УДК 004.056:159.95

Л. О. Нікіфорова, Ю. Є. Яремчук, А. А. Шиян
Вінницький національний технічний університет
Хмельницьке шосе, 95, 21021 Вінниця, Україна

Моделювання вибору оптимального методу протидії загрозам інформаційній безпеці

Побудовано математичну модель для вибору методу протидії загрозам інформаційній безпеці. Виведено загальну формулу для розрахунку економічного ефекту від запровадження методу протидії заданій загрозі інформаційній безпеці. Отримано умови, при виконанні яких використовувати метод протидії заданій загрозі інформаційній безпеці є економічно доцільним. Побудовано оптимізаційну модель для задачі вибору методу протидії заданій загрозі інформаційній безпеці.

Ключові слова: *інформаційна безпека, методи протидії загрозам, методи оцінки ризиків, математична модель, економічна ефективність.*

Вступ

Інноваційний розвиток економіки та становлення економіки знань вимагають все більшої уваги до моделей, методів і технологій захисту інформації. Усе зростаюча роль суб'єктів — носіїв конфіденційної інформації, усе зростаюче проникнення комп'ютерного обладнання, яке використовується як для створення, так і для зберігання інформації, для комунікації між суб'єктами інформаційних процесів, — все це вимагає також зростання уваги до протидії загрозам інформаційній безпеці.

Кількість джерел таких загроз також стрімко зростає відповідно до розвитку технічного оснащення зловмисників та у відповідності до зростання кількості людей, які залучаються до кіберпростору на планеті. Також важливим є те, що у віртуальний простір переводиться все більша кількість видів діяльності людини.

Однак весь цей захист від негативного впливу на інформаційні системи вимагає витрат ресурсів, передовсім економічних, що накладає свої обмеження, які часто носять принциповий характер: економічна діяльність, яка найчастіше здійснюється у рамках підприємства, орієнтована на досягнення максимального прибутку, тоді як заходи протидії загрозам інформаційної безпеки відносяться до витрат.

Таким чином, задача забезпечення інформаційної безпеки є актуальною у науковому плані та має досить великий потенціал для практичного застосування.

© Л. О. Нікіфорова, Ю. Є. Яремчук, А. А. Шиян

Аналіз публікацій та постановка задачі

Інформаційна безпека передбачає захищеність інформації та інфраструктури, яка її підтримує, від випадкових або навмисних впливів природного або штучного характеру, що можуть завдати неприйнятної шкоди суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації та підтримуючої інфраструктури [1–3].

Загрози інформаційній безпеці мають, як правило, статистичну природу. Аналіз методів оцінювання таких ризиків здійснено у [4], де виокремлено такі методи: статистичний, ймовірнісно-статистичний, теоретико-ймовірнісний, експертний і табличний. Однак застосування методів протидії загрозам інформаційній безпеці вимагає фінансових витрат (витрати ресурсів — як технічних, так і людських, у рамках сучасної економічної теорії [5] можна звести до фінансового виміру). Як правило, для визначення цих витрат застосовують метод Гордона-Лоеба [6], у рамках якого використовується явний функціональний вигляд для залежності ймовірності порушення технічної інформаційної системи від інвестицій у захист і від вразливості системи при нульових інвестиціях. Модель [6] приваблива тим, що вона дозволяє обчислити прибуток від зменшення витрат за рахунок втрати інформації внаслідок інвестування у захист інформації. Проте суттєвим недоліком цієї моделі є необхідність використання завдання ймовірності порушення цілісності інформаційної системи у вигляді цілком певної аналітичної залежності, що суттєво зменшує сфери застосування цієї моделі.

Існуючі модифікації моделі Гордона-Лоеба розвиваються у напрямку збільшення кількості введених у [6] аналітичних функцій. Зокрема шляхом помноження її на інші аналітичні функції, явний вигляд яких вводиться авторами модифікацій евристичним шляхом. Таке вдосконалення дозволяє здійснити комп'ютерне моделювання та оптимізацію [7], проте результати будуть справедливими лише для тих випадків, які відповідають введеним евристичним функціям.

Ще одним напрямком постановки задачі на оптимізацію є моделювання систем захисту в мережах передавання інформації [8]. У рамках таких моделей оптимізація здійснюється за технічними характеристиками, проте врахування економічного результату від діяльності систем захисту в рамках цих моделей призводить до значних ускладнень.

Таким чином, розробка загального підходу до задачі на вибір оптимального методу протидії загрозам інформаційній безпеці саме за його впливом на економічну діяльність залишається все ще невирішеною.

Метою статті є розробка загальної моделі для вибору оптимального методу протидії загрозам інформаційній безпеці за його впливом на результати економічної діяльності.

Розробка моделі вибору методу протидії загрозам

Побудуємо математичну модель для розрахунку економічної ефективності для довільного методу протидії загрозам інформаційній безпеці.

Характерними особливостями загального класу загроз інформаційній безпеці є такі:

1) наявність досить чітко визначених і вимірюваних параметрів, що свідчать про *настання* загрози;

2) характеристики розгортання загрози у часі, коли залишається час для того, щоб *управляти* подальшим розгортанням ситуації. Тобто розпочати систему заходів для а) попередження ситуації та б) для зменшення втрат при її настанні;

3) наявність «критичних значень параметрів», за досягненням яких вже *незворотно наступає* кризова ситуація (і управляти ситуацією стає неможливим).

Введемо три класи параметрів, які будуть характеризувати: а) саму загрозу інформаційній безпеці (умови її настання та економічні втрати від неї); б) механізм протидії загрозі інформаційній безпеці (передовсім необхідні для нього економічні витрати); в) утрати від реалізації загрози інформаційній безпеці (за умови, що вона настала, незважаючи на задіяння механізму протидії їй).

Для цього використаємо наступні параметри.

Характеристики самої загрози інформаційній безпеці:

P_k — імовірність настання таких значень показників, які є характерними для реалізації загрози інформаційній безпеці;

V_k — втрати від реалізації загрози інформаційній безпеці (разові);

B_k — втрати від непрацюючого стану інформаційної системи протягом часу її відновлення після реалізації інформаційної загрози (їх можна оцінити як $T_k t_k$, де T_k — втрати за одиницю часу на *відновлення* інформаційної системи *після* реалізації загрози; t_k — час відновлення інформаційної системи).

Характеристики механізму протидії загрозі (загрозам) інформаційній безпеці:

P_m — імовірність досягнення показниками, що характеризують загрозу, тих значень, за яких *розпочинається* дія розглядуваного механізму протидії загрозі (загрозам) інформаційній безпеці;

A — вартість *створення* розглядуваного механізму протидії загрозі (загрозам) інформаційній безпеці;

V_m — втрати від роботи розглядуваного механізму протидії загрозі (загрозам) інформаційній безпеці (разові);

B_m — втрати від непрацюючого стану системи протягом відновлення її після спрацювання механізму протидії загрозі (загрозам) інформаційній безпеці (їх можна оцінити як $T_m t_m$, де T_m — втрати за одиницю часу на *відновлення* інформаційної системи *після* спрацювання механізму протидії загрозі (загрозам) інформаційній безпеці; t_m — час відновлення після спрацювання механізму протидії).

Характеристики, що описують економічні наслідки реалізації загрози (загроз) інформаційній безпеці, незважаючи на спрацювання механізму протидії:

$P(k \mid m)$ — умовна ймовірність реалізації загрози (загроз) інформаційній безпеці після спрацювання механізму протидії;

V_{km} — втрати від реалізації загрози (загроз) інформаційній безпеці *після* спрацювання механізму протидії;

B_{km} — втрати на відновлення системи *після* спрацювання механізму загрозі (загрозам) інформаційній безпеці та її подальшої реалізації, незважаючи на про-

тидію (їх можна оцінити як $T_{km}t_{km}$, де T_{km} — втрати за одиницю часу на *відновлення* інформаційної системи *після* спрацювання механізму протидії загрозі (загрозам) інформаційній безпеці та її подальшої реалізації, незважаючи на протидію; t_{km} — час відновлення *після* спрацювання механізму протидії загрозі (загрозам) інформаційній безпеці та її подальшої реалізації, незважаючи на протидію).

Основна формула для розрахунку економічної ефективності механізму протидії загрозі (загрозам) інформаційній безпеці виводиться із співвідношення, яке задовольняє такій умові: математичне очікування витрат на протидію загрозі (загрозам) інформаційній безпеці (включаючи також і витрати при її настанні незважаючи на протидію) повинна бути *меншою* за вартість відновлення інформаційної системи при реалізації загрози (загроз) інформаційній безпеці без всякої протидії їй.

Математично ця умова може бути виражена наступним співвідношенням:

$$A + P_m(V_n + B_m) + P(k \mid m)\left[V_{km} + B_{km}\right] \le P_k\left[V_k + B_k\right]. \tag{1}$$

Звідси отримуємо таку оцінку для вартості створення механізму протидії загрозі (загрозам) інформаційній безпеці:

$$A \le P_m\left[V_m + B_m\right] \cdot \left(\frac{V_k + B_k}{V_m + B_m} \cdot \frac{P_k}{P_m} - \frac{P(k \mid m)\left[V_{km} + B_{km}\right]}{P_m\left[V_m + B_m\right]} - 1 \right). \tag{2}$$

Із нерівності (2) видно, що, з економічної точки зору, вибір методів протидії загрозі інформаційній безпеці може носити пороговий характер, коли деякі методи протидії можуть бути відхилені як економічно невигідні.

Звичайна умова $A > 0$ призводить до такого твердження, яким задаються *необхідні* умови для вибору методу протидії загрозі інформаційній безпеці.

Твердження. Створення механізму протидії загрозі (загрозам) інформаційній безпеці може бути економічно вигідним тільки за умови виконання нерівності:

$$\frac{V_k + B_k}{V_m + B_m} \cdot \frac{P_k}{P_m} > \frac{P(k \mid m)\left[V_{km} + B_{km}\right]}{P_m\left[V_m + B_m\right]} + 1. \tag{3}$$

Розглянемо більш детально формулу для розрахунку економічної ефективності механізму протидії загрозі (загрозам) інформаційній безпеці, яку можна записати у такому вигляді.

$$I = P_k\left[V_k + B_k\right] - A - P_m(V_n + B_m) - P(k \mid m)\left[V_{km} + B_{km}\right]. \tag{4}$$

Звичайно, при цьому вартість створення механізму протидії загрозі (загрозам) інформаційній безпеці повинна задовольняти умовам нерівності (3).

Для ряду механізмів протидії загрозі (загрозам) інформаційній безпеці останнім членом у (4) можна знехтувати. Наприклад, для механізмів протидії, які полягають у *відключенні* інформаційних систем *завжди* виконується рівність $P(k \mid m) = 0$. Іншими словами, після задіяння такого методу протидії сама загроза

повністю зникає. Як приклад можна навести DDOS-атаки, для яких метод протидії полягає у випереджувальному відключенні інформаційної системи від мережі.

Розглянемо більш детально економічний смисл наявності множника, який включає у себе $P(k \mid m)$ в (4).

У загальному випадку методи протидії загрозі (загрозам) інформаційній безпеці можуть бути реалізовані за двома сценаріями:

1) метод протидії *не гарантує* того, що загрозу буде *повністю* усунуто. Прикладом можуть слугувати ситуації, коли загрозою інформаційній безпеці є несанкціонований доступ до комп'ютерів, а методами протидії слугують різні антивірусні програмні продукти. Для методів із цього класу виконується нерівність $P(k \mid m) \le 1$;

2) метод протидії *впливає* на настання та розгортання загрози (загроз) інформаційній безпеці, *зменшуючи* ймовірність її настання (аж до її *повної відміни*). Прикладами можуть слугувати вже згадуване відключення інформаційної системи від мережі для DDOS-атак, або ж формування так званого «чорного списку» для ряду IP-адрес. Для методів із цього класу виконується нерівність $P(k \mid m) < 1$.

Для методів з обох класів, як правило, будуть виконані такі умови: $V_k >> V_m$, $V_k >> V_{km}$ та $B_k >> B_m$, $B_k >> B_{km}$.

Використовуючи розроблену вище математичну модель, метод вибору оптимального методу протидії *заданій* загрозі інформаційній безпеці за показником його економічної ефективності може бути записано у вигляді такого алгоритму.

1. Сформувати базу даних щодо ймовірностей отримання показниками, які характеризують задану загрозу інформаційній безпеці, таких їхніх значень, які є характерними для початку дії методу протидії загрозі та реалізації самої загрози (це ймовірності P_k та P_m відповідно). Для цього можна використати методи, які описані в [4].

2. Сформувати базу даних щодо умовної імовірності $P(k \mid m)$ для реалізації даної загрози інформаційній безпеці після спрацювання механізму протидії їй.

3. Пункти 1 та 2 повторити для кожного із можливих методів протидії даній загрозі інформаційній безпеці.

4. За формулою (2) здійснити розрахунки для кожного з можливих методів протидії даній загрозі інформаційній безпеці та відбракувати ті із них, для яких ця нерівність не виконується.

5. За формулою (4) для кожного із методів протидії даній загрозі інформаційній безпеці розрахувати величину економічного ефекту.

6. Вибрати для застосування той метод протидії даній загрозі інформаційній безпеці, для якого величина (4) є найбільшою.

Таким чином, постановка задачі на *оптимізацію* для вибору оптимального за економічними показниками методу протидії даній загрозі інформаційній безпеці може бути записана як задача максимізації такого виразу:

$$I_e = \max_m \left\{ P_k \left[V_k + B_k \right] - A - P_m (V_n + B_m) - P(k \mid m) \left[V_{km} + B_{km} \right] \right\}. \qquad (5)$$

У формулі (5) максимум береться за усіма можливими методами протидії заданій загрозі інформаційній безпеці.

У випадку, коли таких загроз інформаційній безпеці є декілька, потрібно здійснити спочатку оптимізацію окремо за методами протидії для кожної із загроз, а потім вже вибрати метод агрегації *додаткових* критеріїв, які характеризують *різні* загрози (здійснити це можна, наприклад, за [9]).

Висновки

Побудовано математичну модель для розрахунку економічної ефективності для довільного методу протидії загрозам інформаційній безпеці. В основу моделі покладено урахування того, що методи протидії загрозам інформаційній безпеці змінюють як імовірність розгортання загрози у часі, так і характеристики загрози. Отримано умови, при виконанні яких створювати механізм протидії заданій загрозі інформаційній безпеці є економічно доцільним і показано, що ефект може носити пороговий характер. Це дозволяє здійснити відбракування економічно неефективних методів протидії загрозам інформаційній безпеці вже на етапі їхнього аналізу. Виведено загальну формулу для розрахунку економічного ефекту від запровадження механізму протидії заданій загрозі інформаційній безпеці. Побудовано алгоритм вибору оптимального методу протидії загрозам інформаційній безпеці за його впливом на результати економічної діяльності та наведено алгоритм її розв'язання.

1. *Стратегія* управління інформаційною безпекою / [Андреєв В.І., Козюра В.Д., Скачек Л.М., Хорошко В.О.]. — К.: ДУІКТ, 2007. — 277 с.

2. *Основи* інформаційної безпеки / [Андреєв В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є.]. — К.: Вид. ДУІКТ, 2009. — 292 с.

3. *Методи* керування інформаційною безпекою; під ред. проф. В.О. Хорошка. — Севастополь: СНУЯЕтаП, 2010. — 328 с.

4. *Вишневська Н.С.* Аналіз методів оцінки ризиків інформаційного простору / Н.С. Вишневська // Інформаційна безпека. — 2013. — № 4(12). — С. 5–7.

5. *Mas-Collel A.* Microeconomic Theory / A. Mas-Collel, M. D. Whinston, J. R. Green. — Oxford : Oxford University Press, 1995. — 977 p.

6. *Gordon L.A.* The Economics of Information Security Investment / L.A. Gordon, M.P. Loeb // ACM Transactions on Information and System Security. — 2002. — Vol. 5, №4. — P. 438–457.

7. *Левченко Є.Г.* Показники продуктивності витрат на захист інформації / Є.Г. Левченко, Р.Б. Прус, Д.І. Рабчун // Безпека інформації. — 2012. — № 2(18). — С. 6–11.

8. *Хорошко В.О.* Оптимізація параметрів систем захисту в мережах передачі інформації / В.О. Хорошко, Ю.Є. Хохлачова // Інформатика та математичні методи в моделюванні. — 2013. — Т. 3, № 1. — С. 69–74.

9. *Новиков Д.А.* Теория управления организационными системами / Д.А. Новиков. — М.: Физматлит, 2007. — 584 с.

Надійшла до редакції 12.12.2014