Література

1. Стандарт ISO/IEC 17799:2000 (BS 7799). Практичні рекомендації з керування інформаційною безпекою.
2. Галатенко В.А. Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий, 2006. — 264 с.
3. Горелова Г.В., Захарова Е.Н., Радченко С.А. Исследование слабоструктурированных проблем социально-экономических систем. Когнитивный подход. - Ростов на Дону: Изд-во РГУ, 2006. – 332с.
4. Силов В.Б. Принятие стратегических решений в нечеткой обстановке. М.: ИНПРО-РЕС, 1995. 228 с.

Надійшла в редколегію 20.06.2011

***

УДК 621.3.019:62-52(075)

Скопа О.О. [1], Казакова Н.Ф. [1], Мініна Є.О. [2]

[1]*Одеський державний економічний університет, м. Одеса*
[2]*Східноукраїнський національний університет ім. В. Даля, м. Луганськ*

ВСТАНОВЛЕННЯ СТУПЕНЮ РИЗИКУ ПІДПРИЄМСТВА ПРИ СКОРОЧЕННІ ОБСЯГУ ПРОФІЛАКТИЧНИХ ВИМІРЮВАНЬ

Розглядаються та порівнюються деякі стратегії організації процедури вимірювань під час експлуатації об'єктів інформаційних мереж.

Постановка проблеми

Частина коштів, що виділяються на створення та експлуатацію каналів зв'язку в інформаційних мережах, витрачається на автоматизацію їх технічних контрольних та тестових вимірювань. Тому однією з практично важливих задач прикладної математичної статистики є обґрунтування мінімально необхідної кількості вимірювань, а також пошук шляхів можливого скорочення їх обсягів. Розглянемо рішення цієї задачі в рамках допущень, прийнятих на практиці.

При проведенні контрольних вимірювань каналів приймається одне з трьох рішень:

– канал відповідає технічним вимогам і повністю дієздатний;

– технічний стан каналу такий, що його характеристики підлягають корекції з метою подальшого використання;

– канал не відповідає технічним вимогам і має бути замінений на іншій.

Підкреслимо особливу роль останнього з рішень. Воно повинно прийматися за результатами комплексного обстеження, де автоматизоване тестування є тільки однією зі складових частин.

Зв'язок проблеми з важливими науковими та практичними завданнями

Зважаючи на сказане, приходимо до висновку про те, що часто методи математичної статистики дозволяють лише ставити, але не остаточно вирішувати питання про подальше використання того чи іншого каналу зв'язку. Рішення про зняття каналу з експлуатації може бути замінено рішенням, наприклад, про звуження діапазону його використання. Таким чином, проблема скорочення обсягу контрольних і профілактичних вимірювань є актуальною та пов'язана з напрямками сучасних наукових досліджень в області інформаціних мереж та їх експлуатації.

Аналіз останніх досліджень і публікацій, в яких покладено початок вирішення проблеми

Розглянемо вказану проблему стосовно теорії вимірювань узагальнених параметрів засобів та мереж телекомунікацій одноразового і короткочасного використання [1, 2]. Аналогічні проблемні завдання (в теорії функціонування складних систем), висвітлені в багатьох доступних літературних джерелах. Серед вчених проблемами аналізу та розробки методів та методик вимірювань для резервних каналів та об'єктів інформаційного і телекомунікаційного забезпечення займалися як вітчизняні, так і зарубіжні теоретики і практики. Серед них можна назвати Р.В.Судакова, Г.А.Птіцина, Є.Ю.Барзіловіча, В.А.Каштанова, Б.В.Гнеденко, Ю.К.Беляєва, А.Д.Соловьева і ін.

Раніше невирішеною частиною загальної проблеми є адаптація відомих методик до їх простого і логічного практичного використання з врахуванням досить великого обсягу інформації про структурну надмірність використовуваних засобів в інформаційних мережах, спрощення самих методик і їх нове смислове трактування.

Постановкой завдання для послідуючого вирішення є задача встановлення допустимого рівня точності при проведенні контрольних і профілактичних вимірювань.

Перейдемо до викладу **основного матеріалу** з математичним обгрунтуванням отриманих результатів.

Розглянемо задачу скорочення обсягу контрольних та профілактичних вимірювань каналів зв'язку в інформаційних мережах за рахунок структурної надмірності системи [3]. Припустимо, що задача може бути вирішена при використанні одного каналу, але для «страховки» передбачається ще $\nu - 1$ додаткових каналів, причому у випадку виходу з ладу головного каналу, миттєво включається в роботу любий з $\nu - 1$ (рис.1), повністю готовий до роботи. У загальному випадку розглядається ситуація, коли для рішення задачі досить, щоб хоча б один з ν каналів системи гарантовано виконав свої функції. Зазначені $\nu - 1$ каналів у даній системі характеризують її структурну надмірність. Виникає питання: чи можливе скорочення числа n'_i вимірювань кожного i -го каналу системи, приведеної на мал. 1, при його автономних вимірюваннях, за рахунок інформації про те, що при реальному функціонуванні системи є ще $\nu - 1$ каналів, тобто за рахунок структурної надмірності? Інтуїтивно зрозуміло, що відповідь повинна бути позитивною, а форма її представлення повинна залежати від того, чи однакові всі канали в системі [4].

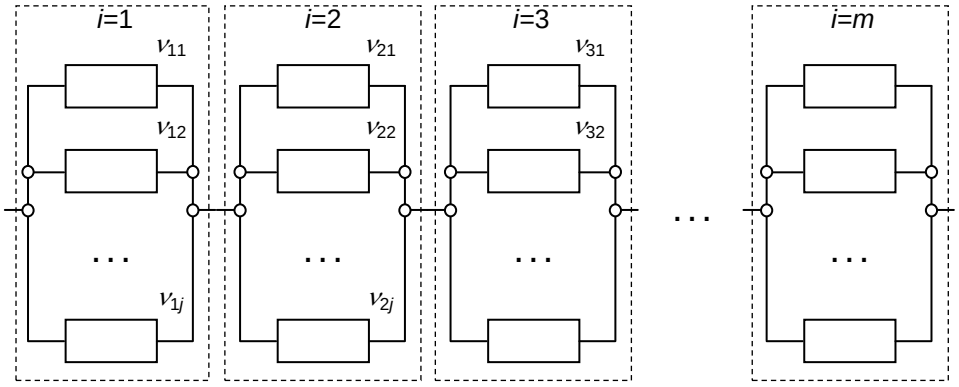

Рис. 1.

Визначення. *Нехай* P_L *– ймовірність безпомилкової роботи каналу зв'язку, а* P_{L_H} –

необхідне значення P_L. *Процедура, в якій рівень* P_L *вважається достатнім, якщо* $\underline{\gamma}$ *-нижня границя* $P_{\underline{L}}$ [5] *для* P_L *задовольняє умові* $P_{\underline{L}} \geq P_{L_H}$, *а рішення про вилучення каналу зв'язку з експлуатації на основі статистичних даних не приймається, назвемо* C_0 *-процедурою.*

Нехай в силу умов організації системи зв'язку канали в ній різні і незалежні, а вимірювання для кожного з ν каналів проводяться за біноміальним планом з зупинкою. Тоді, використовуючи C_0 -процедуру і [5, (10)] для γ -нижньої границі $P_{\underline{L}}$ ймовірності P_L безпомилкової роботи $P_{\underline{L}} = 1 - \left(1 - (1-\gamma)^{\frac{1}{n'\nu}}\right)^{\nu}$, де n' – менша з величин n'_i, $i = \overline{1,\nu}$, а також ґрунтуючись на раніше розглянутих положеннях [6], знаходимо умову, якій повинна задовольняти величина n', у вигляді:

$$n' = \min_{1 \leq i \leq \nu} n'_i \geq \left(n_{0\nu} = \frac{\ln \beta_q}{\nu \ln P_{L_H \nu}} \right),\ P_{L_H \nu} = 1 - \left(1 - P_{L_H}\right)^{\frac{1}{\nu}},$$

де β_q – допустимий рівень ризику підприємства, що експлуатує канал, а $\gamma = 1 - \beta_q$.

Слід врахувати, що ризик підприємства β визначається як ймовірність P прийняття позитивного рішення в той час, як вимоги не виконуються, тобто $\beta = P\left(P_{\underline{L}} \geq P_{L_H} \middle| P_L < P_{L_H}\right)$. Так як $n' \geq n_{0\nu} \Leftrightarrow \bigwedge_{i=1}^{\nu} \left(n'_i \geq n_{0\nu}\right)$, то звідси одержуємо вимогу до обсягу n'_i вимірювань (безпомилкових чи до першої помилки) для i -го каналу:

$$n'_i \geq n_{0\nu} = \frac{\ln \beta_q}{\nu \ln\left(1 - \left(1 - P_{L_H}\right)^{\frac{1}{\nu}}\right)},\ i = \overline{1,\nu}\ . \qquad (1)$$

Приклад. Знайдемо мінімально необхідний обсяг $n_{0\nu} = n_0(\nu)$ для числа n'_i вимірювань (безпомикових чи до першої помилки) кожного з каналів системи зв'язку (мал.1), якщо канали незалежні і різні, причому задано, що $P_{L_H} = 0{,}999$ і $\beta_q = 0{,}1$.

Рішення. З (1) для зазначених умов за допомогою ЕОМ знайдемо необхідні значення і приведемо їх у вигляді графіка (рис.2).

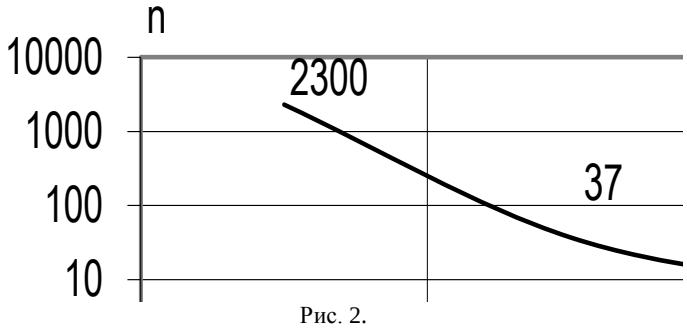

Рис. 2.

Висновки

Таким чином, скорочення вимірювань систем телекомунікацій на надійність за рахунок їх структурної надмірності та по властивості γ-нижньої границі з врахуванням нерівності $P\left(P_{\underline{L}} \geq P_{L_H} \middle| P_L > P_{L_H}\right) \leq P\left(P_{\underline{L}} \geq P_L\right)$ дозволяє встановити, що $\beta \leq P\left(P_{\underline{L}} > P_L\right) \leq 1-\gamma$ [7]. Враховуючи це, можемо зробити висновки:

1. Якщо задані необхідне значення P_{L_H} таке, при якому, у випадку $P_L \geq P_{L_H}$, канал вважається достатньо надійним та для якого встановлений припустимий ризик β_q, то, визначаючи за результатами вимірювань γ-нижню границю $P_{\underline{L}}$ для невідомої ймовірності P_L безпомилкової роботи каналу при $\gamma = 1-\beta_q$ і приймаючи у випадку виконання умови $P_{\underline{L}} = P_{\underline{L}_{1-\beta_q}} \geq P_{L_H}$ позитивне рішення, а при $P_{\underline{L}} < P_{L_H}$ вважаючи, що канал вимагає корегування, можемо обумовити значення ризику на прийнятному рівні $\beta \leq \beta_q$.

2. При виконанні ν умов (1) вимоги по надійності до системи зв'язку, що складається з ν каналів (мал.2), вважаються виконаними. У противному випадку система зв'язку піддається новому укомплектуванню чи ж для каналів проводиться повторне настроювання.

3. З (1) випливає, що з ростом структурної надмірності системи зв'язку мінімально необхідний обсяг $n_{0\nu} = n_{0\nu}(\nu)$ вимірювань (безпомилкових чи до першої помилки) різко зменшується. В такий спосіб шлях скорочення обсягу вимірювань за рахунок структурної надмірності інформаційної мережі існує і є ефективним, однак, при цьому, збільшується вартість системи. В цьому відношенні перспективною для подальшого дослідження варто вважати задачу оптимального резервування [8], сформульовану на ймовірністній основі.

Список літератури

1. Казакова Н.Ф. Методи оцінки надійності систем телекомунікацій з резервом // Праці УНДІРТ. – Одеса, 2003. – №2(34). – С.109-112.

2. Казакова Н.Ф. Порівняння методів управління вибором резервного радіоканалу // Праці УНДІРТ. – Одеса: УНДІРТ, 2002. – №1(29). – С.49-51.

3. Скопа О.О., Казакова Н.Ф., Мурін О.С. Вплив функціональної надмірності резервованих систем телекомунікацій на скорочення обсягів їх випробувань на надійність // Наук. праці ДонНТУ. Серія: Обчислювальна техніка та автоматизація. Випуск 58. – Донецьк: РВА ДонНТУ, 2003. – С.115-121.

4. Мухін О.М., Казакова Н.Ф., Скопа О.О. Планування обсягу випробувань в мережах телекомунікацій // Вісник УБЕНТЗ. – К.: УБЕНТЗ, 2002. – №2. – С. 104-109.

5. Скопа О.О. Інтервальне оцінювання надійності Т-систем з паралельним з'єднанням елементів за результатами їх біноміальних іспитів // Наукові праці Одеської націон. академії зв'язку: Період. наук. збірник з радіотехніки і зв'язку, електроніки та економіки в галузі зв'язку. – Одеса, 2002. – №1. – С.65-70.

6. Казакова Н.Ф. Оптимізація стратегії обслуговування резервних систем зв'язку // Вісник УБЕНТЗ. – К.: УБЕНТЗ, 2002. – №2. – С.79-80.

7. Казакова Н.Ф. Надійність функціонування морських супутникових систем телекомунікацій // Зб. науков. праць Укр. держ. морськ. техн. ун-ту. – Миколаїв: УДМТУ, 2002. – №7(385). – С.109-115.

8. Казакова Н.Ф. Аналітичне розв'язання одновимірної задачі Клопера-Пірсона // Радиотехника: Всеукр. межведомств. научн.-техн. сб. – Харьков: ХНУРЭ. – 2002. – Вып. 128. – С.97-98.

Надійшла в редколегію 22.06.2011

***

УДК. 004.056

Лахно В.А., Петров О.С.

Східноукраїнський національний університет імені В. Даля, м. Луганськ

ЗМІНИ ПРОДУКТИВНОСТІ ОБЧИСЛЮВАЛЬНИХ КОМПЛЕКСІВ ІНФОРМАЦІЙНИХ СИСТЕМ ПІДПРИЄМСТВ В УМОВАХ РЕАЛІЗАЦІЇ КОМП'ЮТЕРНИХ АТАК

У статті викладені результати досліджень, що дозволяють підвищити рівень захисту корпоративних інформаційних систем суб'єктів господарської діяльності. Приведені математичні моделі, описані за допомогою ланцюгів Маркова, а також, результати моделювання інформаційних систем, що мають підключення до Інтернету через різні канали зв'язку.

Ключові слова: ланцюг Маркова, граф станів, автоматизовані інформаційні системи, інформаційна безпека, DoS атака.

Постановка проблеми

На проблему зниження продуктивності корпоративних інформаційних систем (КІС) в результаті навмисного втручання в їх роботу з боку зловмисників, наприклад, при комп'ютерних атаках, стали звертати увагу з 80-х років минулого століття.

Щорічно фіксується тисячі зломів сайтів, серверів, додатків, баз даних і ін. Практично щодня в засобах масової інформації з'являються повідомлення про незаконне проникнення в корпоративні мережі крупних компаній, в мережі Internet викладаються конфіденційні бази даних міністерств, банків та підприємств і т.д. Все це наочно підтверджує необхідність побудови надійної системи інформаційної безпеки (ІБ). Особливо актуальна проблема у випадках, коли зовнішні, загальнодоступні, інформаційні ресурси компанії, взаємодіють напряму з її внутрішніми корпоративними ресурсами.

Ця задача актуальна і при побудові моделей різних класів атак, включаючи аналіз ризиків для комп'ютерних систем, і розробку алгоритмів управління ризиками із захисту інформаційних ресурсів суб'єктів господарської діяльності і фізичних осіб. Як правило, під атаками «відмова в обслуговуванні» (Denial Service attack - DoS-attack) розуміють мережні атаки, що призводять до неможливості для легітимного користувача мережі здобути доступ до ресурсів серверу.Найбільш відомі наступні різновиди DoS-атак [1,3]: TCP SYNflood, TCP FIN Flood; Ping of Death; Tribe Flood Network (TFN) та Tribe Flood Network 2000 (TFN2K); Stacheldracht та ін.

Аналіз попередніх досліджень

Наявні роботи в області моделювання систем масового обслуговування, у тому числі корпоративних інформаційних систем, носять узагальнений характер і не враховують специфіки появи нових класів загроз інформаційної безпеки. Аналіз публікацій у відкритому друці [1- 3, 5, 6] показав, що більшість систем виявлення атак (СВА) на