Магістерська дипломна робота

на тему:

«Моделі та комп’ютерні засоби оцінювання інформаційної безпеки в умовах інформаційної війни»

Виконав: **Гаврилишен В.В.**

студент групи 1БС-15м

Керівник: **Кондратенко Н.Р.**

к.т.н., професор кафедри ЗІ

Мета та задачі дослідження

Мета – дослідження існуючих моделей та комп'ютерних засобів оцінювання інформаційної безпеки та методики їх використання та розробка методу оцінювання інформаційної безпеки в умовах інформаційної війни.

Задачі:

1. Проаналізувати моделі та комп'ютерні засоби оцінювання інформаційної безпеки та методику їх застосування в сфері інформаційної безпеки;
2. Проаналізувати вплив умов інформаційної війни на роботу моделей та існуючої методики їх застосування.
3. Дослідити можливість застосування моделей теорії ігор до задачі оцінювання інформаційної безпеки в умовах інформаційної війни.
4. Розробка програмного засобу реалізації запропонованого методу.

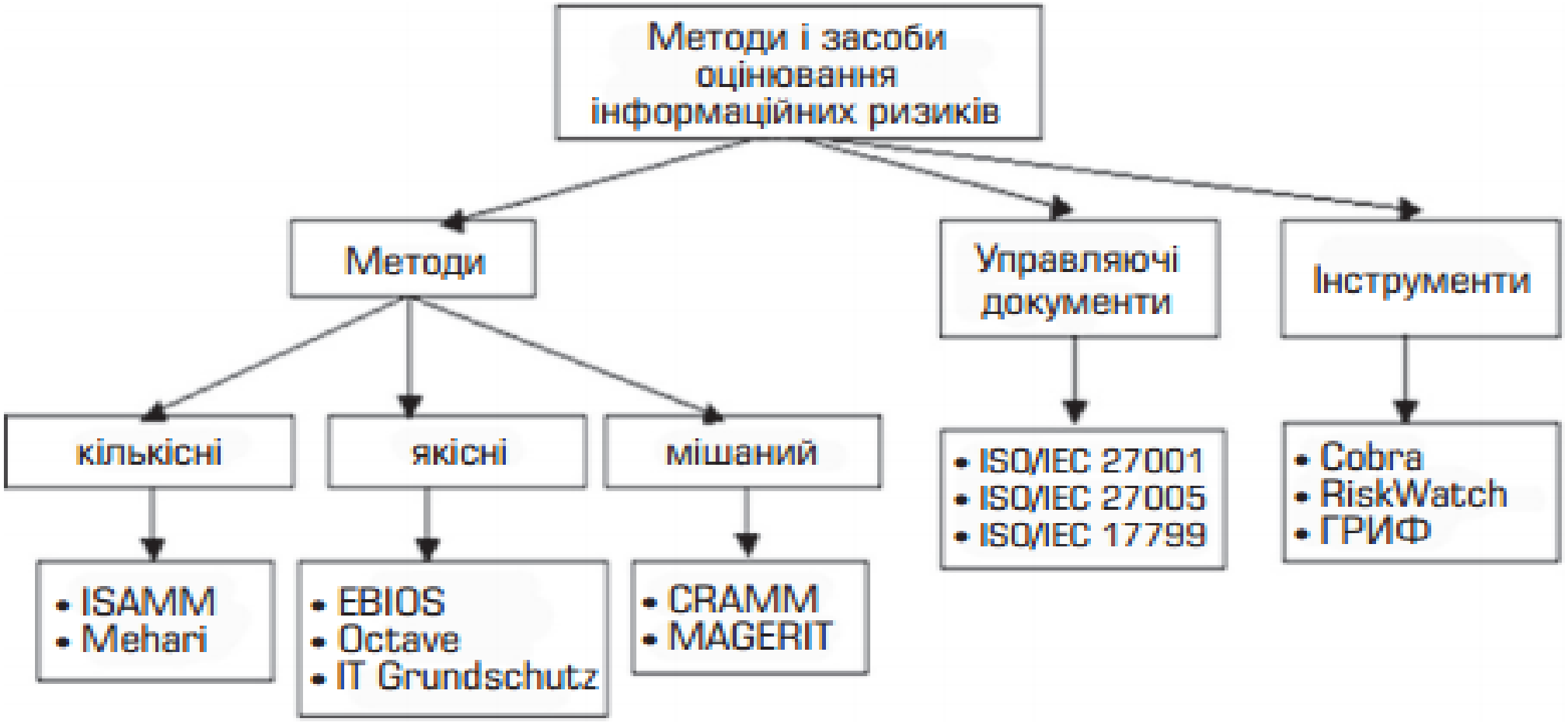
Інформаційна система - це складна, розподілена в просторі система, що складається з безлічі зосереджених (локальних) підсистем (інформаційних вузлів), які мають програмно-апаратними засобами реалізації інформаційних технологій, і безлічі засобів, що забезпечують з'єднання і взаємодія цих підсистем з метою надання територіально віддаленим користувачам широкого набору послуг зі сфери інформаційного обслуговування.

Наявність **засобів захисту інформації** є характерною рисою будь-якої сучасної інформаційної системи. Ефективність захисту інформації в інформаційних системах досягається застосуванням засобів захисту інформації.

RiskWatch використовує визначені Американським інститутом стандартів (**NIST**) оцінки, які називаються **LAFE** і **SAFE**. Local Annual Frequency Estimate (**LAFE**) показує, скільки разів на рік в середньому певна загроза буде реалізована в даному місці (наприклад, в межах міста). Standard Annual Frequency Estimate (**SAFE**) визначає, скільки разів на рік в середньому певна загроза буде реалізована в цій "частині світу" (наприклад, в Північній Америці).

Вводиться також поправочний коефіцієнт, який дозволяє врахувати, що в результаті реалізації загрози ресурс, що необхідно захистити може бути знищений не повністю, а лише частково.

Методи і засоби оцінювання інформаційних ризиків



Переваги та недоліки кількісних і якісних методів оцінювання

	Кількісні методи	Якісні методи
Переваги	- Дозволяють визначати наслідки виникнення інцидентів у кількісний спосіб. - Уможливлюють аналіз витрат і користі при виборі підходу до захисту. - Допомагають отримати достатньо точну картину ризикованої ситуації	Дозволяють визначати сфери та осередки великої небезпеки в стислі терміни та без великих витрат. - Аналіз ризиків і переваг порівняно легкий і дешевий
Недоліки	- Кількісні оцінки неодмінно залежні від розміру та точності вибраної шкали вимірювання. - Результати аналізу можуть бути неточні, зокрема й через відсутність вірогідних даних про перебіг відповідних подій. - Остаточні висновки здебільшого мають спиратися на якісний опис. - Вимагають значно більших витрат, ніж якісні методи, найвищої кваліфікації виконавців і новітніх технічних засобів	- Непридатні для визначення ймовірностей результатів, здобутих чисельними засобами. - Аналіз переваг більш ускладняється за рахунок вибору захисту. - Результати мають загальний характер, усі значення тільки наближені

В даний час на ринку представлена велика різноманітність засобів захисту інформації, які умовно можна розділити на кілька груп:

- Забезпечують розмежування доступу до інформації в автоматизованих системах;

- Забезпечують захист інформації при передачі її по каналах зв'язку;

- Забезпечують захист від витоку інформації по різним фізичним параметрам, виникають при роботі технічних засобів автоматизованих систем;

- Забезпечують захист від впливу програм-вірусів;

- Забезпечують безпеку зберігання, транспортування носіїв інформації і захист їх від копіювання.

Ефективність ІБ можна охарактеризувати як здатність системи протистояти несанкціонованим діям порушника в рамках проектної загрози.

Таким чином, ефективність ІБ і характеризує рівень захищеності об'єкта.

Існують якісні та кількісні методи аналізу ефективності ІБ.

У багатьох випадках якісних оцінок не достатньо, щоб відповісти на питання, наскільки надійна захист об'єкта. Більш точні кількісні методи.

Однак для того, щоб «виміряти» ефективність, необхідно мати обґрунтований критерій (показник оцінки ефективності системи). На практиці зустрічаються такі типи критеріїв.

Критерії ефективності ІБ

1. Критерії типу «ефект-витрати», що дозволяють оцінювати досягнення цілей функціонування СЗІ при заданих витратах (так звана економічна ефективність).

2. Критерії, що дозволяють оцінити якість СЗІ за заданими показниками і виключити ті варіанти, які не задовольняють заданим обмеженням. При цьому використовуються методи багатокритеріальної оптимізації, відновлення функцій і функціоналів, методи дискретного програмування.

3. Штучно сконструйовані критерії, що дозволяють оцінювати інтегральний ефект (наприклад, «лінійна згортка» приватних показників, методи теорії нечітких множин).

Методики оцінювання ІБ

Огляд класичних методик оцінювання інформаційної безпеки Класичні реалізації таких методик, як

- CRAMM,
- FRAP,
- OCTAVE,
- Risk Watch,

базуються на використанні процесної моделі з опитувальною схемою, пропонуючи вже готові стандарти, з яких необхідно вибрати ті, що притаманні системі користувача, та оцінити їх за запропонованою системою критеріїв оцінювання.

Інформаційна війна

Одним із найбільш вагомих факторів, які визначають розвиток сучасного суспільства, є інформація та пов’язані з нею процеси.

Особливої уваги при цьому потребує така форма конфліктної ситуації як **інформаційна війна**, оскільки це явище не тільки гальмує розвиток інформаційного суспільства, а й торкається практично всіх пріоритетних сфер життя в усьому світі.

Інформаційна війна розвивається на сьогодні як самостійна сфера діяльності, а інформація та інформаційні технології поступово стають основним засобом завоювання світу.

Моделі теорії ігор

Теорія ігор — це математичний апарат, що розглядає конфліктні ситуації, а також ситуації спільних дій кількох учасників. Завдання теорії ігор полягає у розробленні рекомендацій щодо раціональної поведінки учасників гри.

Реальні конфліктні ситуації досить складні і обтяжені великою кількістю несуттєвих чинників, що ускладнює їх аналіз, тому на практиці будують спрощені моделі конфліктних ситуацій, які називають **іграми**.

Моделі теорії ігор

Найчастіше розглядається гра з двома гравцями, в якій виграш однієї сторони дорівнює програшу іншої, а сума виграшів обох сторін дорівнює нулю, що в теорії ігор називають **грою двох осіб з нульовою сумою**.

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

Результати (плата) за всіма можливими варіантами гри задаються спеціальними функціями, які залежать від стратегій гравців, як правило, у вигляді **платіжної матриці** такого вигляду, де a_{ij} - значення гри.

Критерії вибору оптимальної стратегії

Критерій крайнього песимізму Вальда. Гравець $P1$ не має ніякої інформації, яку стратегію обирає гравець Р2. Для критерію Вальда

$$W_i(A) = \min a_{ij}.$$

Отже, за критерієм Вальда гравець $P1$ вибирає таку стратегію i_0, для якої

$$min\ a_{i_0 j} = max\ min\ a_{i_0 j}$$

Критерій Байєса (критерій максимального математичного очікування). При використанні цього критерію гравцеві $P1$ повинні бути відомі ймовірності, з якими зловмисник - гравець Р2 - застосовує свої стратегії j. Позначимо ці ймовірності відповідно $q1, q2 \dots qm$

$$W_i = \sum_{j=1}^{m} a_{ij} q_i$$

Оптимальним можна вважати стратегію i_0 гравця Р1, при якій $W_{i_0} = W$.

Критерії вибору оптимальної стратегії

Критерій недостатнього обгрунтування Лапласа. Якщо ймовірності всіх стратегій зловмисника (приблизно) рівні то можна користуватися критерієм Лапласа, для якого

$$W_i = \frac{1}{m}\sum_{j=1}^{m} a_{ij}$$

Критерій песимізму-оптимізму Гурвіца.

Береться

$$W = c \cdot \min a_{ij} + (1 + c) \cdot \max a_{ij} \ ,$$

де c - коефіцієнт песимізму. Крайнього песимізму (c=1) можна протиставити крайній оптимізм (c=0, критерій азартного гравця), коли ставка робиться на найбільший можливий виграш, тобто на найбільший елемент платіжної матриці.

Методика застосування теорії ігор в сфері інформаційної безпеки складається з наступних етапів:

1) Постановка теоретико-ігрової задачі. Визначаються гравці, їх число і стратегії, платіжні функції.

2) Вибір і побудова теоретико-ігрової моделі (типу гри) конфлікту (гри).

3) Рішення гри (знаходження оптимальних стратегій).

Постановка задачі

Захист комп'ютерної системи починається з її опису, та опису доступних засобів захисту і вимог, що ставляться до системи.

Після цього будується безліч допустимих (доступних) проектів захисту, що складають перелік **стратегій адміністратора**.

Складається перелік можливих способів атаки на комп'ютерну систему з боку зловмисників. Це набір його **стратегій нападу**.

Побудова теоретико-ігрової моделі

Розглянемо матричну гру.

Матриця гри. Стратегії адміністратора - гравця А - полягають у встановленні в комп'ютерній системі одного з проектів захисту або відмову від будь-яких дій. Позначимо безліч проектів підсистеми захисту комп'ютерної системи через Z, а поточний стан системи як С. Тоді адміністратор буде вибирати стратегії, відповідні елементам безлічі $A = Z \cup \{C\}$.

Позначимо через U кінцеве безліч узагальнених загроз інформаційній безпеці комп'ютерної системи.

Під узагальненою загрозою розуміється сукупність загроз, подібних за надаваному на комп'ютерну систему впливу і завдаваній шкоді. Розбиття всієї множини загроз на узагальнені загрози формується на базі експертних оцінок.

Побудова теоретико-ігрової моделі

Ігрова стратегія зловмисника - гравця X - полягає у виборі елемента з безлічі $X = U \cup \{U_0\}$, де U_0 - відмова від реалізації загроз інформаційної безпеки.

Кінцева однокрокова антагоністична гра $\Gamma_н$ (матрична гра) задається платіжною матрицею H у вигляді:

$$H = \begin{array}{c} \\ Z_1 \\ \dots \\ Z_{m-1} \\ C \end{array} \begin{array}{c} \begin{array}{cccc} U_1 & \dots & U_{n-1} & U_0 \end{array} \\ \begin{bmatrix} -h_1 - \bar{h}_{11} & \dots & -h_1 - \bar{h}_{1(n-1)} & -h_1 \\ \dots & \dots & \dots & \dots \\ -h_{m-1} - \bar{h}_{(m-1)1} & \dots & -h_{m-1} - \bar{h}_{(m-1)(n-1)} & -h_{m-1} \\ -\bar{h}_{m1} & \dots & -\bar{h}_{m(n-1)} & 0 \end{bmatrix} \end{array},$$

де h_{ij} - оцінки втрат від реалізації зловмисником узагальненої загрози щодо комп'ютерної системи, де реалізовано і-й проект захисту;

h_i - витрати на реалізацію і-го проекту.

Обидві складові беруться зі знаком мінус, так як для власника комп'ютерної системи (адміністратора) це втрати (негативний виграш).

Рішення гри

Рішення гри. Для знаходження рішення гри. т. е. вибору найкращої стратегії захисту, вибору проекту захисту, необхідно визначитися, який критерій прийняття рішення буде використовуватися.

Наприклад, можна використовувати критерій Вальда (максимінний критерій) або Лапласа. Перший з них відображає позицію власника комп'ютерної системи, що готується до найгіршого результату, а другий - позицію «зниження середнього значення очікуваних втрат». У реальній ситуації представляється доцільним застосування декількох критеріїв і порівняння результатів.

Моделі теорії в нечітко визначеному середовищі

У випадку, коли розподіл ймовірностей невідомий, пропонується можливі стратегії учасників описувати у формі нечітких множин. При аналізі такої гри будемо користуватися підходами до задач нечіткого математичного програмування.

Нехай X – універсальна сукупність можливих стратегій учасника, що приймає рішення. Нечіткою ціллю в X буде нечітка підмножина X, яку позначаємо через L. Тоді нечітка ціль описується функцією приналежності

$$\mu_L : X \to [0,1]$$

Виклад моделі обмежується лише іграми двох учасників, але більшість результатів можна поширити і на більшу кількість учасників.

Розробка засобу оцінювання

Щоб розширити можливості проектувальника системи захисту

ДЯКУЮ ЗА УВАГУ