УДК 004.056.5 (045)

КРИТЕРІЇ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ОРГАНІЗАЦІЇ СЕРВЕРНИХ ПЛАТФОРМ

В. О. Борозніченко, Ю.О. Максімов, А. Б. Петренко

Національний авіаційний університет

kszi@ukr.net

Обґрунтовано необхідність оцінки ефективності заходів щодо захисту інформації в інформаційних комп'ютерних мережах. Описано критерії очікуваного значення, критерії «очікуване значення — дисперсія» та критерії граничного рівня. Вказано методику вибору ефективного вільного простору в оперативній пам'яті. Проведено розрахунок для встановлення профілактичного ремонту серверу, щоб мінімізувати втрати через несправність. Визначено рівень схильності до ризику певного серверу.

Ключові слова: інформаційний ризик, сервер, профілактичний ремонт, критерій, мінімізування втрат.

The necessity of evaluating the effectiveness of measures to protect information in computer information networks. Described criteria expected value criteria "expected value — variance" and the threshold criteria. Specified methods of effective space in memory. The calculation to establish preventive maintenance server in order to minimize losses due to malfunction. The level of exposure to the risk of a server.

Keywords: information risk, server, preventive maintenance, criterion, loss minimization.

Вступ

На сьогодні питання інформаційної безпеки з кожним днем усе більше загострюється і є одним з найважливіших для будь-якого підприємства чи установи. Інформаційні технології стрімко розвиваються, а тому, крім безперечної користі, зростає і кількість проблем у сфері інформаційної безпеки.

Безпека інформації передбачає відсутність неприпустимого ризику, пов'язаного з витоком інформації технічними каналами, несанкціонованими і ненавмисними діями на ресурси, що використовуються в автоматизованій системі будь-якого підприємства.

Слід зауважити, що темпи розвитку сучасних інформаційних технологій значно випереджають темпи розробки рекомендаційної та нормативно-правової бази, керівних документів. Тому вирішення питання щодо розробки ефективної політики інформаційної безпеки на сучасному підприємстві безпосередньо пов'язане з проблемою вибору критеріїв і показників захищеності, а також ефективності корпоративної системи захисту інформації. Сучасні методи управління ризиками дозволяють вирішити ряд завдань перспективного стратегічного розвитку підприємства.

Головний напрямок у вирішенні проблем інформаційної безпеки — це інтеграція всіх засобів підприємства в єдиний автоматизований комплекс безпеки [1].

У сучасних умовах одне з актуальних практичних завдань — оцінювання ефективності заходів щодо захисту інформації в інформаційних комп'ютерних системах. Дослідження цього завдання дає можливість розробникам і власникам інформаційних комп'ютерних систем одержувати обґрунтовану оцінку різних методів та засобів захисту інформації.

Прийняття рішень у процесі життєвого циклу автоматизованої системи — тема, що виникла і розвивається внаслідок збільшення кількості ризиків на інформаційну систему та необхідності термінового вирішення проблем, які виникають як наслідок дестабілізуючої дії ризику.

Мета статті

Метою даної статті є визначення методів та засобів прийняття рішень в умовах ризику, на прикладі профілактичного ремонту серверу. Досягнення стабільної роботи серверу на тривалий час, запобігання серйозним поломкам та збільшення терміну його служби, за рахунок необхідного нагляду за технікою, систематичного контролю комп'ютерного обладнання.

Основна частина

Важливим моментом під час розрахунків необхідності профілактичного ремонту серверу є взяття до уваги місце встановлення даного серверу, температура в приміщенні, години його експлуатації та інші характерні відмінності.

Прикладом може бути використання комп'ютерної техніки в зонах великих температур, коли змінюються властивості перехідних опорів, що руйнують захисні покриття.

Велике значення також має постійна зміна температур, вологість повітря, сонячна радіація, пил, пісок та підвищений тиск.

У разі нерегулярного чищення певних деталей комп'ютера від пилу може підвищитися температура в корпусі системного блоку, що може призвести до перегрівання окремих його частин та виходу з ладу комплектуючих. Для уникнення цієї проблеми необхідно раз на тиждень протирати монітор, клавіатуру та системний блок (зовнішня частина) спеціальними вологими серветками. Кожен місяць існує необхідність очищення системного блоку всередині, дотримуючись усіх правил безпеки. Профілактичне очищення комп'ютера необхідно проводити згідно з умовами його розташування в приміщенні.

Далі наведено розрахунки для серверу розташованого у приміщенні, яке відповідає санітарно-профілактичним нормам на території України.

Важливим етапом для продовження життєвого циклу серверу є профілактична технічна діагностика, що включає в себе дослідження станів об'єктів діагностування і розробляє методи їх розпізнання та визначає принципи проектування.

Технічна діагностика складається з:

– перевірки працездатності сервера;

– пошуку несправних компонентів системи та встановлення їх дефектів;

– прогнозування роботи системи на певний проміжок часу.

При виборі методу профілактично-технічного контролю необхідно враховувати, що необхідно отримати в кінцевому результаті та які параметри мають пройти перевірку.

Технічний контроль можна класифікувати на:

а) контроль працездатності;

б) прогнозуючий;

в) діагностичний.

Контроль здійснюється за рахунок методів та засобів контролю технічного стану, програмного та апаратного забезпечення. Існують як активні, так і пасивні засоби контролю.

Вибір методів і засобів профілактичного контролю здійснюється залежно від поставленої мети, завдання та бажаного отримання результату [4].

Якщо мова йде про перевірку комп'ютерних серверів на підприємстві, то доцільним буде вибір таких методів профілактичного контролю:

1) функціональний контроль — перевіряє спроможність сервера виконувати свої обов'язки;

2) функціонально-статичний контроль — перевіряє точність функціонування серверу, в діапазоні роботи при мінімальних та максимальних робочих частотах;

3) внутрішньосхемний контроль — перевірка правильності роботи здійснюється за рахунок подачі тестового впливу на внутрішні контрольні точки друкованих плат, при цьому з внутрішніх контактів контрольних точок цієї плати знімають реакції.

Нижче наведено розрахунок планового профілактичного ремонту серверу.

Критерій очікуваного значення

Використання критерію очікуваного значення зумовлено намаганням мінімізувати очікувані витрати на подолання ризикованих ситуацій. Використання очікуваних величин ризиків припускає можливість багаторазового розв'язання однієї й тієї самої задачі, доки не будуть отримані достатньо точні формули для розрахунку. Математично це має такий вигляд:

нехай x — випадкова величина з математичним сподіванням MX та дисперсією DX. Якщо $x_1, x_2, ..., x_n$ — значення випадкової величини x, тоді середнє арифметичне значення дорівнює $\bar{\bar{x}} = \frac{x_1 + x_2 + ... + x_n}{n}$, має дисперсію $\frac{DX}{n}$. Таким чином, коли $n \to \infty$

$$\frac{DX}{n} \to 0 \text{ та } \bar{x} \to MX .$$

При достатньо великому обсягу вибірки різниця між середнім арифметичним та математичним сподіванням наближається до 0 (гранична теорема теорії ймовірності). Використання критерію очікуваного значення виправдано у випадках, коли одне й те саме рішення необхідно приймати велику кількість разів [2].

Для доведення ефективності даного критерію наведемо такий приклад. Потрібно прийняти рішення про те, у який період необхідно проводити профілактичний ремонт серверу, щоб мінімізувати втрати через несправність. У випадках, коли ремонт буде проводитись часто, витрати на його обслуговування будуть великими при малих втратах у зв'язку з несправностями.

Оскільки не можна передбачити заздалегідь, коли виникне несправність, потрібно знайти ймовірність того, що сервер вийде з ладу в період часу t. У цьому й полягає елемент «ризику».

Математична картина така: сервер ремонтується індивідуально, якщо він зупинений через несправність.

Нехай, візьмемо за T кількість інтервалів часу, за яку виконується профілактичний ремонт усіх n серверів. Необхідно визначити оптимальне значення T, при якому мінімізуються загальні витрати на ремонт непрацюючих серверів та проведення розрахунку на один інтервал часу.

Нехай p_t — імовірність виходу з ладу одного серверу в момент t, а n_t — випадкова величина, що дорівнює кількості всіх машин, що вийшли з ладу в той самий момент. Нехай C_1 — витрати на ремонт зламаного серверу та C_2 — витрати на профілактичний ремонт однієї машини.

Застосування критерію очікуваного значення виправдано, якщо сервери працюють упродовж довгого періоду часу. При цьому очікувані витрати на один інтервал становлять:

$$\hat{I} \div_{\hat{a}} = \frac{C_1 * \sum_{t=1}^{T-1} M(n_t) + C_2 + n}{T},$$

де $M\ n_t$ — математичне сподівання кількості серверів, що вийшли з ладу в момент t.

Оскільки n_t має біноміальний розподіл з параметрами $n, p_t\ q$, то $M(n_t) = m * p_t$. Таким чином:

$$\hat{I} \div_{\hat{a}} = \frac{n * \sum_{t=1}^{T-1} p_t + C_2}{T}.$$

Необхідні умови оптимальності $T*$ мають вигляд:

$$\hat{I} \div_{\hat{a}}(T^* - 1) \geq \hat{I} \div_{\hat{a}}(T^*);$$

$$\hat{I} \div_{\hat{a}}(T^* + 1) \geq \hat{I} \div_{\hat{a}}(T^*).$$

Починаючи з малого значення T, визначають $\hat{I} \div_{\hat{a}}(T)$, доки не будуть виконані умови оптимальності. Нехай $C_1 = 100,\ C_2 = 10,\ n = 50$. Значення p_t наведено в табл. 1.

Таблиця 1

Застосування критерію очікуваного значення

T	p_t	$\sum_{t=1}^{T-1} p_t$	$\hat{I} \div_{\hat{a}}(T)$
1	0,05	0	$(50*(100*0+10))/1 = 500$
2	0,07	0,05	375
3	0,10	0,12	366,7
4	0,13	0,22	400
5	0,18	0,35	450
6	0,19	0,53	525
7	0,21	0,72	585
8	0,23	0,93	644

$$T^* \to \hat{A},\ \hat{I} \div_{\hat{a}}(T^*) \to 366,7.$$

Отже, виходячи із результатів обчислень, можна зробити висновок про те, що профілактичний ремонт необхідно проводити через три інтервали часу [2].

Критерій «очікуване значення — дисперсія»

Попередній критерій (критерій очікуваного значення) можна модифікувати таким чином, що його використання для нечастих подій було доцільним. Якщо *x* — випадкова величина з дисперсією *DX*, то середнє арифметичне $\vec{x}$ має дисперсію $\frac{DX}{n}$. Якщо DX зменшується і вірогідність того, що $\vec{x}$ близьке до MX, збільшується. З цього доцільно ввести критерій, в якому мінімізація дисперсії буде складовою максимізації очікуваного значення.

Для вищенаведеного прикладу застосуємо даний критерій. Потрібно знайти дисперсію витрат за один інтервал:

$$\hat{A}_T = \frac{C_1 * \sum_{t=1}^{T-1} (n_t) + nC_2}{T}.$$

Оскільки n_t, $t = \overline{-1, T-1}$ випадкові величини, то $\hat{A}_{\grave{O}}$ також випадкова; n_t має біноміальний розподіл з $M(n_t) = n * p_t$ та $D(n_t) = (n * p_t) * (1 - p_t)$.

Отже, підставляючи формули отримаємо:

$$D(\hat{A}_t) = D\left(\frac{C_1 * \sum_{t-1}^{T-1} (n_t) + nC_2}{T}\right) = \left(\frac{\tilde{N}_1}{T}\right)^2 D\left(\sum_{t=1}^{T-1} n_t\right) =$$

$$= \left(\frac{C_1}{T}\right)^2 \left(\sum_{t=1}^{T-1} Dn_t\right) = \left(\frac{C_1}{T}\right)^2 \left(\sum_{t=1}^{T-1} np_t(1 - p_t)\right) =$$

$$= n\left(\frac{C_1}{T}\right)^2 \left(\sum_{t=1}^{T-1} p_t - \left(\sum_{t=1}^{T-1} {p_t}^2\right)\right),$$

де $C_2 = \text{const}$. Наслідком зазначеного прикладу є $\grave{I}\ (\hat{A}_{\grave{O}}) = \grave{I}\ (\hat{A}(\grave{O}))$, шуканим критерієм $\grave{I}\ (\hat{A}(\grave{O})) + V * D(\hat{A}_m)$. Константу V можна розглядати як рівень «несхильності до ризику», оскільки V визначає «ступінь можливості» дисперсії $D(\hat{A}_m)$ відносно математичного сподівання. Наприклад, підприємець особливо гостро реагує на зміни у витратах, то він може обирати $V >> 1$. Це надає великого значення дисперсії

$$M(\hat{A}(\grave{O})) + V * D(\hat{A}(\grave{O})) = n * \left\{\left(\frac{\tilde{N}_1}{T} + \frac{C_2}{T^2}\right)\sum_{t=1}^{T-1} p_t - \right.$$

$$\left. - \left(\frac{{C_1}^2}{T}\right)\sum_{t=1}^{T-1} {p_t}^2 + \frac{{C_1}^2}{T}\right\}.$$

За даними наведеного прикладу складено табл. 2.

Із наведеного вище розрахунку можна зробити висновок, що інтервал часу $T = 1$ є доцільним для випадкових ризиків.

Критерій граничного рівня

Цей критерій не дає оптимального рішення, оскільки відповідає визначенню прийнятного способу дій. Для прикладу припустимо, що для роботи користувачів на сервері потрібно *xMb* оперативної пам'яті, тоді неперервна функція для величини вільного місця в будь-який час $F(x)$.

Таблиця 2

Інтервал часу *T*=1 є доцільним для ризиків, що мають випадкову природу

T	p_t	p_t^2	$\sum_{t=1}^{T-1} p_t$	$\sum_{t=1}^{T-1} p_t^2$	$\grave{I}\ (\hat{A}(\grave{O}))+V*D(\hat{A}(\grave{O}))$
1	0,05	0,0025	0	0	500,00
2	0,07	0,0049	0,05	0,0025	6312,50
3	0,10	0,0100	0,12	0,0074	6622,22
4	0,13	0,0169	0,22	0,0174	2731,25
5	0,18	0,0324	0,35	0,0343	6764,00
6	0,19	0,0361	0,53	0,2809	6257,50
7	0,21	0,0441	0,72	0,5184	3800,00
8	0,23	0,0529	0,93	0,8649	13093,8

Якщо вільний простір в оперативній пам'яті в початковий момент невеликий, в майбутньому виникне дефіцит пам'яті. В іншому випадку буде неефективний невикористаний простір. В обох випадках можливі втрати та ризики [2].

Оскільки визначити втрати від дефіциту дуже важко, то встановити необхідний рівень вільного простору можна таким чином, щоб величина очікуваного дефіциту не перевищувала A_1 інформаційних одиниць, а величина неефективного невикористаного простору не перевищувала A_2 одиниць. Іншими словами, нехай I — шуканий рівень ефективного вільного простору в ОП, тоді:

– очікуваний рівень дефіциту пам'яті:

$$\int_1^{\infty}(x-I)F(x)dx \le A_1.$$

– очікуваний рівень неефективного простору:

$$\int_0^{1}(I-x)F(x)dx \le A_2.$$

При довільному виборі A_1 і A_2 вказані умови можуть бути суперечливими. В цьому випадку необхідно зменшити кількість обмежень, щоб забезпечити припущення.

Нехай функція, що характеризує величину простору в момент часу, за необхідного простору ОП дорівнює $F\ x\ = \frac{20}{x^2}$, при x = [10, 20], а при інших випадках функція дорівнює 0.

Тоді:

$$\int_I^{20}(x-I)f(x)dx = \int_I^{20}(x-I)\frac{20}{x^2}dx = 20\left(\ln\frac{20}{I}+\frac{I}{20}-1\right);$$

$$\int_{10}^{I}(1-x)f(x)dx = \int_{10}^{I}(x-I)\frac{20}{x^2}dx = 20\left(\ln\frac{10}{I}+\frac{I}{10}-1\right);$$

$$\ln I-\frac{1}{20}\ge \ln 20-\frac{A_1}{20}-1=1,996-\frac{A_1}{20};$$

$$\ln I-\frac{1}{10}\ge \ln 10-\frac{A_1}{20}-1=1,302-\frac{A_1}{20}.$$

Граничні значення A_1 та A_2 мають бути вибрані таким чином, щоб умови задовольняли хоч одне значення I.

Наприклад, якщо $A_1 = 2MB$, а $A_2 = 4MB$, то умови набувають вигляду:

$$\ln I-\frac{1}{20}\ge 1,896,\ \ln I-\frac{1}{10}\ge 1,102.$$

Із табл. 3 видно, що дві умови виконуються при $I \in 13,17$.

Таблиця 3

Значення *I* має знаходитись між 10 та 20, оскільки саме в цих межах змінюється потреба у просторі ОП

I	10	11	12	13	14
$\ln I-\frac{I}{20}$	1,8	1,84	1,88	1,94	1,96
$\ln I-\frac{I}{10}$	1,3	1,29	1,28	1,26	1,24
I	15	16	17	18	
$\ln I-\frac{I}{20}$	1,97	1,98	1,99	1,99	
$\ln I-\frac{I}{10}$	1,17	1,13	1,09	0,99	

Висновок

Отже, в умовах ризику важливим питанням є прийняття коректних та зважених рішень, негативними наслідками яких можуть бути як погіршення ситуації, так і створення нових ризиків. Первинне виявлення загрози та прийняття рішення про її опрацювання є одним із завдань комплексної системи захисту інформації.

У результаті дослідження було здійснено розрахунок ризику поломки серверу та час, за який потрібно здійснювати профілактичний огляд для його уникнення із застосуванням різних критеріїв прийняття рішень.

1. ***ЛІТЕРАТУРА*** *Астрахов А .М.* Искусство управления ин-формационными рисками / А. М. Астрахов. — М. : ДМК Пресс, 2010 — 312 с.

2. *Родионов И. Б.* Системный анализ. Теория систем и системный анализ / И. Б. Родионов. — 122 с.

3. *Макаревич Л. М.* Управление предпринимательскими рисками: монография / Л. М. Макаревич. — М. : Дело и Сервис, 2006. — 443 с.

4. *Луцкий М. Г.* Базовые понятия управления риском в сфере информационной безопасности / М. Г. Луцкий // Защита информации. — 2011. — № 2. — С. 86–94.

5. *Петренко С. А.* Управление информационными рисками. Экономически оправдання безопасность / С. А. Петренко, С. В. Симонов. — М. : Компания АйТи : ДМК Пресс, 2004. — 384 с.

Стаття надійшла до редакції 20.12.12.