

ЗАСТОСУВАННЯ ПОВНОЇ ГРУПИ ПОДІЙ ДЛЯ ОБЧИСЛЕННЯ ІНТЕГРАЛЬНОГО РИЗИКУ

О. Є. Архипов^{1, а}, Г. Г. Мелішкевич¹

¹Національний технічний університет України «Київський політехнічний інститут»

Анотація

В роботі представлено математично обгрунтовану модель розрахунку середнього ризику через повну групу подій, що дозволяє використовувати її для визначення рівня захищеності інформаційних ресурсів системи з комплексними загрозами.

Ключові слова: загроза, ризик, захищеність системи, повна група подій, множинні зарози, ймовірнісний параметр ризику

Вступ

Інформація - найцінніший товар сьогодення. Це стратегічний ресурс, що лежить в основі прогресу сучасного світу. А отже і успіх ведення бізнесу залежить від того, наскільки цінна для нього інформація захищена. Сфера інформаційних технологій активно розвивається, що дає можливість зловмисникам використовувати значні ресурси та проводити дослідницьку роботу. А отже організації всіх типів та розмірів постійно стикаються із зовнішніми загрозами та атаками, через які стає неможливим визначити, коли та яким чином вони досягнуть своїх цілей, що в свою чергу означає «ризик» для підприємства в цілому. Для уникнення непередбачених збиткових ситуацій, пов'язаних із втратою, порушенням цілісності чи доступності інформаційних ресурсів компанії, необхідно періодично проводити аудит ризиків системи, визначати рівень можливих збитків і на основі аналітичних даних приймати рішення щодо прийняття чи запобігання ризику.

Метою дослідження стало представлення математично обгрунтованої моделі розрахунку ризику, що враховує комплексні загрози системи.

Методика досліджень

Важливим показником рівня безпеки інформаційної системи (ІС) організації, який дозволяє врахувати в загальному вигляді вплив усієї множини загроз, актуальних для даної ІС, є показник інтегрального (узагальненого) ризику. Його знаходження – це остання завершальна стадія аналізу і оцінки ризиків, в ході якої результати представляються профілем ризиків і відображаються в скалярний показник R .

У тривіальному випадку ризик є функцією виду:

$$r = p(t)q(t), \quad (1)$$

де $p(t)$ – ймовірність реалізації деякої загрози по відношенню до конкретного інформаційного ресурсу IR ,

а $q(t)$ – величина збитку, заподіяного реалізацією цієї загрози. У більш загальній постановці, коли існує множина загроз $T = \{t_1, t_2, \dots, t_m\}$, ймовірність реалізації кожної з яких щодо ресурсу IR дорівнює $p(t_i)$, $i = \overline{1, m}$, причому загрози можуть бути сумісними, застосовується формула:

$$R = \sum_{i=1}^m p(t_i)p(t_i), \quad (2)$$

відома як формула сумарного ризику. Однак, як показано в [1], у разі наявності сумісних загроз наведена формула дає завищені значення ризику, її коректне застосування можливе лише у випадку, коли множина загроз – це повна група подій. Тому в [1] для довільної вихідної множини загроз запропоновано процедуру її трансформації у множину комплексних загроз, які утворюють повну групу й наразі дозволяють застосування формули сумарного ризику. Аналогічна процедура використовується і у випадку, коли одна загроза t здатна впливати на стан кількох інформаційних ресурсів, внаслідок чого виникає множина відповідних сумісних втрат. В цьому разі повна група формується з можливих наборів уражених ресурсів [1].

У найбільш загальному випадку маємо множину загроз, елементи якої можуть випадковим чином реалізовуватися щодо елементів множини інформаційних ресурсів. Для цієї ситуації в [1] також наведено процедуру трансформації множин вихідних загроз та ресурсів у певні вторинні комплекси загроз та наборів уражених ресурсів, однак ця третя процедура, на відміну від двох попередніх, розроблена за індукцією і не супроводжується доведенням того, що наслідки трансформації утворюють повну групу.

Викладені нижче матеріали мають «компенсувати» цю прогалину й підтвердити слушність індуктивного введеної процедури.

^аsonet0515@gmail.com

Позначимо множину загроз інформаційним ресурсам ІС як:

$$T = \{t_1, t_2, \dots, t_m\} \quad (3)$$

Утворена на базі цієї множини повна група комплексних загроз матиме вигляд [1]:

$$T = \{\langle t_1, t_2, \dots, t_m \rangle, \langle t_1, t_2, \dots, \bar{t}_m \rangle, \langle t_1, t_2, \dots, \bar{t}_{m-1}, t_m \rangle, \langle t_1, t_2, \dots, \bar{t}_{m-1}, \bar{t}_m \rangle, \dots, \langle \bar{t}_1, \bar{t}_2, \dots, \bar{t}_m \rangle\}, \quad (4)$$

де \bar{t}_i - подія протилежна t_i .

Усі отримані вище комплексні загрози є попарно несумісними, а сума їх ймовірностей дорівнює одиниці.

Позначимо множину інформаційних ресурсів ІС як:

$$IR = \{IR_1, IR_2, \dots, IR_n\}. \quad (5)$$

Тоді повна група, утворена з наборів уражених ресурсів, становить:

$$IR = \{\langle IR_1, IR_2, \dots, IR_n \rangle, \langle IR_1, IR_2, \dots, \bar{IR}_n \rangle, \langle IR_1, IR_2, \dots, \bar{IR}_{n-1}, IR_n \rangle, \langle IR_1, IR_2, \dots, \bar{IR}_{n-1}, \bar{IR}_n \rangle, \dots, \langle \bar{IR}_1, \bar{IR}_2, \dots, \bar{IR}_n \rangle\} \quad (6)$$

При побудові групи подій, виниклих в результаті реалізації загроз щодо сукупності інформаційних ресурсів, вважатимемо, що будь-яка з комплексних загроз може бути реалізована відносно кожного з наборів ресурсів. При цьому, наприклад, подія, яка полягає в тому, що дія першої ($k = 1$) комплексної загрози $\langle t_1, t_2, \dots, t_m \rangle$ призведе до появи ураженого ресурсу виду: $\{\bar{IR}_1, IR_2, \dots, IR_n\}$, матиме ймовірність $p_1, p_2, \dots, p_m \cdot P_{1\bar{IR}_1, IR_2, \dots, IR_n}$.

Підсумуємо ймовірність усіх подій, що входять до побудованої групи:

$$p_1, p_2, \dots, p_m \cdot P_{1IR_1, IR_2, \dots, IR_n} + p_1, p_2, \dots, p_m \cdot P_{1\bar{IR}_1, IR_2, \dots, IR_n} + \dots + p_1, p_2, \dots, p_m \cdot P_{1\bar{IR}_1, \bar{IR}_2, \dots, \bar{IR}_n} + \bar{p}_1, p_2, \dots, p_m \cdot P_{2IR_1, IR_2, \dots, IR_n} + \bar{p}_1, p_2, \dots, p_m \cdot$$

$$\begin{aligned} & \cdot P_{2\bar{IR}_1, IR_2, \dots, IR_n} + \dots + \bar{p}_1, p_2, \dots, p_m \cdot P_{2\bar{IR}_1, \bar{IR}_2, \dots, \bar{IR}_n} + \\ & + \dots + \bar{p}_1, p_2, \dots, p_m \cdot P_{nIR_1, IR_2, \dots, IR_n} + \bar{p}_1, p_2, \dots, p_m \cdot \\ & \cdot P_{n\bar{IR}_1, IR_2, \dots, IR_n} + \dots + \bar{p}_1, p_2, \dots, p_m \cdot P_{n\bar{IR}_1, \bar{IR}_2, \dots, \bar{IR}_n} = \\ & = p_1, p_2, \dots, p_m \cdot (P_{1IR_1, IR_2, \dots, IR_n} + P_{1\bar{IR}_1, IR_2, \dots, IR_n} + \\ & + P_{1\bar{IR}_1, \bar{IR}_2, \dots, \bar{IR}_n}) + \bar{p}_1, p_2, \dots, p_m \cdot (P_{2IR_1, IR_2, \dots, IR_n} + \\ & P_{2\bar{IR}_1, IR_2, \dots, IR_n} + P_{2\bar{IR}_1, \bar{IR}_2, \dots, \bar{IR}_n}) + \bar{p}_1, p_2, \dots, p_m \cdot \\ & \cdot (P_{nIR_1, IR_2, \dots, IR_n} + P_{n\bar{IR}_1, IR_2, \dots, IR_n} + \\ & + P_{n\bar{IR}_1, \bar{IR}_2, \dots, \bar{IR}_n}) = p_1, p_2, \dots, p_m \cdot 1 + \\ & + \bar{p}_1, p_2, \dots, p_m \cdot 1 + \bar{p}_1, p_2, \dots, p_m \cdot 1 = \\ & = p_1 \cdot (p_2 p_3, \dots, p_m + \bar{p}_2 p_3, \dots, p_m + \dots + \bar{p}_2 p_3, \dots, p_m) + \\ & + \bar{p}_1 \cdot (p_2 p_3, \dots, p_m + \bar{p}_2 p_3, \dots, p_m + \dots + \bar{p}_2 p_3, \dots, p_m) = \\ & = (p_2 p_3, \dots, p_m + \bar{p}_2 p_3, \dots, p_m + \dots + \bar{p}_2 p_3, \dots, p_m) \cdot \\ & \cdot (p_1 + \bar{p}_1) = (p_2 p_3, \dots, p_m + \bar{p}_2 p_3, \dots, p_m + \dots + \\ & + \bar{p}_2 p_3, \dots, p_m) \cdot 1 = \dots = 1 \end{aligned} \quad (7)$$

Висновки

Таким чином, сума ймовірностей всіх подій, що увійшли до складу побудованої групи, дорівнює одиниці. Зважаючи, що всі ці події до того ж є попарно несумісними, слід вважати, що побудована група подій є повною і для обчислення значення інтегрального ризику може бути застосована формула сумарного ризику.

За допомогою даної моделі можливо також обчислювати ризики щодо окремих інформаційних активів, на які націлені сукупні загрози. Реалізація представленої методології приводить до необхідності трансформації вихідної ризикової ситуації, що склалась в результаті дії сукупності реальних деструктивних сумісних подій, до ризикової ситуації, що описується дією повної групи комплексних випадкових подій, що формуються з вихідної множини реальних.

Перелік використаних джерел

1. Архипов А. Е. Применение среднего риска для оценивания эффективности защиты информационных систем. — Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — Київ, 2007. — Вип.1(14). — 60-67 с.