Висновки. У роботі розглянуто вплив параметрів генетичного алгоритму на його ефективність для задачі відновлення характеристик антенної гратки при відмовах її модулів. Показано, що такі параметри, як величина популяції та еліти, вірогідність кросоверу, щільність мутації, тип мутації, кросоверу та селекції значно впливають на работу генетичного алгоритму. Кращі результати надають генетичні алгоритми з великою елітою та малою популяцією, рівномірною мутацією та турнамент селекцією.

1. Peters T.J. A conjugate gradient-based algorithm to minimize the sidelobe level of planar antenna arrays with elements failures // IEEE Trans. On Antennas and Propagation. – 1991. – Vol. 39, No. 10. – P. 1497–1504. 2. Levitas M., Horton D.A., Cheston T.C. Practical Failure Compensation in Active Phased Array // IEEE Trans. On Antennas and Propagation. – 1999. – Vol. 47, No 3. – P. 524–535. 3. Yeo B., Lu Y. Array Failure Correction with Genetic Algorithm // IEEE Trans. on Antennas and Propagation. – 1999. – Vol. 47, No. 5. – P. 823–828. 4. Krischuk V., Shilo G., Artyushenko B. Tolerable Linear Antenna Array Design with Genetic Algorithm // Proceedings of the IXth International Conference CADSM'07. – Lviv-Polyana, 2007. – P. 167–169. 5. Гостюхин А.В. Восстановление характеристик направленности активных фазированных антенных решеток при отказах активных модулей: Дис. .. канд. техн. наук. – М., 2005 – С. 108. 6. Lee Y.H., Marvin A.C., Porter S.J. Genetic Algorithm using Real Parameters for Array Antenna Design Optimization // Proceedings of Heigh Frequiency Postgraduate Student Colloquim. – Leeds (GB), 1999. P. 8–13. 7. Олейник М.П. Разработка генетических алгоритмов проектирования элементов телекоммуникационных систем: Дис. ...канд. техн. наук. – М., 2003. – С. 128.

УДК 004.413.4, 004.942, 007.5, 65.011.3, 681.518

А.Ю. Берко, В.А. Висоцька, І.В. Рішняк
Національний університет "Львівська політехніка",
кафедра інформаційних систем та мереж

МЕТОДИ ТА ЗАСОБИ ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Проаналізовано засоби захисту інформації в системах електронної комерції та запропоновано моделі цих систем на основі аналізу та оцінювання інформаційних ризиків.

Analysis of the of proofing tools for electronic commerce systems is considered and the models of these systems on the basis of analysis and evaluation of information risks are offered in the article.

Вступ. Останнім часом повідомлення про атаки "хакерів" все частіше з'являються у засобах масової інформації. Що ж таке "атака на інформацію"? Дати визначення цій дії насправді дуже складно, оскільки інформація, особливо електронна, може мати багато різновидів. Інформацією можна вважати й окремий файл, і базу даних, і один запис у ній, і цілий програмний комплекс. І всі ці об'єкти можуть бути "атаковані" певними особами чи групами осіб. Під час збереження, підтримки і надання доступу до будь-якого інформаційного об'єкта його власник чи уповноважена ним особа накладає певні вимоги чи правила роботи з нею. Навмисне порушення цих правил розцінюється як атака на інформацію [4].

Під інформаційною безпекою системи електронної контент-комерції (СЕКК) розуміють захищеність інформації і підтримувальної інфраструктури від випадкових або навмисних впливів природного чи штучного характеру, викликати нанести збитки власникам або користувачам інформації і підтримувальної інфраструктури. Будь-яке порушення безпеки інформацій в

електронній комерції можна класифікувати як загрозу, уразливість або атаку. Загрозою СЕКК вважається будь-який можливий випадок (навмисний чи ні), який може небажано впливати на активи та ресурси системи. Уразливість СЕКК – це деяка невдала характеристика, яка робить можливим наявність потенційної загрози. Атака на СЕКК є дією зловмисника, яка полягає у використанні деяких уразливих місць щоб спровокувати реалізацію існуючої загрози. З положення про безпеку інформації в електронній комерції можна зробити два важливі висновки [4]:

- Трактування проблем, пов'язаних з інформаційною безпекою, для різних категорій суб'єктів може істотно відрізнятися, наприклад, безпека для режимних державних організацій та комерційних структур;
- Інформаційна безпека не зводиться виключно до захисту інформації. Це принципово ширше поняття. Суб'єкт інформаційних відносин може постраждати (понести матеріальні і/або моральні збитки) не тільки від несанкціонованого доступу до інформації, але і від пошкодження системи, що викликає перерву в роботі. Більше того, для багатьох відкритих організацій (наприклад, навчальних) власне захист інформації за важливістю аж ніяк не займає перше місце.

Проблеми безпеки інформації. У теорії інформаційної безпеки існує основна теорема безпеки системи, доведена для багатьох типів математичних моделей захищених систем та сформульована так: "***Якщо початковий стан системи безпечний і всі переходи системи із стану в стан безпечні, то система безпечна***". Абсолютно очевидно, що для безпечно захищеної СЕК умови даної теореми повинні підтримуватися на всіх стадіях життєвого циклу системи. При цьому основна теорема безпеки системи має перетворитися на основну теорему безпеки для програмного забезпечення системи: "***Якщо програмне забезпечення системи починає свої операції в безпечному стані і всі переходи системи із стану в стан безпечні, то всі стани системи безпечні***" [1–4].

Проблема безпеки інформації та електронна комерція. З масовим впровадженням комп'ютерів в усі сфери діяльності людини обсяг інформації, збереженої в електронному вигляді, зріс у тисячі разів. Зараз скопіювати дискету з файлом, що містить план випуску продукції, набагато простіше, ніж переписувати сотні паперів. А з появою комп'ютерних мереж навіть відсутність фізичного доступу до комп'ютера перестала бути гарантією цілісності інформації.

Які можливі наслідки атак на інформацію? Насамперед, звичайно, нас будуть цікавити економічні втрати [3, 4]:

1. Розкриття комерційної інформації може призвести до серйозних прямих збитків на ринку.
2. Звістка про крадіжку великого обсягу інформації серйозно впливає на репутацію фірми, приводячи до втрат в обсягах торгових операцій.
3. Фірми-конкуренти можуть скористатися вкраденою інформацією, якщо факт крадіжки залишився непоміченим, для того, щоб довести фірму до банкрутства, нав'язуючи їй фіктивні або свідомо збиткові угоди.
4. Підміна інформації як на етапі передачі, так і на етапі збереження у фірмі може привести до величезних збитків.
5. Багаторазові успішні атаки на фірму, що надає будь-який вид інформаційних послуг, зменшують довіру до фірми в клієнтів, що позначиться на обсязі прибутків.

Природно, комп'ютерні атаки можуть спричинити і величезний моральний збиток. Поняття конфіденційності спілкування набуває все більшої важливості. Зрозуміло, що користувачу комп'ютерної мережі не хочеться, щоб його листи, крім адресата, одержували ще 5–10 осіб або, наприклад, весь текст, що набирається на клавіатурі ПК, копіювався в буфер, а потім, при під'єднанні до Інтернету, відправлявся на визначений сервер. А саме так і відбувається в тисячах і десятках тисяч випадків.

Аналіз сучасних досліджень і публікацій. Захист інформації важливий для фінансових систем незалежно від того, на фізичних чи на електронних трансакціях вони засновані. При цьому під інформаційною безпекою електронної комерції розуміють захищеність інформації та під-

тримувальної інфраструктури від випадкових або навмисних впливів природного чи штучного характеру, здатних нанести збитки власникам або користувачам інформації та підтримувальної інфраструктури. Інформація з погляду інформаційної безпеки має такі категорії [3]:

1. **Конфіденційність** – гарантія того, що конкретна інформація доступна тільки тому колу осіб, для кого вона призначена; порушення цієї категорії називають розкраданням або розкриттям інформації.

2. **Цілісність** – гарантія того, що інформація зараз існує в її вихідному вигляді, тобто під час її збереження або передавання не було здійснено несанкціонованих змін; порушення цієї категорії називається фальсифікацією повідомлення.

3. **Автентичність** – гарантія того, що джерелом інформації є саме та особа, що заявлена як її автор; порушення цієї категорії також називається фальсифікацією, але вже автора повідомлення.

4. **Апельованість** – досить складна категорія, але часто застосовувана в електронній комерції – гарантія того, що за необхідності можна буде довести, що автором повідомлення є саме заявлена людина і ніхто інший; відмінність цієї категорії від попередньої в тому, що при підміні автора хтось інший намагається заявити, що він автор повідомлення, а при порушенні апельованості – сам автор намагається "відхреститися" від слів, які він підписав.

Відносно до інформаційних систем застосовуються інші категорії [4]: надійність – гарантія того, що система поводиться в нормальному і позаштатному режимах так, як заплановано; точність – гарантія точного і повного виконання всіх команд; контроль доступу – гарантія того, що різні групи осіб мають різний доступ до інформаційних об'єктів, і ці обмеження доступу постійно виконуються; контрольованість – гарантія того, що в будь-який момент можна здійснити повноцінну перевірку будь-якого компонента програмного комплексу; контроль ідентифікації – гарантія того, що клієнт, під'єднаний у цей момент до системи, є саме тим, за кого себе видає; стійкість до спеціальних збоїв – гарантія того, що під час спеціального внесення помилок у межах заздалегідь обговорених норм система поводитиметься так, як обумовлено заздалегідь [3,4].

Обґрунтуванню критеріїв і створенню методології оцінки інформаційної безпеки (ІБ) приділено значну увагу. Сьогодні можна виділити такі документи, якими зроблено серйозний теоретичний і практичний внесок у розв'язання задач інформаційної безпеки:

1. Критерії оцінки захищеності комп'ютерних систем ("Жовтогаряча книга").
2. Європейські критерії оцінки безпеки інформаційних технологій (розроблені з урахуванням виявлених недоліків і обмежень використання "Жовтогарячої книги").
3. Канадські критерії оцінки безпеки надійних комп'ютерних систем.
4. Федеральні критерії США, розроблені на замовлення уряду США і спрямовані на усунення обмежень, незручностей практичного застосування і недоліків "Жовтогарячої книги".
5. Міжнародний стандарт ISO/IEC 15408 "Критерії оцінки безпеки інформаційних технологій", або Єдині критерії.
6. Робочий проект стандарт CEM-97/017 "Загальна методологія оцінки безпеки інформаційних технологій".

Перераховані нормативні документи, особливо останні два – роблять істотний внесок у формування єдиної міжнародної науково-методологічної бази вирішення проблеми інформаційної безпеки в програмних продуктах та інформаційних технологіях. Аналіз цих документів підтверджує той факт, що для розв'язання задач забезпечення ІБ, поряд з формальними методами моделювання процесів і оцінювання ефективності функціонування систем необхідно широко використовувати методи декомпозиції і структуризації компонентів систем і процесів, неформальні методи оцінки ефективності функціонування і прийняття рішень. Це означає, що апарат системного аналізу необхідно використовувати на всіх етапах життєвого циклу систем захисту інформації [4].

Але існуючі стандарти і документи, які ґрунтуються на них, не дають відповідей на низку ключових запитань.

1. Як створити інформаційну систему, захищену на необхідному рівні, що об'єктивно перевіряється?

2. Як практично сформувати режим безпеки і підтримувати його в умовах постійно змінного зовнішнього оточення і структури самої системи?

3. Який реальний рівень безпеки і наскільки ефективна система захисту інформації?

Поняття системності полягає не просто в створенні відповідних механізмів захисту, а являє собою регулярний процес, що здійснюється на всіх етапах життєвого циклу ІС. При цьому всі засоби, методи і заходи, використовувані для захисту інформації, поєднуються в цілісний механізм – систему захисту інформації (СЗІ).

Вже в перших роботах із захисту інформації було викладено основні постулати, що не втратили своєї актуальності і сьогодні: абсолютний захист створити не можна; СЗІ повинна бути комплексною; СЗІ повинна адаптуватись до умов, які постійно змінюються.

До цих аксіом потрібно додати й інші. По-перше, СЗІ повинна бути саме системою, а не простим, багато в чому випадковим і хаотичним набором деяких технічних і організаційних заходів, як це найчастіше спостерігається на практиці. По-друге, системний підхід до захисту інформації повинен застосовуватися, починаючи з підготовки технічного завдання і закінчуючи оцінкою ефективності і якості СЗІ в процесі її експлуатації.

На жаль, необхідність системного підходу до питань забезпечення безпеки інформаційних технологій поки ще не знаходить належного розуміння в користувачів сучасних ІС. Сьогодні фахівці із різних областей знань так чи інакше змушені займатися питаннями забезпечення інформаційної безпеки. Це обумовлено тим, що ми живемо в суспільстві (середовищі) інформаційних технологій, що накладає відбиток на усі соціальні проблеми людства, зокрема і питання безпеки. Якщо зібрати усіх фахівців разом, то за наявності в кожного з них величезного знань і досвіду створити систему інформаційної безпеки найчастіше так і не вдається. Розмовляючи про ті ж самі речі, фахівці найчастіше не розуміють один одного, оскільки в кожного з них свій підхід, своє уявлення про систему захисту інформації. Такий стан справ зумовлений відсутністю системного підходу до існуючих понять, визначень, принципів, способів і механізмів захисту.

Основні завдання засобів інформаційної безпеки в системах електронної комерції. Для дослідження механізмів загроз ІБ результати окремої оцінки ризиків і рекомендацій не мають великого значення. Вивчення взаємодії системи, норми та ситуації експлікується за допомогою моделей теорії ймовірностей, які передбачають здійснення масового експерименту, за якого одна і та сама загроза ІБ (подія) повторюється багато разів. Ці випробування, що повторюються, утворюють серії, в кожній з яких подія з'являється або не з'являється певну кількість разів [3].

Вибір тієї чи іншої моделі опису оцінки ризиків залежить від побудови імовірнісного випробування і, зокрема, від того, як організовано вибір з переліку окремих його одиниць.

Розглянемо такий елементарний приклад. Нехай з переліку загроз ІБ взято N подій, серед яких n небезпечних з серйозними наслідками та m незначних загроз, і кожна з подій відбувалась на певному проміжку часу x_i разів ($i = \overline{1,k}$, $k = n + m$, $N = \sum_{i=1}^{k} x_i$); події відбулися без певної взаємозалежності, періодичності та черговості. Дослідження випробувань, які полягають у аналізі цих подій на певному проміжку часу, можуть здійснюватись за двома схемами.

За умовами першої схеми кожну здійснену подію вважають такою, що може повторитися через деякий час, після того як у протоколі фіксується результат кожного випробування. Під час кожного наступного дослідження випробування ймовірності появи тієї чи іншої події залишаються незмінними. Ці ймовірності відповідно дорівнюють n/N та m/N. Ймовірнісно-зогрозливий експеримент, який оперує з наслідками взаємно незалежних випробувань, у кожному з яких події загроз зберігають свої безумовні ймовірності, називається *повторною вибіркою*.

За іншою схемою здійснені події вважають такими, що не повторюються. Ймовірність появи тієї чи іншої події у кожному наступному випробуванні залежить від результатів попередніх випробувань. Отже, ми здійснюємо залежні випробування, а ймовірність результату кожного випробування є умовною. Експеримент, який проводять з послідовністю залежних випробувань, у кожному з яких результати мають умовні ймовірності, називається *безповторною (або без повернень) вибіркою*.

Реальний ймовірнісно-загрозливий експеримент можна проводити як за допомогою повторної, так і безповторної вибірки [2].

Для дослідження загроз ІБ та оцінювання ризиків використовують метод серійного спостереження. Суть його полягає в тому, що події (загрози) вибираються з фіксованого переліку групою: наприклад, по 3–5 подій (загроз) тощо. Події, які утворюють серію, не обов'язково мають відбуватися одна за однією; вони можуть реалізовуватись через певний часовий інтервал. Для розв'язування багатьох теоретичних та інженерних задач часто потрібно знати ймовірність появи тієї чи іншої кількості певних одиниць загроз у серії. Якщо випробування ризиків, які утворюють серію, розглядаються як незалежні, то ми можемо здійснювати необхідне прогнозування за допомогою розробленого гіпергеометричного закону. Математична модель ризиків, за якою прогнозують результати гіпергеометричного закону випробувань, є основою для побудови інших імовірнісних моделей, зокрема й тих, котрі широко використовуються у дослідженні переліку загроз ІБ.

Гіпергеометричний закон може поширюватися тільки на скінченні генеральні сукупності, об'єм яких відомий. Оскільки в задачах про загрози в ІБ об'єм генеральної сукупності ризиків, які породжуються відкритою СЕК, зазвичай не є скінченною величиною, то застосування вказаного закону для прогнозування результатів дослідів загроз у безповторних вибірках виявляється нереальним. Разом з цим, за певних умов гіпергеометрична ймовірність добре апроксимується біноміальною ймовірністю. Тому, не ризикуючи втратити математичну строгість, розрахуємо ймовірність появи події A рівно x разів у нашій безповторній вибірці так, ніби йдеться про повторну вибірку. Іншими словами, ми застосовуємо до безповторних вибірок біноміальний закон.

Розглянемо S серій або вибірок, кожна з яких складається з N незалежних випробувань [4]. Загроза (подія) A може з'явитись у кожній серії x разів (x = 0, 1, 2, …, N). Отже, є групи серій, в яких A з'являється 0, 1, 2, ..., N разів. Тобто відносна частота появи події A рівно x разів у одній серії визначається співвідношенням

$$f_N(x) = S_x / S ,$$

де S_x – кількість серій, у яких подія A з'явиться рівно x разів.

Апріорна ймовірність появи події A в одній навмання взятій серії дорівнює

$$p \approx \frac{\sum x S_x}{NS},$$

і, отже,

$$q \approx 1 - \frac{\sum x S_x}{NS}.$$

В одержаному теоретичному розподілі кожному значенню x співвіднесена не його ймовірність, а деяка теоретично очікувана кількість серій (вибірок) S_x^T, у яких подія A з'являється рівно x разів.

Оскільки

$$S_x^T = SP_N(x) = SC_N^x p^x q^{N-x}, \qquad (1)$$

то величини S_x^T та $P_N(x)$ зв'язані коефіцієнтом пропорційності S.

Так, для визначення особливостей ІБ деякої системи електронної комерції було навмання зафіксовано 100 часових проміжків (відрізків) функціонування СІЗ по Δt діб кожен (наприклад, 10 діб кожен).

Приклад розподілу частот появи загроз у цих серіях подано в табл. 1. Необхідно обчислити теоретичний біноміальний розподіл ймовірностей появи x загроз у одній серії.

Таблиця 1

Приклад розподілу частот появи загроз

Кількість появ події x	0	1	2	3	4	5	6	7	8	9	10	
Емпіричні частоти появи вибірок S_x	0	1	4	15	33	27	11	4	2	1	2	ΣS_x =100

У прикладі S=100, N=10. Використовуючи добутки величин x та S_x, наведені у табл. 1, знаходимо

$$p = \frac{\sum xS_x}{NS} = \frac{0\cdot 0 + 1\cdot 1 + 2\cdot 4 + 3\cdot 15 + \cdots + 8\cdot 2 + 9\cdot 1 + 10\cdot 2}{10\cdot 100} = \frac{460}{1000} = 0.46.$$

Візьмемо $p \approx 0.3$ та $q \approx 0.7$, тоді на основі подвійної нерівності

$$Np + p - 1 \le x_0 \le Np + p. \qquad (2)$$

маємо $10\cdot 0.3 - 0.7 < x_0 < 10\cdot 0.3 - 0.7 + 1$, або $2.3 < x_0 < 3.3$, звідки випливає, що $x_0 = 3$. Тоді $P_N(x_0) = P_{10}(3) = C_{10}^3 \cdot 0.3^3 \cdot 0.7^7$. Звідси (використовуючи калькулятор з функцією x^y або логарифми), знаходимо, що $P_{10}(3) = 0.2667$. Отже, $S_x^T = SP_{10}(3) = 100\cdot 0.2667 \approx 26.67$. Решту значень очікуваної кількості вибірок наведено у табл. 2.

Таблиця 2

Очікувана кількість вибірок

X	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
S_x	0	1	4	15	33	27	11	4	2	1	2	**100**
$P_N(x)$	0.0282	0.1211	0.2335	0.2668	0.2001	0.1029	0.0368	0.0090	0.0014	0.0001	0.0000	**1.0**
S_x^T	3	12	23	27	20	10	4	1	0	0	0	**100**

Визначення вимог до заходів захисту і вибір основних рішень щодо забезпечення режиму ІБ. Визначення вимог до засобів захисту передбачає такі етапи: формулювання вимог до ІБ на основі аналізу функцій і задач ІС з урахуванням проведеного аналізу ризиків. Вимоги до ІБ формулюються в термінах функцій і механізмів безпеки; вибір профілю захисту (класу захищеності системи електронної комерції від несанкціонованого доступу (НСД)). У виборі основних рішень щодо забезпечення режиму ІБ проводиться структуризація комплексу заходів за рівнями: адміністративному (розроблення і виконання програми ІБ); організаційному (організація роботи персоналу і регламентація його дій); програмно-технічному (програмно-технічна реалізація механізмів безпеки).

На **адміністративному рівні забезпечення ІБ** повинні бути вироблені: система підтримки керівництвом організації заходів щодо забезпечення ІБ, виконання правових і договірних вимог у сфері ІБ; процедура доведення до відома співробітників основних положень концепції ІБ, вимоги по навчанню персоналу правилам ІБ; система контролю за реалізацією прийнятих рішень і відповідальні посадові особи.

На **організаційному рівні забезпечення ІБ** мають бути розглянуті: організаційна структура служби, що відповідає за забезпечення режиму ІБ, розподіл обов'язків; комплекс профілактичних заходів (попередження появи вірусів, попередження ненавмисних дій, які призводять до порушення ІБ); організація доступу співробітників сторонніх організацій до ресурсів системи електронної комерції; організація доступу користувачів і персоналу до конкретних ресурсів системи електронної комерції; політика щодо окремих аспектів: віддалений доступ до системи електронної комерції, використання відкритих ресурсів (Інтернет), використання несертифікованого програмного забезпечення (ПЗ) тощо.

На **програмно-технічному рівні забезпечення ІБ** розглядаються програмно-технічні засоби, які реалізують задані вимоги. Якщо вимоги формулювалися в термінах функцій (сервісів) безпеки, розглядаються механізми безпеки і відповідні їм варіанти програмних і апаратних реалізацій [1–4]. Якщо вимоги формулювалися за підсистемами ІС, розглядаються варіанти програмно-апаратної реалізації цих підсистем. Під час розгляду різних варіантів рекомендується враховувати такі аспекти: управління доступом до інформації і сервісів, враховуючи вимоги до розподілу обов'язків і ресурсів; реєстрація подій у журналі з метою щоденного контролю або спеціальних розслідувань; перевірка і забезпечення цілісності критично важливих даних на всіх стадіях їх опрацювання; захист конфіденційних даних від несанкціонованого доступу, зокрема використання засобів шифру-

вання; резервне копіювання критично важливих даних; відновлення роботи системи електронної комерції після відмов, особливо для систем з підвищеними вимогами щодо доступності; захист від внесення несанкціонованих доповнень і змін; забезпечення засобів контролю, наприклад, за допомогою використання програм у вибірковому контролі та альтернативні варіанти програмного забезпечення для повторення критично важливих обчислень.

Висновки. Запропоновано методи прогнозування результатів масових випробувань ризиків в системах електронної комерції. Такі прогнози поки що можна здійснювати стосовно повторних вибірок, ґрунтуючись на класичному означенні ймовірності, тобто за умови, що дослід здійснюється відносно обмеженої за обсягом сукупності об'єктів

1. Берко А.Ю., Висоцька В.А., Чирун Л.В. Алгоритми опрацювання інформаційних ресурсів в системах електронної комерції // Вісн. Нац. ун-ту "Львівська політехніка". – 2004. – № 519. – С. 10–20. 2. Берко А.Ю., Висоцька В.А. Проектування навігаційного графу web-сторінок бази даних систем електронної комерції // Вісн. Нац. ун-ту "Львівська політехніка". – 2004. – № 521. – С. 48–57. 3. Береза А.М. Електронна комерція. – К., 2002. 4. Верес О.М., Верес О.О., Рішняк І.В. Методи оцінки та моделі управління банківськими ризиками // Вісн. Нац. ун-ту "Львівська політехніка". – 2004. – № 519.

УДК 621.382

Білаль Аль-Забі, А.Б. Керницький, С.П. Ткаченко
Національний університет "Львівська політехніка",
кафедра систем автоматизованого проектування

ВСТАНОВЛЕННЯ ІСНУВАННЯ НЕОБХІДНИХ УМОВ ЕКВІВАЛЕНТНОСТІ СХЕМ

Розглянуті можливі шляхи встановлення існування необхідних умов еквівалентності схем РЕА під час розв'язання задач верифікації і функціональної декомпозиції схем. У першому випадку необхідно реалізувати класифікатор схемних елементів. Інший варіант розв'язання задачі – реалізація класифікатора схемних ланцюгів.

Some possible ways to determine scheme equivalence necessary conditions have been considered. Scheme equivalence is to be checked while solving the problems of verification or functional decomposition of schemes. In the first case, a scheme element classifier is to be realized. Another solution variant applies net classifier.

Вступ. Під час розв'язання задач функціональної декомпозиції схем верифікації результатів проектування буває необхідно розробити ефективні алгоритми попарного встановлення еквівалентності схем. Водночас задачі такого типу належать до NP-повних задач [1], розв'язання яких вимагає достатньо великих часових витрат навіть у разі використання поліноміальних алгоритмів, побудованих на евристичних прийомах. У зв'язку з цим виникає проблема попереднього, з відносно невеликими часовими витратами, аналізу можливості розв'язання задачі, тобто встановлення існування необхідних умов еквівалентності схем.

Моделі схем та їх елементів. При встановленні еквівалентності схем значну увагу необхідно приділити вибору моделей схем та їхніх елементів, оскільки це може суттєво вплинути на ефективність розв'язку задач як з погляду швидкодії, так і з погляду власне встановлення функціональної еквівалентності схем (які, наприклад, відповідають окремим конструктивам або схемі вхідного завдання) і відновленої з результуючої топології. Відповідно, на вибір моделі можуть вплинути такі фактори: