УДК 004.72.056.52:004.4
DOI: 10.31673/2409-7292.2024.010008

**Пепа Ю. В., Хорошко В. О.,
Хохлачова Ю. Є., Аль-Далваш А.**

МЕТОДИКА АНАЛІЗУ ТА ОЦІНКИ ЗАХИЩЕНОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ З УРАХУВАННЯМ СТУПЕНЯ ПЕРЕКРИТТЯ ЗАГРОЗ

У даний час захист інформації в автоматизованих системах став невід'ємною частиною переважної більшості діяльності різноманітних галузей людської діяльності. В статті розглянуто вплив загроз на об'єкти, що підлягають захисту. Основна увага приділена аналізу основних випадків впливу загроз та реакції захисних механізмів на зовнішнє втручання. Причому система захисту розглядається в комплексі, як декілька захисних механізмів з можливими взаємозв'язками і власною ефективністю протидії на певні види загроз. Архітектура системи захисту має недосконаліть і пропускає деякі загрози на області захисту, що створює небезпеку для інформації. На підставі аналізу основних можливих випадків запропоновано модель системи захисту інформації з повним перекриттям загроз, яка дозволяє враховувати внутрішні взаємозв'язки загроз, власне архітектуру системи захисту та можливих об'єктів захисту, а також дозволяє розкрити структуру системи захисту інформації, провести оцінку ефективності роботи її бар'єрів на відомі види загроз або їх комбінації. Авторами проведено кількісна оцінка оптимальних ймовірностей захисних механізмів, які дозволяють забезпечити найменший пропуск загроз на області захисту. На відміну від відомих моделей модель процесу захисту інформації з повним перекриттям загроз дозволяє враховувати внутрішні взаємозв'язки загроз, системи захисту інформації та об'єктів захисту, а також дозволяє розкрити структуру системи, виділити та оцінити ефективність роботи бар'єрів, що перекривають області вразливостей механізмів захисту інформації.

Ключові слова: бар'єр захисту, матриця загроз, область захисту, функціональний зв'язок, стійкість.

Вступ

У даний час захист інформації в автоматизованих системах став невід'ємною частиною переважної більшості діяльності різноманітних галузей людської діяльності. Аналіз великих систем різної природи та архітектури, а також управління процесами захисту інформації, їхнього функціонування знаходяться серед нагальних задач, що стоять перед спеціальностями, які проектують та експлуатують ці системи. Одним з підходів до вирішення зазначених задач є побудова та дослідження моделей захисту інформації, як основного об'єкту дослідження на етапі проектування різноманітних систем з вбудованим механізмом захисту інформації.

Аналіз публікацій

Ще на етапі раннього проектування велика кількість дослідників ставила перед собою мету абстрактного осмислення майбутньої системи захисту інформації (СЗІ) в залежності від цілей, задач, місця та обстановки, в якій вони будуть функціонувати [1-4]. Для цього дуже важливо розібратися в існуючих підходах побудови моделей захисту. При цьому основне призначення моделей полягає у створенні передумов для об'єктивної оцінки загального стану інформаційної системи з точки зору міри вразливості або рівня захищеності інформації в ній. Необхідність в таких оцінках зазвичай виникає при аналізі загальної ситуації з метою вироблення стратегічних рішень при організації захисту інформації.

З аналізу моделей захисту інформації найбільш повно описує СЗІ модель захисту інформації з повним перехрестям загроз [3, 6]. В цій моделі вважається, що кожній загрозі в СЗІ протистоїть будь-який механізм захисту. Таким чином, побудована за цим принципом СЗІ не дозволяє впливати загрозам на області, що захищаються. Однак такий підхід не розкриває внутрішніх зв'язків у самій СЗІ, що призводить до помилок під час проектування та розробки СЗІ. У зв'язку з цим, виникає об'єктивна необхідність аналізу процесів захищеності інформації в автоматизованих системах.

Мета статті – оцінити стійкість бар'єрів СЗІ та запропонувати модель захисту інформації з повним перекриттям загроз, яка враховує внутрішні взаємозв'язки загроз та структуру СЗІ.

Основна частина

Для подальшого розгляду процесу захищеності системи необхідно проаналізувати внутрішні взаємозв'язки в самій системі захисту.

У механізмах захисту СЗІ існують наступні області:

1. Області вразливості СЗІ **V**, на які впливають загрози для СЗІ.

2. Бар'єри захисту **B**, які встановлюються у СЗІ для блокування загроз, які впливають на області вразливості СЗІ.

У цьому випадку СЗІ розглядається як сукупність областей вразливостей СЗІ і бар'єрів, блокуючих ці небезпеки, з точки зору, критеріїв безпеки інформації.

Простежимо у запропонованій моделі [3, 4] процес впливу загроз на області, що захищаються. Для цього розглянемо крайні випадки роботи системи, яка має область загроз, області вразливості СЗІ, область бар'єрів і область, що підлягатиме захисту.

Випадок 1.

Умови. Необхідно проаналізувати роботу системи при впливі на неї різних загроз «за відсутності бар'єрів» у СЗІ (бар'єри не затримують загрози). Тобто необхідно простежити шляхи впливу загроз на області, що захищаються відповідно до рис. 1.

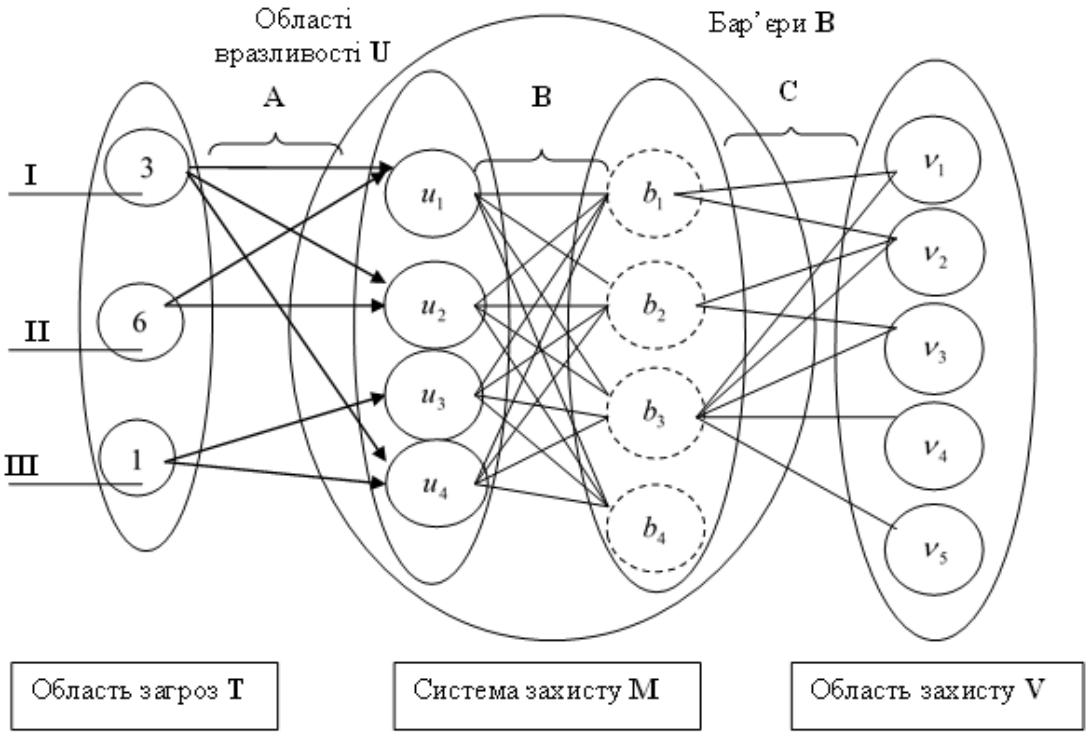

Рис. 1. Приклад процесу впливу загроз на область, яка підлягає захисту

На СЗІ впливає три типи загроз **T**, які поділяються на атаки, відмови та аварії, які властиві будь-якій автоматизованій системі. Ці загрози по різному впливають на ділянці вразливості СЗІ (область **A** на рис. 1). У СЗІ з повним перекриттям кожну область уразливості перекриває повний набір бар'єрів. Бар'єри СЗІ не затримують бар'єри, тобто для загроз розглядається максимальна кількість шляхів впливу загроз (область **B** на рис. 1). СЗІ захищає конкретні області – **V** (область виходи загроз із СЗІ до областей, що захищаються – **C**).

1. Визначимо порядок розподілу загроз по областях вразливості:

$$\mathbf{X} = (\mathbf{AT}),$$

де **X** – кількісна матриця впливів загроз на виході областей вразливості СЗІ; **A** – матриця впливу загроз на СЗІ; **T** – кількісна матриця загроз впливу:

© Пепа, Ю. В., Хорошко, В. О., Хохлачова, Ю. Є., & Аль-Далваш, А. (2024). Методика аналізу та оцінки захищеності систем захисту інформації з урахуванням ступеня перекриття загроз. Сучасний захист інформації, 1(57), 69–76. https://doi.org/10.31673/2409-7292.2024.010008.

$$\begin{vmatrix}1&1&0\\1&1&0\\0&0&1\\1&0&1\end{vmatrix}\times\begin{vmatrix}3\\6\\1\end{vmatrix}=\begin{vmatrix}9\\9\\1\\4\end{vmatrix}.$$

2. Визначимо порядок проходу загроз через СЗІ:

$$\mathbf{Y}=\left(\mathbf{BX}\right), \tag{1}$$

де **Y** – кількісна матриця проходу загроз через СЗІ; **B** – матриця функціональних залежностей всередині СЗІ:

$$\begin{vmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{vmatrix}\times\begin{vmatrix}9\\9\\1\\4\end{vmatrix}=\begin{vmatrix}23&23&23&23\end{vmatrix}.$$

Очевидно, що матриця **B** матиме по стовпцях і рядках одиницю (наявність шляху впливу загрози) у разі, коли кожну область вразливості перекривають всі наявні «умовні бар'єри». В цьому випадку на виході небезпеки рівномірно розподілятися на всіх шляхах.

3. Визначимо кількості загроз, що впливають на області, що захищаються:

$$\mathbf{Z}=\left(\mathbf{YC}\right), \tag{2}$$

де **Z** – кількісна матриця впливів загроз на області системи, що захищаються; **C** – матриця впливу загроз на області, що захищаються:

$$\begin{vmatrix}23&23&23&23\end{vmatrix}\times\begin{vmatrix}1&1&0&0&0\\0&1&1&0&0\\1&1&0&0&1\\0&0&1&1&0\end{vmatrix}=\begin{vmatrix}46\\69\\46\\23\\23\end{vmatrix}.$$

Заключний вираз для визначення шляхів впливу загроз на області, що захищаються, матиме вигляд:

$$\mathbf{Z}=\mathbf{C}\left(\mathbf{B}\left(\mathbf{AT}\right)\right). \tag{3}$$

Вираз (3) є показником, що визначає виконання умови забезпечення захисту об'єкта за наявності загрози t_i [2, 3]. З останнього матричного виразу для визначення шляхів впливу загроз на області, що захищаються, можна зробити висновок, що необхідно звернути увагу на шляхи максимального впливу загроз на області, що захищаються, (в нашому випадку – максимальна кількість загроз припала на 1, 2 і 3 області, що захищаються – див. рис. 2).

Для вирішення цієї проблеми розглянемо наступний випадок.

© Пепа, Ю. В., Хорошко, В. О., Хохлачова, Ю. Є., & Аль-Далваш, А. (2024). Методика аналізу та оцінки захищеності систем захисту інформації з урахуванням ступеня перекриття загроз. Сучасний захист інформації, 1(57), 69–76. https://doi.org/10.31673/2409-7292.2024.010008.

Випадок 2.

Умови. Необхідно проаналізувати роботу системи при впливі на неї різних загроз за наявності бар'єрів, що мають різні показники стійкості [4]. Тобто потрібно оцінити роботу СЗІ за умов нестабільності бар'єрів згідно з рис. 3.

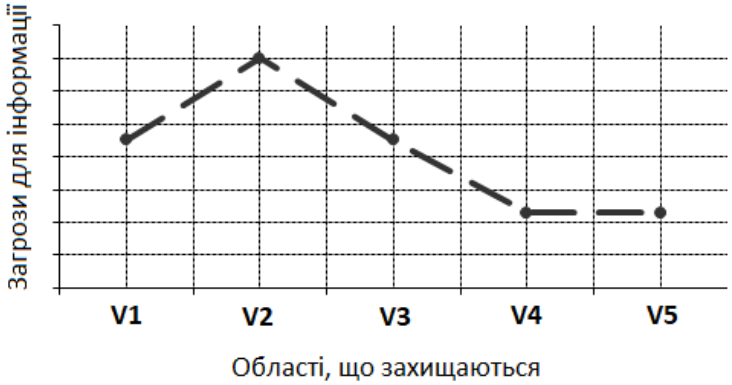

Рис. 2. Аналіз шляхів впливу загроз на області, що захищаються

Надалі умови щодо впливу загроз збігаються з випадком 1. У СЗІ області вразливості перекриваються кількома бар'єрами з їхньої загальної сукупності. Бар'єр b_1 може пропустити загрозу з ймовірністю $p_{b_1} = 0,2$. Бар'єр b_2 – з ймовірністю $p_{b_2} = 0,4$, а наступні бар'єри: $p_{b_3} = 0,1$, $p_{b_4} = 0,3$. Надалі умови збігаються з випадком 1.

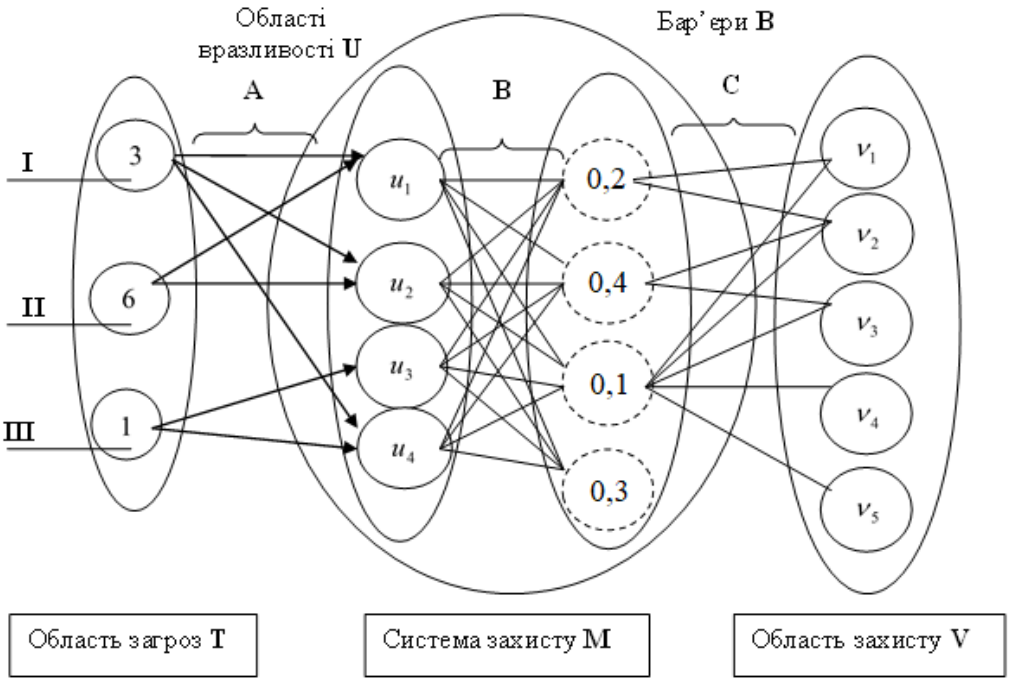

Рис. 3. Приклад процесу впливу загроз на область,
що захищається за наявності нестабільних бар'єрів у СЗІ

Обчислення:

1. Етап 1 з обчислення повторюється. На виході областей уразливості буде наступна кількісна матриця розподілених загроз по областям уразливості:

$$\begin{vmatrix}1 & 1 & 0\\ 1 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 1\end{vmatrix} \times \begin{vmatrix}3\\ 6\\ 1\end{vmatrix} = \begin{vmatrix}9\\ 9\\ 1\\ 4\end{vmatrix}.$$

2. Визначимо порядок проходу загроз через СЗІ.
Відповідно до (1) визначимо матрицю **B** та наявність загроз на виході СЗІ:

$$\begin{vmatrix}0{,}2 & 0{,}4 & 0{,}1 & 0{,}3\\ 0{,}2 & 0{,}4 & 0{,}1 & 0{,}3\\ 0{,}2 & 0{,}4 & 0{,}1 & 0{,}3\\ 0{,}2 & 0{,}4 & 0{,}1 & 0{,}3\end{vmatrix} \times \begin{vmatrix}9\\ 9\\ 1\\ 4\end{vmatrix} = \begin{vmatrix}6{,}7 & 6{,}7 & 6{,}7 & 6{,}7\end{vmatrix}.$$

Через усі бар'єри СЗІ проходить приблизно 7 загроз.
4. Відповідно до (2) отримуємо:

$$\begin{vmatrix}7 & 7 & 7 & 7\end{vmatrix} \times \begin{vmatrix}1 & 1 & 0 & 0 & 0\\ 0 & 1 & 1 & 0 & 0\\ 1 & 1 & 0 & 0 & 1\\ 0 & 0 & 1 & 1 & 0\end{vmatrix} = \begin{vmatrix}14\\ 21\\ 14\\ 7\\ 7\end{vmatrix}.$$

На рис. 4 показано вплив загроз на об'єкти, що захищаються.

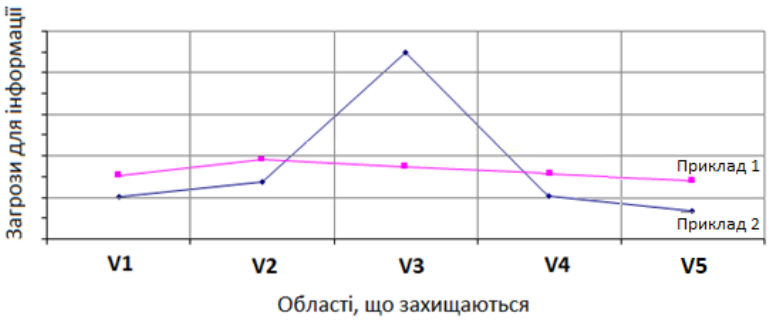

Рис. 4. Аналіз захисту СЗІ областей, що захищаються
при збільшенні стійкості захисту бар'єрів

З рис. 4 видно, що найбільш уразливі 1, 2 і 3 області, що захищаються, але кількість загроз, що впливають на ці області, зменшилася. Необхідно звернути увагу на надійність бар'єрів, через які надходять загрози на ці області.

Випадок 3.

Умови. Необхідно проаналізувати роботу СЗІ при впливі на неї різних загроз за умови, що бар'єри повністю блокують загрози. Тобто необхідно простежити роботу ідеальної СЗІ згідно з рис. 1.

Обчислення:

1. Етап 1 розв'язання задачі такий самий, як і у випадку 1.

© Пепа, Ю. В., Хорошко, В. О., Хохлачова, Ю. Є., & Аль-Далваш, А. (2024). Методика аналізу та оцінки захищеності систем захисту інформації з урахуванням ступеня перекриття загроз. Сучасний захист інформації, 1(57), 69–76. https://doi.org/10.31673/2409-7292.2024.010008.

2. Визначимо порядок проходу загроз через СЗІ. На цьому етапі в матриці враховані функціональні зв'язки в СЗІ, а цифра 1 буде показувати, як бар'єри пропускають загрозу, цифра 0 – відповідно не пропускають загрозу. У цьому випадку матриця і результат на виході СЗІ будуть мати вигляд:

$$\begin{vmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{vmatrix} \times \begin{vmatrix} 9 \\ 9 \\ 1 \\ 4 \end{vmatrix} = \begin{vmatrix} 0 & 0 & 0 & 0 \end{vmatrix}.$$

3. На цьому етапі можна сказати, що результуючим показником кількості загроз в областях, що захищаються, буде нуль:

$$\begin{vmatrix} 0 & 0 & 0 & 0 \end{vmatrix} \times \begin{vmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{vmatrix} = \begin{vmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{vmatrix}.$$

На рис. 5 показано роботу СЗІ з повним перекриттям загроз.

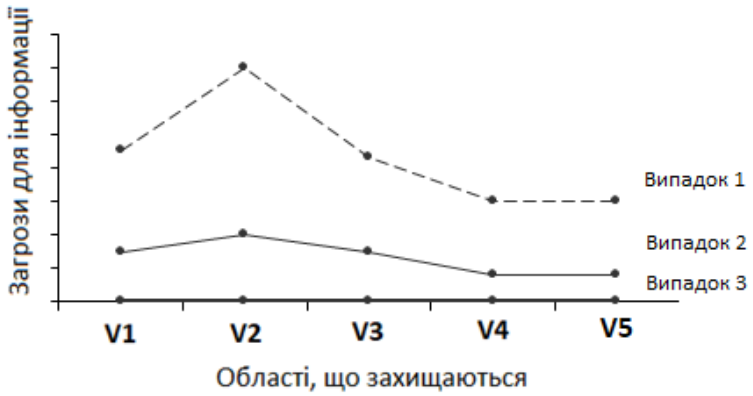

Рис. 5. Аналіз роботи СЗІ з повним перекриттям загроз
зі збільшенням стійкості бар'єрів

Як видно з рис. 5 збільшення надійності бар'єрів СЗІ призвело до блокування загроз на рівні СЗІ. Для оцінки системи на етапі проектування необхідно знати, наскільки бар'єри СЗІ здатні виконувати покладені на них функції залежно від впливу на них різних загроз [2]. Для цього розглянемо наступний випадок. Для ускладнення завдання послабимо живучість СЗІ, для чого зменшимо кількість взаємних зв'язків у СЗІ.

Випадок 4.

Умови: Відповідають випадку 3. Зменшено кількість функціональних зв'язків у СЗІ. Завдання таке ж як і у випадку 3. Необхідно проаналізувати роботу системи при впливі на неї різних загроз за наявності бар'єрів, що мають різні показники стійкості і мають різні взаємозв'язки з областями вразливості СЗІ (при цьому прибрано по одному зв'язку бар'єра з областю вразливості). Тобто необхідно оцінити роботу СЗІ в умовах нестабільності бар'єрів та зменшеній кількості функціональних зв'язків усередині СЗІ згідно з рис. 3.

Ймовірність пропуску бар'єрами загроз збігаються з умовами випадку 2.

Обчислення:

1. Етап 1 збігається з попередніми випадками. На виході областей вразливості буде наступна кількісна матриця розподілених загроз по областям вразливості:

$$\begin{vmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{vmatrix} \times \begin{vmatrix} 3 \\ 6 \\ 1 \end{vmatrix} = \begin{vmatrix} 9 \\ 9 \\ 1 \\ 4 \end{vmatrix}.$$

2. Визначимо порядок проходу загроз через СЗІ.

Відповідно до (1) визначимо матрицю **B** та наявність загроз на виході СЗІ:

$$\begin{vmatrix} 0{,}2 & 1 & 1 & 0{,}1 \\ 0{,}2 & 1 & 0{,}1 & 1 \\ 1 & 0{,}4 & 1 & 0{,}3 \\ 0{,}2 & 1 & 1 & 0{,}3 \end{vmatrix} \times \begin{vmatrix} 9 \\ 9 \\ 1 \\ 4 \end{vmatrix} = \begin{vmatrix} 12{,}2 & 14{,}9 & 14{,}8 & 13 \end{vmatrix}.$$

Видно, що на виході СЗІ погрози розподілилися по бар'єрах приблизно так:

- через бар'єр 1 проходить 12 загроз;
- через бар'єр 2 проходить 15 загроз;
- через бар'єр 3 проходить 15 загроз;
- через бар'єр 4 проходить 13 загроз.

3. Відповідно до (3) отримуємо:

$$\begin{vmatrix} 12 & 15 & 15 & 13 \end{vmatrix} \times \begin{vmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{vmatrix} = \begin{vmatrix} 27 \\ 42 \\ 28 \\ 13 \\ 15 \end{vmatrix}.$$

На рис. 6 показано зміну стійкості бар'єрів СЗІ.

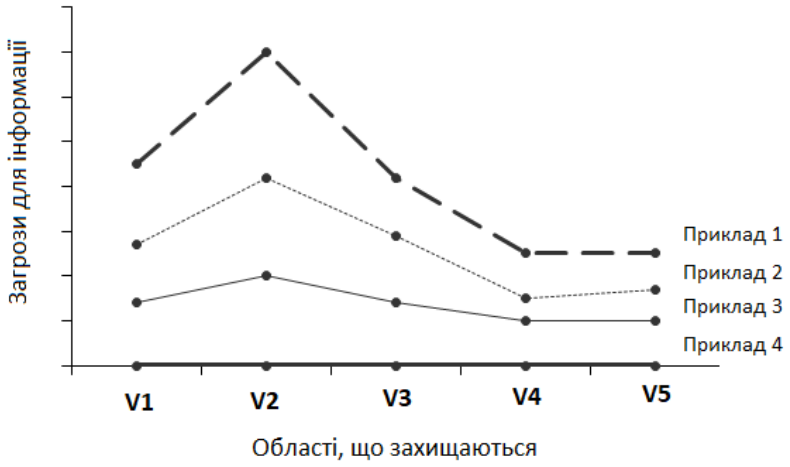

Рис. 6. Аналіз роботи СЗІ за зміни стійкості бар'єрів СЗІ

Як видно з рис. 6, порівняно з випадком 2, кількість загроз збільшилася в залежності від зменшених взаємних зв'язків між бар'єрами. Найбільше збільшення відбулося в області 2, найменше – в області 4.

Розрахунки роботи моделі процесу захисту, наведені у випадках 1 - 4, представлених на рис. 1 - 6, дозволяють зробити такі висновки.

Висновки

Методика аналізу та оцінки захищеності систем з урахуванням ступеня перекриття загроз є важливим інструментом для забезпечення надійного захисту інформації в сучасних інформаційних системах. Використання цієї методики дозволяє визначити потенційні загрози для інформаційної системи та оцінити їх вплив на її безпеку. При використанні методики слід враховувати різноманітність загроз і враховувати їх ступінь ймовірності виникнення. Оцінка ступеня перекриття загроз дозволяє ефективно розподілити ресурси для захисту інформації, фокусуючи увагу на найбільш критичних напрямках.

На відміну від відомих моделей запропонована модель процесу захисту інформації з повним перекриттям загроз дозволяє враховувати внутрішні взаємозв'язки загроз, СЗІ та об'єктів захисту, а також дозволяє розкрити структуру СЗІ, виділити та оцінити ефективність роботи бар'єрів, що перекривають області вразливостей механізмів захисту СЗІ.

При збільшенні стійкості бар'єрів системи захисту **M** кількість минулих загроз в області, що захищаються, зменшується. Але у зв'язку з тим, що бар'єри мають різні характеристики стійкості, за рахунок внутрішніх зв'язків у самій системі захисту відбувається перерозподіл загроз через «слабкі» бар'єри.

Результати аналізу і оцінки можуть бути використані для розробки та впровадження стратегій захисту, що відповідають конкретним потребам та умовам організації. Постійне оновлення методики з урахуванням нових загроз та технологічних розвитків є ключовим аспектом забезпечення ефективного захисту інформації у майбутньому.

Перелік посилань

1. Ланде, Д. В., Субач, І. Ю., Бояринова, Ю. Є. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки. – К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018. – 300 с.

2. Домарєв, В. В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k) [Текст] / В. В. Домарєв, Д. В. Домарєв. – Донецьк: «Велстар», 2012. – 146 с. – ISBN 978-966-2759-00-6.

3. Павлов, І. М., Хорошко, В. О. Проектування комплексних систем захисту інформації. – К.: ВІТІ-ДУІКТ, 2011. – 245 с.

4. Браіловський, М. М., Зибін, С. В., Пискун, І. В. та ін. Технології захисту інформації. – К: ЦП «Компринт», 2021. – 296 с.

5. Козюра, В. Д., Ткач, Ю. М., Шелест, М. Є. та ін. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах. – Ніжин: ФОП Лук'яненко В.В., 2019. – 144 с.

6. Романов, О. І., Ливенцев, С. П., Павлов, І. М. Математична модель захисту інформації в автоматизованих мережах спеціального призначення // Збірник наук. праць ВІТІ НТУУ «КПІ». – Київ, 2004. – № 5. – С. 23-31.

7. Сальник, В.В & Гуж, О.А & Закусіло, В.С & Сальник, С.В & Бєляєв, П.В. (2021). Методика оцінки порушень захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах. Збірник наукових праць Харківського національного університету Повітряних Сил. 77-82. 10.30748/zhups.2021.70.11.

8.Degtyareva L. Аналіз структури системи захисту інформації / L. Degtyareva, MiroshnykovaM., S. Voloshko // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2019. – Т. 2 (54). – С. 78-82. – doi:https://doi.org/10.26906/SUNZ.2019.2.078.

Надійшла 27.01.2024