логику проведения атак, подобных описанным выше, и, соответственно, формализовать правила их обнаружения.

Список литературы
1. http://www.virtualizationsecuritygroup.ru/publikatsii/obnaruzhenie-incidentov.html
2.http://www.virtualizationsecuritygroup.ru/publikatsii/bezopasnost-virtualnih-infrastruktur.html
3. http://www.virtualizationpractice.com

МОДЕЛЮВАННЯ СИСТЕМИ ЗАХИСТУ З ВИКОРИСТАННЯМ МОДЕЛІ ГІПЕРГРАФІВ

Т.В. Бабенко, О.І. Авчиннікова
(Україна, Дніпропетровськ, ДВНЗ «Національний гірничий університет»)

Для математичного моделювання дискретних слабо структурованих процесів та систем, в яких присутня множина критеріїв, стохастичність, інтервальність одним з найбільш підходящих математичних інструментаріїв структурування об'єктів моделювання є інструментарій теорії гіперграфів [4].

Під даний різновид процесів може підпадати процес аналізу захищеності об’єкта інформаційної діяльності, що базується на структуруванні багатьох критеріїв.

Згідно [2,3], гіперграф – це таке узагальнення простого графа, коли ребрами можуть бути не лише двоелементні, а й будь-які підмножини вершин.

Нехай V – кінцева непуста множина, $\mathcal{E}$ – деяке сімейство непустих (необов'язково різних) підмножин множини V. Пара $H = (V, \mathcal{E})$ називається гиперграфом з множиною вершин V та множиною ребер $\mathcal{E}$.

Множину відносин "об'єкт-загроза" можна відтворити за допомогою гіперграфа$H = (O, T)$, рисунок 1, в якому множина вершин $O = \{o_1, \dots, o_5\}$ позначає множину об’єктів захисту, множина ребер $T = \{t_1, \dots, t_8\}$ позначає множину загроз, спрямованих на об’єкт захисту o_i.

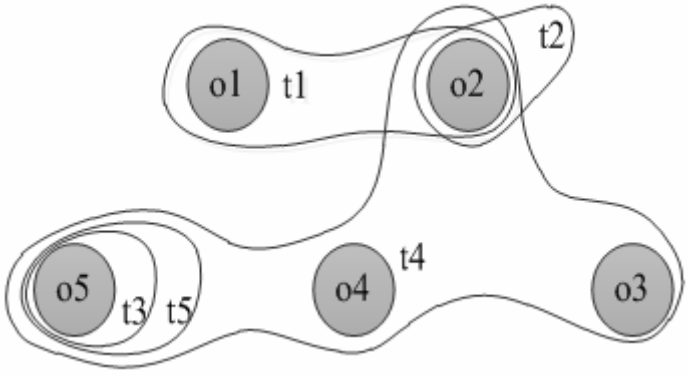
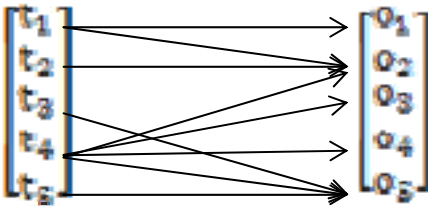


Рис. 1. Гіперграф $H = (O, T)$, діаграма Венна

Використання гіперграфів, як інструменту моделювання, дозволяє систематизовано відобразити сукупність основних факторів впливу на систему захисту автоматизованої системи та їх взаємодію.

Зображення гіперграфу у вигляді діаграми Венна, дивись рисунок 1, є класичним. Така модель достотно візуалізує взаємозв'язок між об'єктами та забезпечує дослідника інформацією, необхідною для розуміння принципів організації автоматизованої системи.

Проте, у багатьох випадках для візуалізації гіперграфа доцільно буде використовувати граф інциденцій чи граф Кеніга [5], дивись рисунок 2 – це дводольний граф $K(H) = (V, \mathcal{E})$ з множиною вершин $(V \cup \mathcal{E})$ та множиною ребер, що їх поєднують якщо в Hвершина vє інцидентною ребру ε.



T O

Рис. 2. Кенігове уявлення гіперграфа $H = (O, T)$

Існує ще один спосіб зображення гіперграфів – у вигляді плоского гіперграфа, рисунок 3.

Для переходу до цього зображення позначимо кожну вершинукругом, а гіперребро – крапкою, що з'єднанаребрами з множеною інцидентних вершин.При цьому ребра повинні пересікатися лише у місці спільної вершини.

Плоске кенігове уявлення гіперграфа також називають «недвудольною технікою» у [1]. Даний спосіб дозволяє легко отримувати інформацію про зв'язок між елементами гіперграфа бо має дуже поросту та наглядну структуру. Проте, неможливість перехрещення ребер при побудові даної моделі гіперграфа накладає істотне обмеження на випадки її практичного використання.

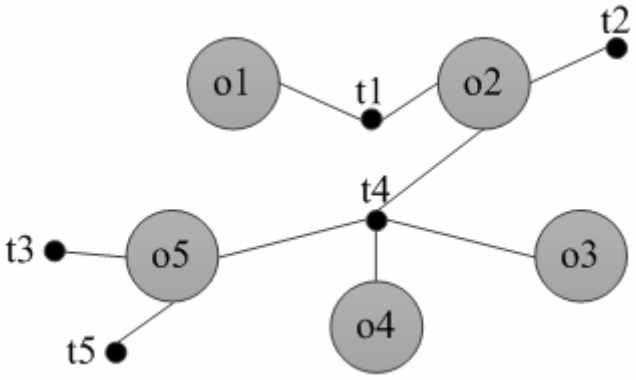


Рис. 3. Плоске кенігове уявлення гіперграфа $H = (O, T)$

Наступна техніка візуалізації гіперграфів активно використовується в моделювання електронних систем [1], вона названа «шинною». Техніка полягає у зображення гіперребер у вигляді прямих, а входження вершин у гіперребро – під'єднанням вершини до ребра через відрізок. При цьому точка з'єднання прямої гіперребра та відрізка входження вершини виділяється вузлом (збільшеною точкою), дивись рисунок 4, де відповідно множина $T = \{t_1, \dots, t_5\}$ – загрози, що спрямовані на ресурси автоматизованої системи, а $O = \{o_1, \dots, o_5\}$ – множина об'єктів захисту.

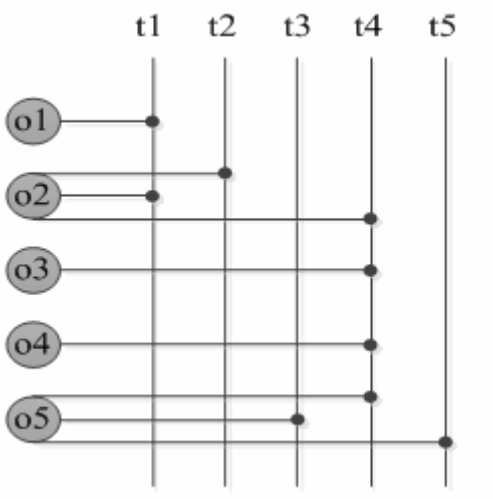


Рис. 3. Модель гіперграфа $H = (O, T)$ за «шинною технікою»

Існує також схожа на «шинну техніку» зображення гіперграфа «блочна техніка», на практиці дуже часто можна зустріти їх комбінацію.

Для моделювання структури системи захисту автоматизованої системи можуть також бути використані l-дольні гіперграфи [3].

Гіперграф $G = (V, \mathcal{E})$ називається l-дольним, якщо його множина вершин розбита на частки (підмножини) V_s, $s = 1,2 \dots, l$, так, що:

1. кожні дві вершин з однієї долі не є суміжними;
2. у кожного ребра $e \in E$ кожна пара вершин $v', v'' \in e$, належать різним долям.

Якщо в гіперграфі G немає кратних ребер і ступінь всякого ребра $e \in E$ дорівнює l ($|e| = l$), то такий гіперграф називають l-однорідним. Гіперграф G називається 3-долинним 3-однорідним, якщо множину вершин V розбито на три підмножини V_s, $s = \overline{1,3}$так, що в кожному ребрі $e = (v_1, v_2, v_3) \in E$ його вершини належать різним долям, тобто $v_s \in V_s$, $s = \overline{1,3}$. У цьому випадку гіперграф G позначається як $G = (V_1, V_2, V_3, E)$.

Таким чином, аналіз можливості застосування гіперграфів, як інструменту моделювання в задачах інформаційної безпеки дозволяє зробити висновок, що використання зазначеного інструментарію є достатньо перспективним для вирішення задач синтезу та аналізу моделі загроз автоматизованій системі обробки інформації класу 3 та оцінки рівня її захищеності.

Список літератури

1. Многоуровневая декомпозиция гиперграфовых структур (Електрон. ресурс.) / Спосіб доступу: URL: http://wwwcdl.bmstu.ru/it/batischev1.html – Загол. з екрана.

2. Емеличев В.А., О. И. Мельников, В. И. Сарванов, Р. И. Тышкевич Глава XI: Гиперграфы // Лекции по теории графов. – М.: Наука, 1990. – С. 298– 315. – 384 с.

3. Омельченко Г.Г. Гиперграфовые модели и методы решения дискретных задач управления в условиях неопределенности.

4. Омельченко Г.Г. Гиперграфовые модели и методы решения дискретных задач управления в условиях неопределенности, диссертация на соискание ученой степени кандидата физико-математических наук, 2004.

5. Зыков А.А. Гиперграфы // Успехи математических наук. – 1974. – № 6 (180).

МЕТРИКИ ЭФФЕКТИВНОСТИ ПРОЦЕССОВ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д.С. Тимофеев, И.А. Ковальская
(Украина, Днепропетровск, ГВУЗ «Национальный горный университет»)

В процессе управления любым направлением деятельности необходимо вырабатывать осознанные и эффективные решения, принятие которых помогает достичь определенных целей. Решение можно принять только на основании фактов и анализа причинно-следственных связей.

Метрика - это инструмент, позволяющий взвешенно и объективно принимать управленческие решения по улучшению работы мер и процессов по обеспечению информационной безопасности (ИБ). Отслеживая метрики на регулярной основе, можно выявить недостатки (или потенциальные недостатки) в процессах обеспечения ИБ и принять своевременные и обоснованные меры по их улучшению и устранению коренных причин возникших отклонений.

Метрики необходимы для того, чтобы:

- показать, каким образом деятельность по безопасности вносит непосредственный вклад в достижение целей безопасности;
- измерить, как изменения в процессе отражаются на достижении целей безопасности;
- выявить существенные аномалии в процессах и принять обоснованные решения по исправлению или улучшению процессов [3].

Для создания эффективных критериев оценки системы управления информационной безопасности используется методика S.M.A.R.T. Согласно данной методике, метрика должна быть: