

УДК 621.391.3

В.Я. Воропаєва (канд. техн. наук, доц.), І.Л. Щербов (ст. викл.)
Донецький національний технічний університет, м. Донецьк
кафедра автоматики і телекомунікацій, кафедра військової підготовки
E-mail: voropayeva@donntu.edu.ua, schil@rtf.donntu.edu.ua

АДАПТУВАННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ДО ЗОВНІШНІХ ВПЛИВІВ

*Проведено аналіз порядку прийняття рішення щодо адаптування інформаційно-телекомунікаційних систем (ІТС) до зовнішніх впливів. Класифіковані типові загрози зовнішнього впливу на ІТС. Запропоновано математичний апарат для вирішення задачі оптимізації процесу прийняття рішення щодо адаптування ІТС до зовнішніх впливів. **Ключові слова:** інформаційно-телекомунікаційна система, зовнішній вплив, адаптування, прийняття рішення, багатокритеріальна оптимізація.*

Загальна постановка проблеми

Сучасний стан розвитку інформаційно-телекомунікаційних технологій сприяє кожній людині мати вільний доступ до інформаційних ресурсів світового суспільства, можливість отримання освітніх послуг, реалізувати інші потреби.

Тому розвиток інформаційного суспільства в Україні та впровадження новітніх інформаційних комп'ютерних технологій в усі сфери суспільного життя і в діяльність органів державної влади та органів місцевого самоврядування визначається одним з пріоритетних напрямів державної політики [1].

Реалізація даного напрямку державної політики безпосередньо залежить від розвитку інформаційно-телекомунікаційних систем (ІТС) та їх властивості зберігати повністю або частково свої функції за умови впливу дестабілізуючих чинників. Для того щоб надати можливість кожній людині повною мірою реалізувати свої потреби в інформаційному просторі, для ІТС мають бути виконані вимоги щодо здатності забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації [2].

Реалізація даних вимог значною мірою залежить від спроможності системи адаптуватися до зовнішніх впливів, що виникають при її функціонуванні.

Постановка завдань дослідження

Особливе місце серед актуальних питань оптимізації структури і параметрів телекомунікаційних мереж та систем є задачі, пов'язані із забезпеченням живучості інформаційно-телекомунікаційних систем. При цьому під живучістю ІТС розуміють властивість, що характеризує, зокрема, і здатність системи ефективно функціонувати за наявності ушкоджень (руйнацій складових) або відновлювати цю здатність за визначений проміжок часу [3].

Одним із факторів, що впливає на живучість ІТС, є загрози зовнішнього впливу. Під загрозливим впливом на ІТС слід розуміти внутрішні та зовнішні фактори, які можуть вивести з ладу або значно погіршити показники якості функціонування програмного та апаратного забезпечення ІТС, зокрема комутаційного обладнання та каналів зв'язку [4]. Особливістю функціонування інформаційно-телекомунікаційних систем з точки зору адаптації до зовнішніх впливів є їхня нестаціонарність, нестабільність, складність у прогнозуванні та висока динаміка зміни зовнішнього середовища. Це призводить до

необхідності прийняття рішень в умовах невизначеності інформації. Зокрема, ці рішення стосуються адаптації засобів забезпечення інформаційної безпеки в мережах загального користування [5].

Таким чином, для забезпечення живучості ІТС важливим є створення системи підтримки рішень як на етапі її створення, так і в процесі функціонування. При цьому важливо врахувати такі задачі як:

1. Визначення послуг, які передбачені ІТС та властивостей інформації, що циркулює.
2. Необхідність задовольняти сукупності технічних вимог для забезпечення сумісної роботи продуктів різноманітних виробників.
3. Пошук ефективних способів сумісного використання каналів зв'язку та забезпечення електромагнітної сумісності.
4. Можливі загрози.
5. Можливість модернізації.
6. Собівартість.

Вирішення завдань і результати дослідження

Аналізуючи визначені задачі, можна зробити висновок, що прийняття рішення щодо адаптування інформаційно-телекомунікаційних систем до зовнішніх впливів зводиться до вибору варіанту забезпечення живучості інформаційно-телекомунікаційних систем в умовах невизначеності. Це обумовлено неповнотою історичних даних щодо функціонування ІТС в різноманітних умовах, а також надійності апаратних і програмних засобів; впливу на ІТС реалізованих можливих загроз та інш.

Тому можна вважати, що рішення поставленої задачі зводиться до рішення задачі багатокритеріальної оптимізації в умовах невизначеності [6] структури і вектору параметрів $\bar{X} = |x_1, \dots, x_i, \dots, x_n|$ деякої ІТС S . Певна j -а властивість системи S характеризується величиною показника $q_j(\bar{X})$; $j = \overline{1, m}$. Тоді система в цілому буде характеризуватися вектором показників $\bar{Q} = |q_1, \dots, q_j, \dots, q_m|$.

При цьому вказана невизначеність може мати різний характер:

- структурна невизначеність, коли невідомий точний перелік складових системи або зовнішніх факторів, які впливають на її функціонування;
- параметрична невизначеність, коли значення кількісних показників властивостей системи $q_j(\bar{X})$; $j = \overline{1, m}$ задані у вигляді імовірнісних характеристик, нечіткої логіки (функцій приналежності) або інтервальних значень.

Найчастіше для виключення або мінімізації впливу невизначеності на результати рішення задачі багатокритеріальної оптимізації перш за все намагаються визначитися зі структурою ІТС та переліком можливих загроз, які можуть розглядатися як обмеження на роботу системи. Після цього визначаються зі шляхами подолання параметричної невизначеності, використовуючи розподіл ймовірностей чи можливостей для кількісних показників властивостей системи або задаючи нечіткі інтервали їх границь.

Цей підхід вимагає певного узагальнення та формалізації суб'єктивних процедур оцінювання зазначених показників, на відміну від евристичного підходу, коли особа, що приймає рішення, оцінює ситуацію, спираючись на досвід та інтуїцію [7]. Після формулювання та формалізації критерію оптимізації, тобто визначення «найкращого в певному сенсі вектора \bar{Q} », слід визначитися з множиною (областю) допустимих рішень (ОДР) задачі. До ОДР можуть входити як уся множина M_s варіантів системи S , так і деяка підмножина. При цьому звуження ОДР, що може виконуватися із застосуванням обох підходів (евристичного та формалізованого), очевидно призводить до прискорення рішення задачі багатокритеріальної оптимізації.

Аналогічним чином зменшує кількість обчислювальних операцій і, відповідно, прискорює процес знаходження рішення зменшення розмірності вектору параметрів \bar{Q} за рахунок виділення найважливіших в певній ситуації показників (властивостей) системи S . Для визначення, які ж саме параметри необхідно оптимізувати при прийнятті рішення, приведемо на рис. 1 алгоритм прийняття рішення щодо адаптування ІТС до зовнішніх впливів.

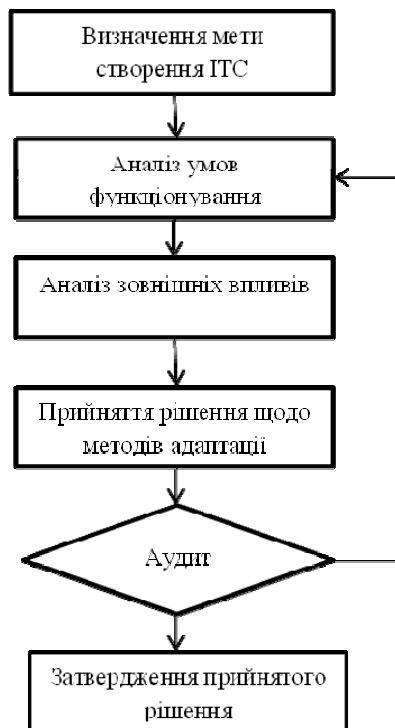


Рисунок 1 — Алгоритм адаптації ІТС до зовнішніх впливів

На першому етапі визначається мета створення ІТС і як наслідок — визначаються основні властивості інформації, що буде оброблятися в системі, та на адаптування яких слід в першу чергу звернути увагу при реалізації зовнішніх впливів. Наприклад для ІТС, що призначена для задоволення потреб суспільства на отримання інформації в довідково-пошукових системах, необхідно забезпечити адаптування до зовнішніх впливів таких властивостей інформації як доступність та цілісність. В ІТС банківської сфери виникає необхідність додатково до вже зазначених властивостей інформації звернути увагу й на конфіденційність, що в свою чергу підвищує множину загроз для інформації від зовнішніх впливів.

При аналізі умов функціонування необхідно деталізувати:

- програмне та апаратне забезпечення ІТС,
- інформаційні потоки та канали зв'язку по яким буде передаватися інформація;
- фізичне середовище, в якому буде функціонувати ІТС;
- персонал, який буде залучено до робіт зі створення та експлуатації ІТС.

При аналізі зовнішніх впливів необхідно враховувати всю множину загроз, що здійснюють або потенційно можуть здійснювати вплив на систему, як зовнішніх так і внутрішніх та виділити з них найбільш актуальні.

Для оптимізації прийняття рішення пропонується починати класифікувати загрози для інформації, що циркулює в ІТС, виходячи із властивостей інформації, а саме цілісності, доступності, конфіденційності.

Види загроз для інформації в ІТС умовно поділені на групи і представлено на рис. 2.

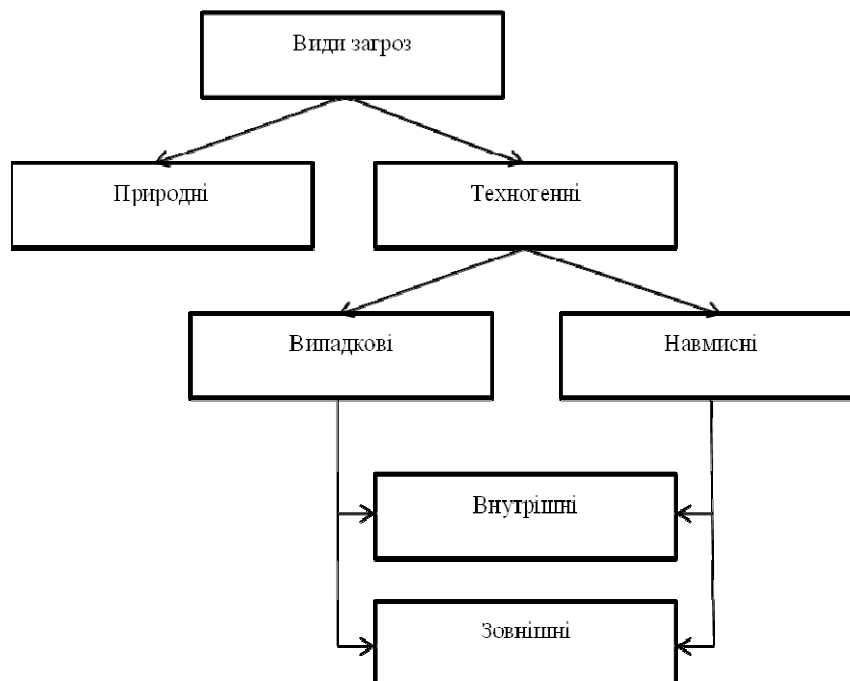


Рисунок 2 — Загальна класифікація загроз для інформації в ІТС

Загрози зовнішнього впливу на ІТС поділяються на природні та техногенні. Природні спричиняються стихійними природними явищами. Техногенні загрози є наслідком діяльності людини, технічних засобів і систем.

В свою чергу техногенні загрози поділяються на випадкові та навмисні.

Випадкові загрози можуть виникнути в наслідок силових деструктивних впливів (електромагнітний вплив, механічне пошкодження), помилок при проектуванні ІТС, або спричинятися помилками у програмному забезпеченні, збоями та відмовами апаратури та систем забезпечення, помилками персоналу тощо.

Навмисні загрози обумовлені цілеспрямованими діями людей із застосуванням технічних або програмних засобів, спрямованих на виведення системи з ладу.

За місцем розміщення джерела загроз відносно ІТС випадкові і навмисні загрози поділяються на внутрішні та зовнішні.

Виходячи з того, що прийняття рішення щодо адаптування ІТС до зовнішніх впливів здійснюється для визначеної ІТС у визначений час, можна сформулювати основні вимоги при прийнятті рішення.

Рішення повинно об'єктивно враховувати усі складові ІТС та загрози до інформації від зовнішніх впливів.

Рішення повинно ґрунтуватися на накопиченому досвіді в прийнятті рішень щодо адаптування ІТС до зовнішніх впливів. Цей досвід, як вже зазначалося вище, може формалізуватися у вигляді масивів експертних оцінок, на базі яких будуються розподіли ймовірностей або набір правил нечіткої логіки для класифікації зовнішніх впливів згідно рис.2.

Рішення має бути ефективним, тобто давати оптимальне в заданих умовах значення критерію \bar{Q} . Найчастіше задачу багатокритеріальної оптимізації намагаються

трансформувати в однокритеріальну [6] шляхом введення узагальненої оцінки якості або функції корисності $F(\bar{X})$ альтернативних рішень $\bar{X} = |x_1, \dots, x_i, \dots, x_n|$.

При цьому абсолютні показники $q_i(\bar{X}); j = \overline{1, m}$ замінюють нормованими показниками $q_j^*(\bar{X}); j = \overline{1, m}$, на базі експертної оцінки присвоюють вагові коефіцієнти важливості цих показників $k_j(\bar{X}); j = \overline{1, m}$, так що $0 \leq k_j \leq 1, \sum_{j=1}^m k_j = 1$. Сама функція корисності може бути представлена у вигляді адитивної функції виду $F(x) = \sum k_j q_j^*(x)$. Це суттєво спрощує задачу і дозволяє використовувати для її рішення відомі методи дослідження операцій, зокрема лінійного програмування, теорії масового обслуговування, стохастичних мереж Петрі, теорії графів.

На решті, рішення повинно бути стійким, забезпечуючи адаптацію ІТС до зовнішніх впливів та прийнятне функціонування ІТС протягом певного відрізка часу, тобто гарантуючи живучість системи.

Вимоги стійкості та адаптивності є дуже важливими, бо дозволяють при обмежених витратах на проектування або функціонування ІТС підтримувати знайдений оптимум критерію за рахунок реакції на зміну зовнішніх впливів. Динамічний характер поведінки останніх висуває зазначені вимоги на перше місце серед властивостей, необхідних ІТС.

Етап аудиту має за мету з'ясувати наскільки прийняте рішення щодо адаптування ІТС до зовнішніх впливів відповідає вимогам, що визначаються в технічному завданні на створення ІТС. Якщо прийняте рішення відповідає заданим вимогам, то воно затверджується, якщо ні — процес відпрацювання рішення повертається на попередній етап.

На етапі аудиту важливим є експертний висновок, що базується як правило на накопиченому досвіді. Однак враховуючи сучасні темпи розвитку інформаційно-телекомунікаційних технологій, можна констатувати той факт, що у випадку неповноти історичних даних про результати деструктивних впливів на живучість ІТС (як в цілому на ІТС так і на окремі її складові), існує можливість помилки в експертній оцінці прийнятого рішення щодо адаптування ІТС до зовнішніх впливів [8].

Висновки

Виходячи із аналізу процесу прийняття рішення щодо адаптування ІТС до зовнішніх впливів, можна зробити наступні висновки.

1. Запропоновано алгоритм адаптації ІТС до зовнішніх впливів, що має включати етапи визначення мети створення ІТС, аналізу умов функціонування системи, класифікацію зовнішніх впливів, вибір оптимального варіанту адаптації системи, аудит та затвердження обраного рішення.

2. Для оптимізації прийняття рішення слід класифікувати загрози ІТС, виходячи із властивостей інформації, що циркулює, а саме цілісності, доступності, конфіденційності.

3. Задачу багатокритеріальної оптимізації слід трансформувати в однокритеріальну шляхом введення скалярної функції корисності, нормованих показників якості та призначення вагових коефіцієнтів їх важливості.

4. При прийнятті рішення необхідно використовувати сучасні системи автоматизованого проектування та експертні системи підтримки прийняття рішень.

Список використаної літератури

1. Україна. Закони. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки [Текст]: Закон України: [прийнято Верховною Радою України

- 09.01.2007 р]. — К.: Відомості Верховної Ради України офіційне видання від 23.03.2007 р., № 12, стаття 102. — С. 511.
2. Україна. Закони. Про телекомунікації [Текст]: Закон України: [прийнято Верховною Радою України 18.11.2003 р]. — К.: Відомості Верховної Ради України від 19.03.2004 р., № 12, стаття 155.
 3. Додонов А.Г. Живучесть информационных систем / А.Г. Додонов, Д.В. Ландэ. — К.: Наук. думка, 2011. — 256 с.
 4. ITU_T E.408 Recommendation. Telecommunication networks security requirements <http://www.itu.int/rec/T-REC-E.408-200405-I/en>.
 5. Воропаева В.Я. Вопросы обеспечения информационной безопасности в сетях общего пользования / В.Я. Воропаева, В.А. Попов, И.В. Стародубов // Наукові праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація. — 2000. — Вип. 20. — С. 159–165.
 6. Безрук В.М. Многокритериальная оптимизация в планировании телекоммуникационных сетей / В.М. Безрук, Д.В. Рыбалко // 17-я Международная крымская конференция “СВЧ-техника и телекоммуникационные технологии” (КрыМиКо’2007): материалы конференции. — Севастополь: Вебер, 2007. — С.338–340.
 7. Герасимов Б.М. Системы поддержки принятия решений: проектирование, применение, оценка эффективности / Б.М. Герасимов, М.М. Дивизинюк, И.Ю. Субач. — Севастополь: Издательский центр СНИЯЭиП, 2004. — 320 с.
 8. Тюрин М.В. Методы и средства повышения достоверности экспертной оценки живучести телекоммуникационных систем и компьютерных сетей: автореферат диссертации на соискание ученой степени кандидата технических наук / М.В. Тюрин. — М., 2008. — 23с.

Надійшла до редакції:
20.02.2012 р.

Рецензент:
д-р п.наук, проф. Стефаненко П.В.

V.J. Voropaeva, I.L. Shcherbov. Aadaptation of Information-Telecommunication Systems to External Influences. The analysis of an order of decision-making on adaptation ITS to external influences is carried out. Typical threats of external influence on ITS are classified. The mathematical apparatus for solving the problems of optimization of process of decision-making for the purpose of adaptation ITS to external influences is offered.

Keywords: *information-telecommunication system, external influence, decision-making, multicriteria optimization.*

В.Я. Воропаева, И.Л. Щербов. Адаптирование информационно-телекоммуникационных систем к внешним воздействиям. Проведен анализ порядка принятия решения по адаптации ИТС к внешним воздействиям. Классифицированы типовые угрозы внешнего воздействия на ИТС. Предложен математический аппарат для решения задач оптимизации процесса принятия решения с целью адаптации ИТС к внешним воздействиям.

Ключевые слова: *информационно-телекоммуникационная система, внешнее воздействие, принятие решения, многокритериальная оптимизация.*

© Воропаева В.Я., Щербов И.Л., 2012