leftarrow\omega_e+\omega_i$;
15. if (D відповідає $D=q$)
16. $\omega_{q,e}\leftarrow\omega_{q,e}+\omega_i$;
17. end if
18. end for
19. return $\omega_{q,e}\ /\ \omega_e$

Алгоритм 2: Визначення відношення часткового порядку STEP(*NAG*, SETP_i).

Згідно з Байєсівським мережевим графом атаки (*NAG*), можна дізнатись множину вузлів упорядкованого шляху атаки *D*.

© Кожухівський, А. Д., & Коровайченко, Ю. Ю. (2023). Методика прогнозування ймовірності інсайдерської атаки на основі аналізу Байєсівських мереж. Сучасний захист інформації, 4(56), 33–41. https://doi.org/10.31673/2409-7292.2023.030404.

Вхідні дані: мережевий граф атаки (*NAG*), вхідний ступінь, вихідний ступінь, відношення часткового порядку (POS), відношення порядку рядків STEP, довільні вузли *X* та *Y*, множина *M* із оператором AND.

1. Вихідні дані: набір вузлів із відношенням порядку рядків Байєсівської мережі.
2. *POS* ←∅; POS_i ←∅; SETP_i ←∅; *M*←∅;
3. for（кожна змінна вузла *X* з λ_1=0;
4. Усі змінні вузлів *Y* які мають прямий зв'язок з вузлом *X* у *NAG* повинні бути знайдені;
5. If (вихідний ступінь *Y*>1, і 2 приєднані вузли до *Y* є оператором AND.
6. *M*←*M*∪{ $X_1 \wedge X_2$ };
7. end if;
8. *POS*←*POS*∪{<*X*,*Y*>};
9. λ_2 (вихідний ступінь *X*) ← 0;
10. end for;
11. У множині POS, усі множини часткового порядку POS_i незалежно від оператора AND мають бути визначені.
12. У множині POS_i, усі множини послідовностей рядків $SETP_i$ з операторами AND слід визначити.
13. return $SETP_i$.

Моделювання застосування мережевої Байєсівської моделі

Для перевірки достовірності запропонованої методики прогнозування інсайдерської атаки розглянемо приклад, наведений на рис. 2. Дослідження будемо проводити шляхом моделювання методом Монте-Карло, для чого встановимо, що змінні визначаються за допомогою генератора випадкових чисел. Наприклад, для випадкової змінної *X*, яка може набувати значень 1 або 0, ймовірність $P(X=0)=p$, а $P(X=1)=1-p$. Процес отримання ймовірностей *P* наступний: дійсне число *x*, яке лежить у проміжку [0, 1], генерується генератором випадкових чисел. Якщо значення *x* попадає до проміжку [0, *p*], то тоді значення *X* = 0, у протилежному випадку *X* = 1.

Для моделювання будемо застосовувати наступний алгоритм.

Алгоритм 3. Визначення частоти та ймовірності реалізації інсайдерської атаки.

1. *n* ← визначення кількості випробувань;
2. *m* ← визначення кількості кроків випробувань;
3. $N = Table\left[0,\{10\},\{m\}\right]$ – визначення початкового масиву кількості успішних атак;
4. $P = Table\left[0,\{10\},\{m\}\right]$ – визначення початкового масиву ймовірності успішних атак;
5. $Do\left[$
6. $p=\frac{d_i}{10};\ i=0;\ j=0;\ k=IntPart\left[\frac{n}{m}\right];\ d_j=1;$ – початкові значення змінних;
7. $While[i \le n,$ – цикл обчислення кількості та ймовірності успішних атак;
8. $i=i++;$
9. $If\left[\left(\left(Rnd[]\le p\right)\wedge\left(Rnd[]\le p\right)\right)\vee\left(Rnd[]\le p\right)\vee\left(\left(\left(Rnd[]\le p\right)\wedge\left(Rnd[]\le p\right)\right)\wedge\left(Rnd[]\le p\right)\right),$
10. $If\left[\left(Rnd[]\le p\right),\right.$
11. $If\left[\left(Rnd[]\le p\right), j=j++\right]$
12. $\left.\right]$
13. $\left.\right];$ – кінець роботи циклу *While*;

© Кожухівський, А. Д., & Коровайченко, Ю. Ю. (2023). Методика прогнозування ймовірності інсайдерської атаки на основі аналізу Байєсівських мереж. Сучасний захист інформації, 4(56), 33–41. https://doi.org/10.31673/2409-7292.2023.030404.

14. $If\left[i == k, N_{d_i,d_j} = j; P_{d_i,d_j} = \frac{j}{k}; d_j = d_j ++; k = k + IntPart\left[\frac{n}{m}\right]\right];$
15. $\Big]$,
16. $\{d_i, 1, 10\}\Big]$; – кінець роботи циклу Do;
17. $Return[N]$ – результати кількості успішних атак;
18. $Return[P]$ – результати ймовірності успішних атак.

На рис. 3. наведено результати моделювання за кількістю успішних атак. Початкові дані: кількість випробувань – 10000; кількість кроків випробувань – 10. Як бачимо, зі збільшенням числа випробувань та початкової ймовірності проникнення до ресурсу (окремого вузла мережі) загальна кількість проникнень збільшується. У граничному випадку, коли початкова ймовірність дорівнює 1, а кількість кроків максимальна, кількість успішних атак досягає максимуму 10000.

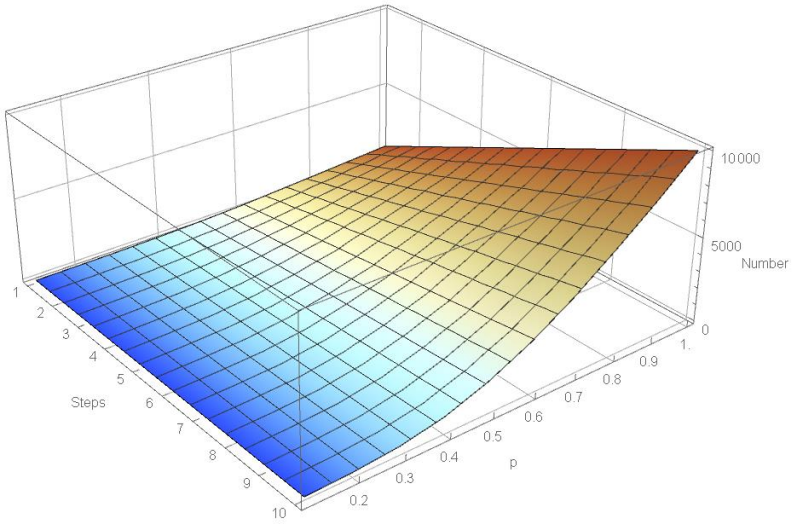

Рис. 3. Результати моделювання за кількістю успішних проникнень до вузла 7.

На рис. 4 наведено результати моделювання за тих самих умов, що і на рис. 3.

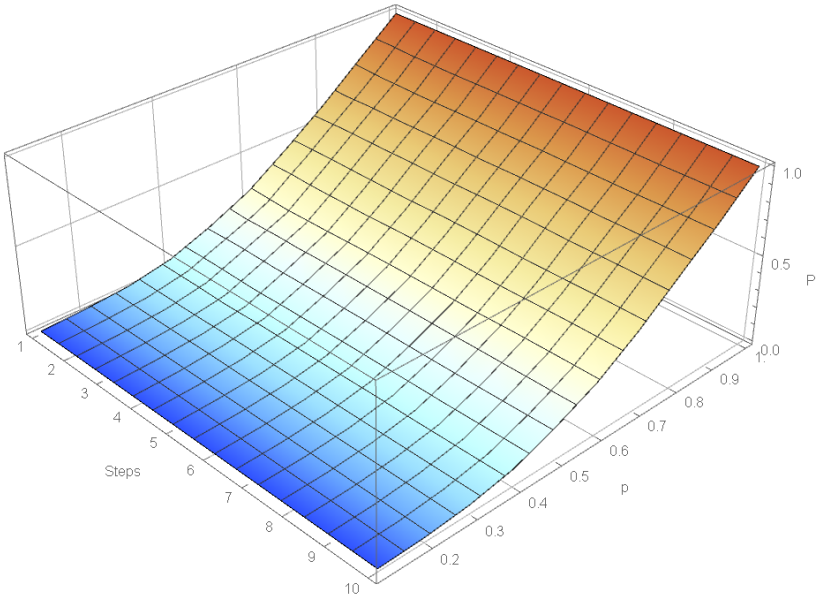

Рис. 4. Результати моделювання ймовірності проникнення до вузла 7.

© Кожухівський, А. Д., & Коровайченко, Ю. Ю. (2023). Методика прогнозування ймовірності інсайдерської атаки на основі аналізу Байєсівських мереж. Сучасний захист інформації, 4(56), 33–41. https://doi.org/10.31673/2409-7292.2023.030404.

Як бачимо, збільшення початкової ймовірності проникнення до ресурса (окремого вузла мережі) дає збільшення загальної ймовірності проникнення до вузла 7. У граничному випадку, коли початкова ймовірність дорівнює 1, загальна ймовірність також прямує до 1. Разом з тим, при такій кількості випробувань (10000) результат майже не залежить від поточного кроку випробувань і загальна ймовірність залишається сталою.

Таким чином, можна зробити висновок, що забезпечення ефективного захисту найбільш важливих ресурсів організації, доступ до яких здійснюється через інші ресурси (вузли), цілком залежить від ефективності захисту окремих вузлів, навіть якщо їх важливість не є надто високою.

Висновок

Інсайдерська загроза залишається однією з найсерйозніших проблем, з якими сьогодні стикаються підприємства. Інсайдери мають набагато більші можливості, ніж зовнішні зловмисники, тому вони можуть легко обходити сигналізації внутрішньої безпеки, різні брандмауери, системи виявлення вторгнень та контроль доступу та, нарешті, успішно реалізувати поведінку атак. Дослідження інсайдерської загрози все ще перебуває на первинному етапі і на сьогоднішній день практично немає ефективних методів боротьби з такою загрозою. Байєсівська мережа вирішує головним чином проблему невизначеності, з огляду на те, що фактори внутрішньої загрози є складними та невизначеними. Отже, мережева структура внутрішньої загрози, яка описана в Байєсівською моделлю, може бути використана для обчислення загальної вірогідності інсайдерських атак. Результати моделювання, наведені в цій роботі, можуть достатньо точно і ефективно передбачити таку загрозу.

Перелік посилань

1. Xie, Peng & Li, Jason & Ou, Xinming & Liu, Peng & Levy, Renato. (2010). Using Bayesian Networks for Cyber Security Analysis. Proceedings of the International Conference on Dependable Systems and Networks. 211-220. 10.1109/DSN.2010.5544924.

2. Davide Cerotti and Daniele Codetta Raiteri and Giovanna Dondossola and Lavinia Egidi and Giuliana Franceschinis and Luigi Portinale and Roberta Terruggia. A Bayesian Network Approach for the Interpretation of Cyber Attacks to Power Systems. 2019, Italian Conference on Cybersecurity. https://api.semanticscholar.org/CorpusID:59615894

3. Wang, Jiali & Neil, Martin & Fenton, Norman. (2019). A Bayesian Network Approach for Cybersecurity Risk Assessment Implementing and Extending the FAIR Model. Computers & Security. 89. 101659. 10.1016/j.cose.2019.101659.

4. Matteo Iaiani, Alessandro Tugnoli, Valerio Cozzani, Genserik Reniers, Ming Yang, A Bayesian-network approach for assessing the probability of success of physical security attacks to offshore Oil&Gas facilities, Ocean Engineering, Volume 273, 2023, 114010, ISSN 0029-8018, https://doi.org/10.1016/j.oceaneng.2023.114010.

5. Jinsoo Shin, Hanseong Son, Rahman Khalil ur, Gyunyoung Heo, Development of a cyber security risk model using Bayesian networks, Reliability Engineering & System Safety, Volume 134, 2015, Pages 208-217, ISSN 0951-8320, https://doi.org/10.1016/j.ress.2014.10.006.

6. Żebrowski, P., Couce-Vieira, A., Mancuso, A. (2022). A Bayesian Framework for the Analysis and Optimal Mitigation of Cyber Threats to Cyber-Physical Systems. Risk Analysis, 42, 2275–2290. https://doi.org/10.1111/risa.13900

7. Niamat Ullah Ibne Hossain, Morteza Nagahi, Raed Jaradat, Chiranjibi Shah, Randy Buchanan, Michael Hamilton. Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: a system of systems problem. ournal of Computational Design and Engineering, Volume 7, Issue 3, June 2020, Pages 352–366, https://doi.org/10.1093/jcde/qwaa029

8. Wang, H., Wang, Y., & Yang, G. (2013). A Predictive Model of Insider Threat Based on Bayesian Network. International Journal of Online and Biomedical Engineering (iJOE), 9(S4), pp. 69–74. https://doi.org/10.3991/ijoe.v9iS4.2660.

Надійшла: 17.10.2023 Рецензент: д.т.н., с.н.с. Лаптєв О.А.

© Кожухівський, А. Д., & Коровайченко, Ю. Ю. (2023). Методика прогнозування ймовірності інсайдерської атаки на основі аналізу Байєсівських мереж. Сучасний захист інформації, 4(56), 33–41. https://doi.org/10.31673/2409-7292.2023.030404.