МЕТОДИКА ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ АПРІОРНОЇ НЕВИЗНАЧЕНОСТІ

Борисенко Л.А., Добринін І.С.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна.

E-mail: lesia.borysenko@nure.ua,
ihor.dobrynin@nure.ua

Abstract

The article reflects the importance of developing and implementing an information security management system. An appropriate mathematical apparatus for decision-making in conditions of a priori uncertainty is determined. A methodology for building an information security management system in conditions of a priori uncertainty is proposed using mathematical apparatus game theory with nature. Optimality criteria were analyzed and the expediency of their use was determined.

Впровадження системи управління інформаційною безпекою (далі – СУІБ) є стратегічним рішенням організації. На проектування СУІБ компанії впливають потреби та цілі підприємства, вимоги безпеки, використовувані процеси, а також масштаби діяльності і структура організації. Загальноприйнятим є факт, що стандарт ISO/IEC 27001:2022 містить кращі практики і принципи з управління інформаційною безпекою компанії, впровадження яких дозволить забезпечити захист від сучасних інформаційних ризиків. Проте ті організації, які не стикались із загрозами втрати конфіденційних даних, мають повну невизначеність у побудові СУІБ. З огляду на це, метою роботи була поставлена розробка методики побудови системи управління інформаційною безпекою в умовах апріорної невизначеності.

Очевидно, що етап аналізу ризиків є найважливішим для розробки ефективної СУІБ, але в умовах апріорної невизначеності, з якою стикається доволі широкий пласт компаній, майже неможливо правильно та чітко оцінити ризики виникнення тієї чи іншої загрози. Отже, однією з головних проблем прийняття рішень в умовах апріорної невизначеності є її власне розкриття.

Вагомим внеском у виборі засобів захисту конфіденційних даних при розробці СУІБ є результати математичних перетворень. Перелік останніх, в свою чергу, визначається за допомогою підсумку аналізу наявних ризиків та вразливостей активів.

Для того, щоб знайти оптимальний математичний апарат, який може стати в нагоді у пошуку найкращої стратегії при побудові СУІБ в умовах апріорної невизначеності, було досліджено метод аналізу ієрархій, теорію корисності, а також теорію ігор, яка має досить широку класифікацію. Перелічені математичні методи мають безліч переваг та можуть бути застосовані при прийнятті рішень у розробці системи управління інформаційною безпекою. Але слід відмітити, що вищезазначені теорії, окрім однієї, засновані на виборі певних критеріїв, на знаннях про визначені ризики та загрози, що має організація. Таким чином, при дослідженні теорії ігор був відокремлений розділ, що стосується ігор з природою, в яких усвідомлено діє тільки один гравець, а інший – навмання. Природа не має на меті отримання виграшу, що і відрізняє цей тип ігор.

Взагалі, управління інформаційною безпекою певною мірою і є грою – уповноважена особа компанії захищається від атак зловмисника, а той, в свою чергу, шукає слабкі місця в системі захисту інформації для отримання власної вигоди. Як правило, при побудові СУІБ переважна кількість рішень приймається в умовах невизначеності, що свідчить про важливість дослідження математичних апаратів, що можуть надати інформацію для прийняття доцільних рішень.

Природа – узагальнене поняття супротивника, який не переслідує власних цілей у конфлікті. Відповідно, в іграх з природою задача вибору оптимальної стратегії для гравця з одного боку полегшується, а з іншого – ускладнюється через дефіцит інформації про поведінку природи.

Отже, поставимо задачу. Припустимо, що А – адміністратор безпеки певного підприємства, метою якого є вибір максимально ефективних та оптимальних засобів захисту, має перелік певних стратегій A_1, A_2, …, A_m; а В – природа, яка має стани B_1, B_2, … , B_n. Таким чином, гра з природою відображається у вигляді платіжної матриці (матриці виграшів), кожним елементом a_{ij} якої є виграш адміністратора безпеки А з використанням стратегії, що була обрана відповідно до кожного можливого стану природи В. Початковий вид такої матриці поданий у вигляді таблиці 1.

Таблиця 1. Платіжна матриця для теорії ігор ходом природи

	B_1	B_2	B_3	…	B_n	$E(x_i)$
A_1	a_{11}	a_{12}	a_{13}	…	a_{1n}	$E(x_i)$
A_2	a_{21}	a_{22}	a_{23}	…	a_{2n}	$E(x_i)$
…	…	…	…	…	…	…
A_m	a_{m1}	a_{m2}	a_{m3}	…	a_{mn}	$E(x_i)$

Слід зазначити, що строки відповідають за обране рішення адміністратором безпеки А, а стовпці – за певний стан природи В. Параметром $E(x_i)$ виступає оцінка стратегії, що була підрахована згідно з певним критерієм оптимальності, які розглянуто дещо нижче.

Важливий зроблений висновок: зробив похибку при формуванні платіжної матриці, можна отримати зовсім інший кінцевий результат, що буде хибним для певної стратегії і призведе адміністратора безпеки до програшу в грі зі станами природи. Така модель поведінки схожа на теорію хаосу, яка на цей проміжок часу залишається маловивченою в застосуванні її на практиці. Теорія хаосу свідчить про те, що складні системи надзвичайно сильно залежні від початкових умов і невеликі зміни у навколишньому середовищі призводять до непередбачуваних наслідків [1].

Перш за все, організація повинна подбати про найм співробітника, який спеціалізується на розрахунках збитків при певному типі атаки на активи компанії за умовою, якщо вона була виконана зі стовідсотковим успіхом на користь зловмисника. На цьому етапі повинні враховуватися як поточні засоби захисту інформації (за їх наявності), так і ті, що були запропоновані організацією для впровадження належної та ефективної системи управління інформаційною безпекою підприємства. Таким чином, узагальнюючи все вищеподане, запропонованою автором формулою для розрахунку виграшу стратегії адміністратора a_{ij} є:

$$a_{ij} = G - (F + C), \tag{1}$$

де G – кількісний збиток організації при реалізації певного стану природи з урахуванням тих засобів захисту інформації, що є в компанії на поточний проміжок часу;

F – кількісний збиток компанії при реалізації певного стану природи з урахуванням запропонованих адміністратором безпеки засобів захисту інформації;

С – вартість запропонованого засобу захисту інформації.

Цілком очевидно, що неможливо передбачити наслідки вибору певної стратегії адміністратором безпеки в умовах апріорної невизначеності. Саме тому при розв'язанні задач про прийняття рішень в умовах невизначеності можуть бути застосовані певні критерії оптимальності [2]. Критерій оптимізму призначений для вибору найбільшого елементу матриці з її максимально можливих елементів. Він використовується, коли гравець опиняється у безвихідному становищі і коли будь-який його крок з однаковою ймовірністю може бути як абсолютним виграшем, так і повним провалом. Таким чином, критерій максімакса передбачає, що розвиток ситуації буде сприятливим для особи, яка приймає рішення. Критерій песимізму є протилежністю вищезазначеного правила. Він призначений для вибору найменшого елементу матриці з її мінімально можливих елементів, а також передбачає, що розвиток ситуації буде несприятливим для особи, яка приймає рішення. Критерій Лапласа стверджує, що якщо апріорна інформація щодо можливих станів природи є відсутньою, то можна вважати їх виникнення однаково ймовірним. У такому випадку слід обирати ту стратегію, яка забезпечить виграш, тобто оптимальним вважається рішення, якому відповідає найбільша сума.

Критерій Вальда призначений для вибору з переліку стратегій варіанту з найбільшим показником ефективності з мінімально можливих показників для кожного з представлених варіантів. Критерій забезпечує максимізацію мінімального виграшу, який може бути отриманий при реалізації кожного з варіантів стратегій, орієнтуючи гравця на обережну лінію поведінки, що спрямована на отримання доходу та мінімізацію можливих ризиків одночасно.

Критерій Севіджа допускає розумний ризик заради одержання додаткового прибутку. У ситуації невизначеності цим критерієм можна користуватися при впевненості, що випадковий збиток, який може виникнути при прийнятті недоцільного рішення, не приведе організацію до повного краху. Суть критерію полягає в виборі тієї стратегії, яка не дозволить допустити занадто високих втрат, до яких вона може призвести.

Критерій Гурвіца призначений для вибору деякого середнього елементу матриці, що відрізняється від крайніх станів – мінімального та максимального елементів. Він дозволяє уникнути крайніх станів у прийнятті рішення – невиправданого оптимізму або ж крайнього песимізму, і вибрати найімовірніший варіант стратегії, який забезпечить найкращу ефективність.

Підсумовуючи опис всіх вищезазначених критеріїв, можна дійти висновку, що кожне з правил має свої сліпі зони, які не дозволяють охопити всі можливі аспекти ситуації. Так, наприклад, критерій оптимізму зовсім не враховує ймовірності виникнення негативних для гравця наслідків, а критерій песимізму – навпаки, занадто зациклений на обережній поведінці, що не дозволяє підприємству отримати максимальну вигоду від гри. Очевидно, що в прийнятті рішень в умовах апріорної невизначеності повинні враховуватися всі або переважна кількість критеріїв для отримання більшого об'єму даних щодо кожної стратегії з метою їх подальшого аналізу, що є дуже цінним в умовах апріорної невизначеності. Слід зазначити, що результати підрахунків вище перелічених критеріїв можуть суттєво відрізнятись один від одного, що пов'язано з факторами наявності як невизначеності ситуації, так і безсумнівної суперечливості гіпотез.

Як і будь-яка методика, запропонована методика побудови системи управління інформаційною безпекою має певні обмеження та припущення. Перш за все – для отримання вхідної інформації необхідно використовувати дані аналітичних агентств. Також отримані дані мають доповнюватись з урахуванням власного досвіду адміністратора безпеки, на основі чого і формується платіжна матриця. Організація повинна чітко розуміти свою політику, яка може як приймати ризики, так і навпаки – взагалі їх виключати (для визначення комбінації критеріїв оптимальності, що будуть застосовані). Бажано передбачити всі ситуації, з якими може стикнутися CISO, але перелік можливих станів природи залишається досить імпровізованим.

Отже, адміністратор безпеки, знаючи та враховуючи вищеподані обмеження та припущення методики побудови СУІБ, може створити доцільну та достатньо ефективну систему управління інформаційною безпекою для організації, яка опинилась в умовах апріорної невизначеності, з метою протидії витоку конфіденційної інформації в наслідок реалізації кібератак, а також природних катаклізмів. Запропонована методика може бути використана компаніями, які мають на меті захистити свої активи для знаходження балансу інтересів бізнесу та інформаційної безпеки, а також для підвищення довіри зацікавлених сторін, але стикнулися зі станом невизначеності при побудові СУІБ.

*Л*ітература

1. Найман Е. Як купувати дешево та продавати дорого / Ерік Найман. – М.: Альпіна Паблішерз. – 2011. – С. 220 с 248.

2. Моделі й методи прийняття рішень: навч. посіб. / С.А. Ус, Л.С. Коряшкіна; М-во освіти і науки України, Нац. гірн. ун-т. – Д. : НГУ, 2014. – 300 с.

3. Ігри з природою в умовах невизначеності: URL: https://moodle.kstu.ru/mod/book/view.php?id=11481 (дата звернення: 07.11.2023).

4. Saaty, T. L. The Analytic Hierarchy Process / T. L. Saaty. – New York: McGraw-Hill International, 1980. 287 с.

5. Ihor Dobrynin, Tamara Radivilova, Nadiia Maltseva and Dmytro Ageyev. "Use of Approaches to the Methodology of Factor Analysis of Information Risks for the Quantitative Assessment of Information Risks Based on the Formation of Cause-And-Effect Links", 2018 5th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, Ukraine, 2018. p. 229 – 233, DOI:10.1109/INFOCOMMST.2018.8632022.