УДК 519.213

В.В. Мохор, д-р техн. наук, ІПМЕ ім. Г.Є. Пухова НАН України, м. Київ,
В.В. Цуркан, ІСЗЗІ НТУУ «КПІ», м. Київ

ОЦІНЮВАННЯ ЗАКОНУ РОЗПОДІЛУ ВЕЛИЧИНИ ЗБИТКІВ УНАСЛІДОК РЕАЛІЗАЦІЇ ЗАГРОЗИ «ВІДСУТНІСТЬ АБО НЕДОСТАТНІСТЬ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ»

The problem of estimation of size distribution law of damages in the absence or insufficient sample size of the universe and the initial data suggested approach to finding the most expected value of losses due to information security threats.

Забезпечення функціональності комп'ютерної техніки, що використовується в організації, здійснюється через регулярне технічне обслуговування. Якщо воно не проводилось або був проведений недостатній обсяг робіт у процесі технічного обслуговування, можуть виникнути непередбачувані збитки внаслідок реалізацій загрози «Відсутність або недостатність технічного обслуговування» [1], наприклад:

1. Батареї джерела безперебійного живлення внаслідок відсутності технічного обслуговування можуть мати недостатню ємність. Внаслідок цього джерело безперебійного живлення не зможе підтримувати живлення при вимкненій електроенергії, що призведе до втрат інформації або виходу з ладу джерела безперебійного живлення. Для зазначеної ситуації, за даними на серпень 2010 року втрати можуть дорівнювати [2]:

– до 2000 гривень за відновлення інформації в залежності від обсягу накопичувача, складності та терміновості виконання робіт; при цьому вартість виконання робіт може змінюватися у процесі відновлення інформації;

– до 500 гривень, у залежності від категорії ремонту джерела безперебійного живлення або від 300 до 7000 тисяч гривень за нове джерело безперебійного живлення у разі неможливості ремонту старого.

2. Лазерний принтер може вийти з ладу через перегрів тому, що вентиляційна решітка не очищується згідно інструкції. Внаслідок цього втрати можуть дорівнювати [2]:

– від 100 до 300 гривень у залежності від складності ремонту без урахування вартості запасних частин;

– від 600 до 600000 гривень при купівлі нового лазерного принтера в залежності від його марки.

3. Комп'ютерна техніка, що знаходяться у серверній кімнаті, влітку може перегріватися від високої температури через недостатнє охолодження та кондиціонування приміщення (наприклад, відсутній чи несправний кондиціонер), що може призвести до виходу з ладу серверів. Для запобігання цьому, кондиціонери повинні регулярно обслуговуватись та підтримуватись в

чистоті з метою забезпечення їхнього надійного та безвідмовного функціонування. Інакше, внаслідок недотримання зазначених вимог, витрати можуть дорівнювати, наприклад [2]:

– від 100 до 500 гривень у залежності від складності ремонту без урахування вартості запасних частин та фреону;

– від 1300 до 80000 гривень при купівлі нового кондиціонера в залежності від його моделі;

– від 500 до 3000 гривень за відновлення інформації в залежності від обсягу накопичувача, складності та терміновості виконання робіт. При цьому вартість виконання робіт може змінюватися у процесі відновлення інформації;

– від 800 гривень у залежності від складності ремонту сервера без урахування вартості комплектуючих деталей;

– від 3000 до 700000 гривень при купівлі нового сервера в залежності від його моделі.

Припустимо, що в організації з метою забезпечення безпеки інформації реалізована система управління інцидентами, функціонування якої направлене на виявлення інцидентів, котрі сприяють появі загроз безпеці інформації [3], зокрема загрози: *відсутність або недостатність технічного обслуговування*. При цьому одним із ключових процесів системи управління інцидентами в контексті безпеки інформації є:

– виявлення небезпеки та оповіщення про неї;

– збирання інформації про небезпеку з метою визначення чи є вона інцидентом;

– ***облік кількості інцидентів***.

У свою чергу, для оцінки процесу технічного обслуговування в організації використовується модель зрілості Cobit, яка містить *п'ять градацій* її рівня [4]:

1 – початковий. В організації усвідомлюють існування проблем пов'язаних з забезпеченням безпеки інформації та необхідність їх вирішення. При цьому відсутні стандартизовані процеси та організаційний підхід до управління;

2 – інтуїтивний. В організації процеси досягли рівня при котрому різні працівники, які виконують одну й ту ж задачу, використовують схожі процедури. При цьому відсутнє формалізоване навчання та інформування про прийняті в організації процедури, відповідальність за котрі повністю покладена на працівників;

3 – визначений. В організації процедури стандартизовані, документально оформлені та доводяться до відома працівників в процесі навчання. При цьому процедури прості та являють собою формалізований варіант практики;

4 – управляємий. В організації існує можливість контролю та оцінки ступеня відповідності прийнятим процедурам. Процеси постійно

вдосконалюються та відповідають загальноприйнятій практиці. Автоматизовані та інструментальні засоби для управління процесами використовуються епізодично;

5 – оптимізований. В організації процеси визначені відповідно до найкращих практик, котрі базуються на результатах неперервного вдосконалення та порівняння з іншими організаціями завдяки використанню моделей зрілості процесів.

Визначені рівні виступають характеристиками профілів зрілості процесу технічного обслуговування, які в організації сприймають як опис можливого стану речей в теперішньому та майбутньому. При цьому перехід до вищого рівня можливий тільки при виконанні всіх вимог попередніх рівнів.

З урахуванням вище наведених вихідних даних, необхідно оцінити закон розподілу величини збитків унаслідок реалізації загрози «Відсутність або недостатність технічного обслуговування» за умови відсутності або недостатності обсягу вибірки з генеральної сукупності початкових даних для оцінювання.

Нехай x – неперервна випадкова величина збитків унаслідок реалізації загрози безпеці інформації з законом розподілу $f(x)$. До того ж, за одиницю вимірювання величини збитків вважатимемо тисячу гривень. Для вибору виду закону розподілу $f(x)$ визначимо наступні умови і обмеження [5]:

1. Функція $f(x)$ – неперервна в кожній точці x_0 інтервалу $(0,\infty)$, тобто виконується наступна рівність

$$\lim_{x \to x_0} f(x) = f(x_0).$$

2. Функція $f(x)$ – гладка, тобто має неперервну похідну $f'(x)$ в кожній точці x інтервалу $(0,\infty)$.

3. Функція $f(x)$ – невід'ємна

$$f(x) \geq 0.$$

4. Значення x величини збитків належать інтервалу $(0,\infty)$ і, як наслідок,

$$\int_0^\infty f(x)dx = 1.$$

5. Імовірність нульових збитків практично дорівнює нулю.

6. Існує скінченна, менша за одиницю ймовірність найбільш очікуваного значення $x_{оч.}$ величини можливих збитків.

7. Функція $f(x)$ монотонно зростає від нуля до свого максимуму $f(x_{оч.})$, після чого спадає, тобто в усіх точках інтервалу $(0,\infty)$ друга похідна функції $f(x)$ від'ємна

$$f''(x) < 0.$$

8. Імовірність значних збитків практично дорівнює нулю.

Після того, як вибрано закон розподілу $f(x)$ з урахуванням зазначених умов та обмежень, слід:

1. Визначити сутність та кількість параметрів, котрими можна задати закон розподілу $f(x)$.

При цьому, слід зауважити, що функція $f(x)$ може бути визначена одним, двома або трьома параметрами. Їх можна поділити на три основних види, – параметри положення μ, масштабу λ, форми θ, кожен з котрих має визначений фізичний та геометричний зміст [6]. До того ж

– параметр положення μ характеризує положення області можливих значень величини збитків на числовій осі;

– параметр масштабу λ визначає масштаб вимірювання значень величини збитків;

– параметр форми θ визначає форму кривої розподілу величини збитків.

У зв'язку з цим, для позначення закону розподілу величини збитків у загальному випадку будемо використовувати наступний символ $f_x(\mu,\lambda,\theta)$. Його форма може змінюватися в залежності від кількості параметрів, котрі визначаються по контексту задачі оцінювання ймовірності реалізації загрози безпеці інформації.

2. Провести дослідження щодо вибору виду закону розподілу величини збитків унаслідок реалізації загрози безпеці інформації з урахуванням:

– зазначених умов і обмежень, котрим повинен задовольняти закон розподілу $f(x)$;

– визначених параметрів, котрими задається $f(x)$.

3. Обчислити оцінки параметрів вибраного експериментально закону розподілу величини збитків унаслідок реалізації загрози безпеці інформації.

При обчисленні оцінок, їх прийнято вважати хорошими, якщо вони обґрунтовані, незміщені, ефективні. Одним із методів знаходження точкових оцінок, котрий задовольняє зазначеним вимогам є метод максимальної правдоподібності [7]. Його суть полягає в знаходженні максимуму функції правдоподібності.

Оскільки, X – параметр, котрий потрібно знайти. Тоді згідно з принципом максимальної правдоподібності в якості оцінки слід вибрати те значення параметра X, для котрого функція правдоподібності $L(x \mid X) = f(x \mid X)$ приймає максимум. При цьому її стаціонарні значення є коренями рівняння

$$L'(x \mid X) = \frac{\partial L(x \mid X)}{\partial X} = 0.$$

Після того, як буде знайдено всі локальні максимуми функції правдоподібності, серед них слід вибрати найбільший, котрий і буде

шуканим значенням параметра X.

Наведені три пункти можна вважати методикою знаходження найбільш очікуваної величини збитків $x_{оч.}$. Відповідно до сформованої методики, по-перше, за умовою задачі визначимо параметри, котрими можна задати вид закону розподілу $f(x)$. Для ситуації, що розглядається, це

– кількість інцидентів пов'язаних з відсутністю або недостатністю технічного обслуговування;

– рівень зрілості процесу технічного обслуговування, $\overline{1,5}$.

Оскільки вид $f(x)$ визначається двома параметрами, то закон розподілу величини збитків унаслідок реалізації загрози безпеці інформації матиме наступну форму запису

$$f_X(\mu,\lambda).$$

По-друге, користуючись запропонованими умовами і обмеженнями, проведемо дослідження в системі Maple 13 щодо вибору виду закону розподілу величини збитків унаслідок реалізації загрози «Відсутність або недостатність технічного обслуговування». За результатами проведеного експерименту встановлено, що для опису залежності ймовірності реалізації загрози безпеці інформації від величини збитків доцільно взяти класичний закон розподілу Вейбула-Гніденко

$$f_X(a,c)=\frac{c}{a}\left(\frac{x}{a}\right)^{c-1}\exp\left(-\left(\frac{x}{a}\right)^{c}\right),$$

який характеризується параметрами: a - масштабу, c - форми. При цьому, в процесі дослідження було з'ясовано, що параметр a слід використовувати для опису кількості інцидентів пов'язаних із відсутністю або недостатністю технічного обслуговування, а параметр c - рівня зрілості процесу технічного обслуговування.

Для прикладу, розглянемо ситуацію, коли в організації технічне обслуговування досягло рівня, при котрому різні працівники виконують одну й ту ж задачу та використовують схожі процедури в контексті технічного обслуговування. При цьому не існує формалізованого навчання та інформування про прийняті в організації процедури, відповідальність за використання котрих повністю покладена на окремих працівників. Згідно з описом рівнів моделі зрілості, ситуація, що розглядається, відповідає другому рівню, тобто $c=2$.

Користуючись системою Maple 13, промоделюємо випадки, коли було зареєстровано 1, 5, 10 інцидентів пов'язаних з зазначеною загрозою. Графічне представлення отриманих залежностей «імовірності реалізації загрози «Відсутність або недостатність технічного обслуговування», розподіленої по закону Вейбула-Гніденко від величини збитків матиме вид представлений на рисунку 1.

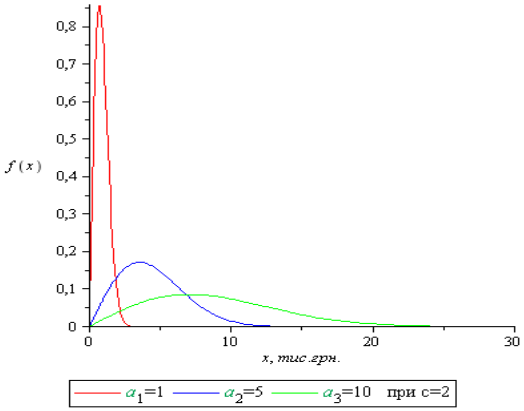

Рис. 1. Закон розподілу величини збитків унаслідок реалізації загрози «Відсутність або недостатність технічного обслуговування»

По-третє, знайдемо найбільш очікувані значення $x_{оч.}$ величини збитків унаслідок реалізації загрози «Відсутність або недостатність технічного обслуговування». Для цього, спочатку виразимо функцію $f(x)$ через логарифм і знайдемо першу похідну, тобто:

$$\left(\ln f(x)\right)' = \left(\ln\left(\frac{c}{a}\left(\frac{x}{a}\right)^{c-1} e^{-\left(\frac{x}{a}\right)^{c}}\right)\right)' = \left(\ln\frac{c}{a} + \ln\left(\frac{x}{a}\right)^{c-1} + \ln\left(e^{-\left(\frac{x}{a}\right)^{c}}\right)\right)' =$$

$$= \left(\ln c - \ln a + (c-1)\ln x - (c-1)\ln a - \left(\frac{x}{a}\right)^{c}\right)' =$$

$$= \left(\ln c\right)' - \left(\ln a\right)' + \left((c-1)\ln x\right)' - \left((c-1)\ln a\right)' - \left(\left(\frac{x}{a}\right)^{c}\right)' \times \left(\frac{x}{a}\right)' =$$

$$= 0 - 0 + \frac{c-1}{x} - 0 - c\left(\frac{x}{a}\right)^{c-1}\frac{1}{a} = \frac{c-1}{x} - \frac{c}{a}\left(\frac{x}{a}\right)^{c-1}.$$

Оскільки, в організації технічне обслуговування знаходиться на другому рівні зрілості ($c = 2$), то вираз для похідної перепишемо наступним чином

$$\frac{\partial\left(\ln f(x \mid X)\right)}{\partial X} = \frac{c-1}{x} - \frac{c}{a}\left(\frac{x}{a}\right)^{c-1} = \frac{1}{x} - \frac{2x}{a^2}. \qquad (1)$$

Застосуємо принцип максимальної правдоподібності для знаходження найбільш очікуваної величини збитків $X = x_{оч.}$ для випадків, коли було

зареєстровано один, п'ять, десять інцидентів ($a_1 = 1, a_2 = 5, a_3 = 10$). Для цього, результат диференціювання (1) прирівняємо до нуля

$$\frac{1}{x} - \frac{2x}{a^2} = 0$$

і розв'яжемо отримане рівняння щодо x. Внаслідок цього отримаємо

$$x = \sqrt{\frac{a^2}{2}} = \frac{a}{\sqrt{2}}.$$

Звідси,

– при $a_1 = 1$, $x^1 = x^1_{оч.} = \frac{a_1}{\sqrt{2}} = \frac{1}{\sqrt{2}} = 0{,}707$;

– при $a_2 = 5$, $x^2 = x^2_{оч.} = \frac{a_2}{\sqrt{2}} = \frac{5}{\sqrt{2}} = 3{,}535$;

– при $a_3 = 10$, $x^3 = x^3_{оч.} = \frac{a_3}{\sqrt{2}} = \frac{10}{\sqrt{2}} = 7{,}07$.

Перевіримо правильність проведених обчислень найбільш очікуваних значень величини збитків. Для цього, обчислимо значення моди $\hat{x}$ закону розподілу Вейбула-Гніденко

$$\hat{x} = a\left(\frac{c-1}{c}\right)^{\frac{1}{c}}$$

і порівняємо отримані значення зі знайденими $x_{оч.}$, тобто

– при $a_1 = 1$

$$\hat{x}^1 = a_1 \cdot \left(\frac{c-1}{c}\right)^{\frac{1}{c}} = 1 \cdot \left(\frac{2-1}{2}\right)^{\frac{1}{2}} = \left(\frac{1}{2}\right)^{\frac{1}{2}} = \sqrt{0{,}5} = 0{,}707;$$

– при $a_2 = 5$

$$\hat{x}^2 = a_2 \cdot \left(\frac{c-1}{c}\right)^{\frac{1}{c}} = 5 \cdot \left(\frac{2-1}{2}\right)^{\frac{1}{2}} = 5\left(\frac{1}{2}\right)^{\frac{1}{2}} = 5\sqrt{0{,}5} = 5 \cdot 0{,}707 = 3{,}535;$$

– при $a_3 = 10$

$$\hat{x}^3 = a_3 \cdot \left(\frac{c-1}{c}\right)^{\frac{1}{c}} = 10 \cdot \left(\frac{2-1}{2}\right)^{\frac{1}{2}} = 10 \cdot \left(\frac{1}{2}\right)^{\frac{1}{2}} = 10 \cdot \sqrt{0{,}5} = 10 \cdot 0{,}707 = 7{,}07.$$

Таким чином, $x^1_{оч.} = \hat{x}^1 = 0{,}707$, $x^2_{оч.} = \hat{x}^2 = 3{,}535$, $x^3_{оч.} = \hat{x}^3 = 7{,}07$.

Отже, на підставі проведеного аналізу отриманих результатів, можна зробити наступні висновки:

1. Закон розподілу величини збитків є неперервною, гладкою функцією, котра монотонно зростає від нуля до свого максимуму, після чого спадає при збільшенні величини можливих збитків.

2. На графіку залежності «ймовірність реалізації загрози – величина збитків» слід виділити чітко виражені три точки:

– при $x = 0$, $f(x) \to 0$ – ймовірність нульових збитків практично дорівнює нулю, оскільки хоча б незначні збитки існують завжди;

– при $x = x_{оч}$, $f(x) \to \max$ – ймовірність найбільш очікуваної величини збитків унаслідок реалізації загрози «Відсутність або недостатність технічного обслуговування» скінченна і максимальна;

– при $x \to \infty$, $f(x) \to 0$ – ймовірність значних збитків, як практично неможливої події, близька до нуля.

3. Вид вибраного закону розподілу Вейбула-Гнеденко, відповідає визначеним аспектам, описуючи залежність ймовірності реалізації загрози «Відсутність або недостатність технічного обслуговування» від величини збитків, що дає підстави стверджувати про адекватність вибраної моделі.

4. Застосування принципу максимальної правдоподібності дозволяє знайти найбільш очікуване значення величини збитків $x_{оч.}$, при котрому закон розподілу $f(x)$ має максимальне значення. При цьому особливість використання зазначеного методу полягає в тому, що він застосовується за умови відсутності або недостатності початкових даних.

5. Використання моди закону розподілу Вейбула-Гніденко для перевірки правильності обчислень $x_{оч.}$ дозволило підтвердити правильність отриманих значень за умови зміни кількості інцидентів a.

1. *G 2.5 Fehlende oder unzureichende Wartung* [Електронний ресурс]//G 2 Organisatorische Mängel/IT-Grundschutz-Kataloge/Das Bundesamt für Sicherheit in der Informationstechnik. – 2009. – Режим доступу: https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/kataloge/g/g02/g02005.html. – Дата доступу: червень 2010. – Назва з екрану.

2. *Каталог товаров и услуг Украины* [Електронний ресурс]. – 2010. – Режим доступу: http://price.ua/. – Дата доступу: серпень 2010. – Назва з екрану.

3. *ISO/IEC TR 18044:2004*. Information technology. Security techniques. Information security incident management. – Чинний з 2004-10-25. - London: British Standards Institution, 2004. – 60 с.

4. *Cobit 4.1*: [Перевод на русский язык И.А. Вдовин]. – М.: Аудит и контроль информационных систем, 2008. – 240 с.

5. *Фихтенгольц Г.М.* Основы математического анализа. – Том I. – М.: Издательство «Наука», 1968. – 440 с.

6. *Вадзинский Р.Н.* Справочник по вероятностным распределениям. – СПб.: Наука, 2001. – 295 с.

7. *Кендалл М., Стюарт А.* Статистические выводы и связи. – М.: Главная редакция физико-математической литературы изд. - ва «Наука», 1973. – 899 с.

Поступила 6.10.2010р.