УДК 621.039

Вдосконалення методів прийняття рішень в системах захисту.

Совершенствование методов принятия решений в системах защиты.

Improving decision-making methods in security systems.

Науковий керівник - кафедра радіотехнічних пристроїв; доцент, кандидаттехнічних наук – Агаджанян А. Р., магістр – Кожухар А. В.
Научный руководитель – кафедра радиотехнических устройств; доцент, кандидат технических наук –Агаджанян А. Р., магістр – Кожухар А В.
Supervisor - department of radio engineering devices; associate professor, candidate of technical sciences – Ahadzhanian A. R., master –Kozhukha rA. V.

Анотація. Вдосконалюються методи прийняття рішень в СПР, шляхом використання методів теорії ігор..

Ключові слова: управління інформаційною безпекою, теорія ігор, кібербезпека, системи прийняття рішень.

Аннотация. Совершенствуютс яметоды принятия решений в СПР, путем использования методов теории игр .

Ключевые слова: управление информационной безопасностью, теорія игр, кибербезопасность, системы принятия решений.

Annotation.Abstract. methods of decision-making in DMS are improved by using methods of game theory.

Keywords: information security management, game theory, cybersecurity, decision making systems.

У зв'язку з постійно зростаючим обсягом інформації, яка циркулює і використовується людьми в різних сферах життєдіяльності, зростає роль автоматизованих систем підтримки прийняття рішень (СППР).

Системи прийняття рішень, або, інтелектуальні системи підтримки прийняття рішень (ІСППР) у загальному вигляді — це система, яка асистує особам, які приймають рішення в прийнятті цих самих рішень, використовуючи інструментарії дата майнінгу, моделювання та візуалізації, включаючи відповідне програмне забезпечення, стійке за якістю, інтерактивне і гнучке з налагодження.

Незважаючи на величезні зусилля, спрямовані на вирішення цієї проблеми, використання новітніх розробок в підходах і технологіях захисту інформації, дана задача залишається актуальною і не втрачає своєї гостроти.

Складність завдання захисту інформації продиктована труднощами її формалізації і антагоністичною природою самої проблеми. На жаль, більшість розроблених і розглянутих в літературі методів не враховують антагоністичні особливості задач захисту інформації а це, в свою чергу,призводить до низької ефективності в їх використанні.

Великою перевагою теорії ігор є те, що її розрахунок можна легко перенести в електронний вигляд, що автоматизує роботу і покращить результати досліджень.

Метою моєї роботи є підвищення ефективності прийняття рішень шляхом застосування антагоністичних методів теорії ігор. Тобто теорія ігор має необхідний інструментарій для розглядання і розробки рішень та завдань пов’язаних з захистом інформації. Особливу увагу потрібно звернути на вирішення антагоністичних ігор.

Антагоністична гра — це система Г = (X, Y, F), де X — множина стратегій першого гравця, Y — множина стратегій другого гравця, F (x,y) — функція виграшу. Перший гравець прагне максимізувативати функцію F, а другий гравець — мінімізувати цю функцію. Будемо вважати, що множини X і Y компактні, а функція F (x, y) — безперервна.

Особливу увагу я приділив вирішенню матричних антогоністичних ігор. Антагоністична гра називається матричною, якщо множини стратегій гравців кінцеві. В цьому випадку можна покласти

$X= \{1,\dots n\}, \quad Y= \{1, \dots m\}, \quad F(i,j) = a_{ij}, \quad i= 1,\dots,n, \quad j= 1,\dots m.$

Таким чином, матрична гра повністю визначається матрицею A=(a_ij), i = 1, ... n, j= 1,… m. Зроблено це для спрощення задачі.

Моделювання задачі

Підприємство самостійно може обрати стратегію захисту інформації С1, С2, С3. Кожна стратегія має коефіцієнт корисної дії рішень р1, р2, р3. Значення ККД також буде залежати від часу прийняття рішення(вчасно, невчасно). Також будуть враховуватися ресурси виділені для захисту відповідного класу секретності. Побудуємо таблицю задачі табл.1.

Потрібно:

1) надати описаній ситуації ігрову схему, вказати допустимі стратегії сторін, скласти матрицю;

2) дати рекомендації вибору стратегії за видами, які забезпечують підприємству максимальний прибуток.

Щоб зменшити розмірність матриці можна вважати, що одночасно на всі три види стратегії ресурси виділенні для захисту інформації можуть приймати лише один клас секретності: особливої важливості, цілком таємний або таємний.

Таблиця 1 — Таблиця даних

Стратегія захисту інформації	ККД рішення	ККД рішення		Ресурси виділенні для захисту відповідного класу секретності		
		Прийняте вчасно	Прийняте невчасно	Особливої важливості	Цілком таємної	Таємної
С1	6.3	7.8	6.5	15	10	8
С2	7.1	7.9	7.2	40	26	10
С3	5.8	7.4	6.1	28	17	15

Ігрова схема:

У грі беруть участь 2 гравця: А — захисник, В — атакуючий.

Гравець А прагне вибрати таку стратегію рішень, щоб отримати максимальний ККД обраних рішень. Стратегіями гравця А є:

А1 – Захист інформації особливої важливості;

А2 – Захист цілком таємної інформації;

А3 – Захист таємної інформації.

Гравець В прагне витратити мінімальну кількість часу на злом захисту. Стратегіями гравця В є:

В1 – Затрачений час на злам інформації особливої важливості

B2 - Затрачений час на злам цілком таємної інформації.
B3 - Затрачений час на злам таємної інформації.
Інтереси гравців А і В - протилежні.

Визначимо зміну ККД від вчасності реагування табл.2.

Таблиця 2 — Зміна ККД від вчасності реагування

Стратегіязахистуінформації	ККД рішення	Цінавчасно принятого рішення	Цінаневчасно принятого рішення
C1	6.3	7.8-6.3=1.5	6.5-6.3=0.2
C2	7.1	7.9-7.1=0.8	7.2-7.1=0.1
C3	5.8	7.4-5.8=1.6	6.1-5.8=0.3

Для спрощення ціна невчасно прийнятого рішення не зменшує його ціну, будемо вважати, що ціна буде зменшуватися коли рішення не прийнято взагалі.
Розрахуємо елементи матриці табл.3.

Таблиця 3 — Розрахунок елементів матриці

Захист	Атака			
	Стратегії	Особливоїважливості: 15+40+28	Цілкомтаємно: 10+26+17	Таємно: 8+10+15
	Особливоїважливості: 15+40+28	15*1,5+40*0,8+28*1,6=99.3	10*1.5+(15-10)*0.2+26*0.8+(40-26)*0.1+17*1.6+(28-17)*0.3=68.7	8*1.5+(15-8)*0.2+10*0.8+(40-10)*0.1+15*1.6+(28-15)*0.3=52.3
	Цілкомтаємно: 10+26+17	10*1,5+26*0,8+17*1,6 =63	10*1,5+26*0,8+17*1,6 =63	8*1.5+(10-8)*0.2+10*0.8+(26-10)*0.1+15*1.6+(17-15)*0.3=46.6
	Таємно: 8+10+15	8*1,5+10*0,8+15*1,6 =44	8*1,5+10*0,8+15*1,6 =44	8*1,5+10*0,8+15*1,6 =44

Отримали матрицю відношення табл.4.

Таблиця 4 — Матриця відношення

Стратегії	A1	A2	A3
31	93,3	68,7	52,3
32	63	63	46,6
33	44	44	44

Я використав методи мінімаксу, максиміну, графічний та метод Брауна-Робінсона для вибору найкращого варіанту прийняття рішення, і знаходження так званої Нешовської рівноваги, якщо вона є в обраній грі.

Вирішення даних методів давно автоматизовано і не потребує представлення або детального розбору рішення даної задачі. Всі вище перечисленні методи зводять рішення задачі до оптимального вибору стратегій альтернатив (31, А3). Саме стратегії (1;3) є сідловою точкою, даної матриці, а значить оптимальними стратегіями для захисника і атакуючого будуть саме ці стратегії.

Потрібно розуміти, що я не створив нові методи теорії ігор, а використав уже існуючі для вирішення задачі з вибору найліпшої стратегії.

Плюсами теорії ігор є:

- Простота розрахунків;
- Легкість в автоматизації;
- Порівняно високий коефіцієнт корисної дії, в порівнянні з іншими методами;
- Простота обслуговування СПР створених на основі теорії ігор;
- Наявність методів для рішення антагоністичних задач.

У цій роботі я запровадив модель кібербезпеки разом із теоретичними інструментами теорії ігор, щоб довести, що методи прийняття рішень не настільки ефективні у забезпеченні ефективних графіків захисту, як ті, що обчислюються теорією ігор Неша.

Література

1. Acquisti, A., Grossklags, J.: Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. In: Proc. of the 2nd Annual Workshop on Economics and Information Security (WEIS 2003), vol. 3 (2003).
2. Alpcan, T., Ba¸ sar, T.: Network security: A decision and game-theoretic approach. Cambridge University Press (2010).
3. Grossklags, J., Christin, N., Chuang, J.: Secure or insure?: a game-theoretic analysis of information security games. In: Proc. of the 17th International Conference on World Wide Web (WWW 2008), pp. 209–218. ACM (2008).
4. Hankin, C., Malacaria, P.: Payoffs, intensionality and abstraction in games. In: Coecke, B., Ong, L., Panangaden, P. (eds.) Abramsky Festschrift. LNCS, vol. 7860, pp. 69–82. Springer, Heidelberg (2013).
5. Johnson, B., Grossklags, J., Christin, N., Chuang, J.: Nash equilibria for weakest target security games with heterogeneous agents. In: Jain, R., Kannan, R. (eds.) Gamenets 2011. LNICST, vol. 75, pp. 444–458. Springer, Heidelberg (2012).

АгаджанянАрутюнРубенович,
АгаджанянАрутюнРубенович,
AhadzhanianArutiun,
Кожухар Андрій Вадимович,
Кожухар Андрей Вадимович,
KozhukharAndrii.