УДК 681.3.06

А.М. Хнигічева, О.М. Новіков,
А.О. Тимошенко

МОДЕЛЮВАННЯ ЗАХИЩЕНОСТІ СКЛАДНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ІЗ ВИКОРИСТАННЯМ ЛОГІКО-ЙМОВІРНІСНОГО МЕТОДУ

Вступ

Питання інформаційної безпеки є одним із найважливіших питань національної безпеки України [1]. Це пов'язано з швидким розвитком інформаційних технологій у світі, що в свою чергу впливає на розвиток даних технологій у кожній країні окремо.

Із врахуванням відомого закону Мура [2] інформаційні технології з кожним роком розвиваються в кілька разів швидше, ніж в попередні роки. Питання інформаційної безпеки в цих умовах набуває принципового значення.

Важливим моментом у розвитку інформаційно-комунікаційних систем було введення єдиного підходу до формалізації будови систем із відкритою архітектурою та еталонної моделі взаємодії відкритих систем ISO/OSI [3, 4]. Саме тому системи з відкритою архітектурою характеризуються складною взаємодією окремих інформаційних систем різного походження, що відносить їх до класу структурно складних.

Різні аспекти безпеки структурно складних систем розглядались І.О. Рябініним, О.С. Можаєвим та іншими вченими [5, 6]. У працях цих науковців було запропоновано та розвинуто логіко-ймовірнісні методи для дослідження надійності складних систем у суднобудуванні, нафтогазовій промисловості, економіці, бізнесі тощо [7]. У працях Харрісона, Руссо, Ульмана, Белла, Лападула, Біба та інших дослідників було запропоновано низку моделей безпеки структурно складних інформаційних систем, що широко використовуються для дослідження інформаційної безпеки [8]. У працях вітчизняних учених М.З. Згуровського і Н.Д. Панкратової запропоновано методологію дослідження безпеки структурно складних систем з позиції системного аналізу [9, 10]. В.П. Горбулін і А.Б. Качинський розглядали питання безпеки систем різного характеру з позиції їх як складових національної безпеки [11], О.М. Новіков і А.О. Тимошенко досліджували захищеність інформації, що обробляється в інформаційно-комунікаційних системах із відкритою архітектурою та багаторівневим стеком протоколів [12]. Захищеність інформації прийнято визначати такими властивостями, як конфіденційність, цілісність та доступність інформації. Однак у зв'язку із складністю, багатоаспектністю та широким поширенням інформаційно-комунікаційних систем питання аналізу безпеки систем даного класу залишається актуальним.

Як уже зазначалося, ефективним підходом до аналізу захищеності інформації, що обробляється в інформаційно-комунікаційних системах, є логіко-ймовірнісний метод. Використання цього методу дає можливість за наявними відомими загрозами та механізмами їх нейтралізації обчислювати інтегральний показник захищеності даної системи. За своїм змістом інтегральний показник захищеності системи є ймовірністю збереження системою захищеного стану, що об'єднує різні показники ймовірностей збереження системою захищеного стану, які залежать від реалізації загроз, спрямованих на окремі властивості інформації: конфіденційність, цілісність та доступність. Крім зазначених вище переваг інтегрального показника захищеності, можна назвати окремі випадки, коли актуальним є аналіз часткових показників захищеності: за конфіденційністю, цілісністю та доступністю. Такий аналіз є необхідним у випадках підвищених вимог до окремих властивостей інформації [13]. Дослідження, спрямовані на вирішення даної проблеми, потребують подальшого розвитку.

Постановка задачі

Метою даної статті є розробка підходу до аналізу захищеності інформаційно-комунікаційних систем, що базується на використанні логіко-ймовірнісного методу і відрізняється покомпонентним виокремленням загроз захищеності складної інформаційної системи з подальшою інтеграцією їх у складі єдиного комплексного показника захищеності. Останнє дасть змогу підвищити якість аналізу захищеності системи та зменшити витрати на етапі проектування системи захисту інформації.

Моделювання захищеності інформації з використанням логіко-ймовірнісного підходу

Проблеми оцінки ймовірності відмов компонентів складних технічних систем під впливом загроз, а також аналізу ризиків, пов'язаних

з їх реалізацією, досліджені в працях О.С. Можаєва, І.О. Рябініна, Є.Д. Соложенцева [5–7]. Згідно з логіко-ймовірнісним підходом, запропонованим у даних публікаціях, визначення ймовірності виникнення небезпечного стану системи (НСС) $\text{Н}_\text{с}$ визначається таким виразом:

$$\text{Н}_\text{с} = P\{F(X_1,...,X_m) = 1\},$$

де $F(X_1,...,X_m)$ – функція алгебри логіки від умови небезпечних станів системи.

При цьому ймовірність виникнення безпечного стану $\text{Б}_\text{с}$ визначається як

$$\text{Б}_\text{с} = P\{F'(X_1,...,X_m) = 1\} = 1 - \text{Н}_\text{с}.$$

Для побудови моделі захищеності використаємо підхід, запропонований у [12], що базується на моделі безпеки з повним перекриттям [14].

Модель системи безпеки з повним перекриттям будується згідно з постулатом, що система безпеки повинна мати принаймні один засіб для забезпечення безпеки на кожному можливому способі реалізації (впливу) загрози.

У моделі точно визначається кожна область, що вимагає захисту, оцінюються засоби забезпечення безпеки з погляду на їх ефективність та їх внесок у забезпечення безпеки у всій системі.

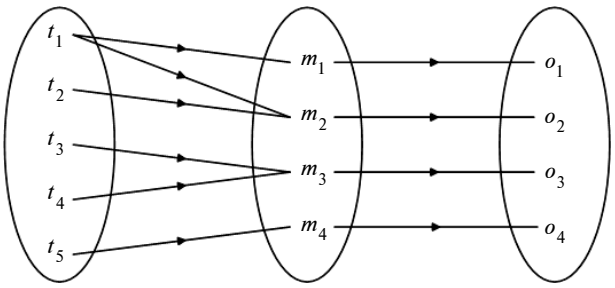

Рис. 1. Модель безпеки з повним перекриттям

На рис. 1 наведено модель безпеки з повним перекриттям, де $t_1,...,t_5 \in T$; T – множина загроз безпеці системи; $m_1,...,m_4 \in M$; M – множина механізмів захисту; $o_1,...,o_4 \in O$, де O – множина об'єктів, які потрібно захищати.

Вибір характеристик загроз, які вводяться в модель, і способів їх реалізації

Вибір характеристик загроз є ключовим моментом у розробці моделі безпеки. Згідно з [13] вибір загроз безпеці інформації здійснюється із врахуванням особливостей конкретної системи, інформаційних об'єктів, що обробляються в даній системі, та зовнішніх чинників. Коли можливі загрози вибрані, то за допомогою існуючих підходів, викладених у [15], проводиться їх класифікація і на основі експертної оцінки знаходяться значення показників, що характеризують можливий вплив на систему результатів реалізації загрози.

Для знаходження даних показників використаємо підхід, запропонований у [12]. Виберемо показником, що характеризує загрозу, показник ефективності реалізації загрози, що відображає в собі як імовірнісні характеристики реалізації загрози, так і збиток, який реалізація загрози може завдати системі.

Згідно з цим підходом вираз для розрахунку показника ефективності реалізації i-ї загрози, спрямованої на порушення певної властивості інформації на j-му рівні стеку проколів E_{ij}, має вигляд

$$E_{ij} = Q_{ij} R_{ij}, \qquad (1)$$

де Q_{ij} – показник, що характеризує частку (величину) збитку, що вноситься i-ю загрозою в сумарний вихідний ефект; R_{ij} – показник, що характеризує ймовірність реалізації i-ї загрози.

Таким чином, множина загроз T в моделі, що розробляється, має бути виражена множиною показників ефективності їх реалізації $E = \{E_i\}$, $i \in \{1,...,L\}$, де E_i – показник ефективності реалізації i-ї загрози; L – кількість виявлених загроз, внесених у множину загроз T.

Згідно з [12] після аналізу ризиків здійснюється вибір механізмів захисту.

Вибір характеристик механізмів захисту, які вводяться в модель

Другим ключовим моментом при побудові моделі безпеки є вибір характеристик механізмів захисту. Ймовірність працездатності механізму захисту в [12] визначається як ймовірність запобігання з його допомогою відповідній загрозі. Дана характеристика визначається таким чином:

$$P_{M_i} = M_i K_i,$$

де M_i – цілочисельний параметр, значення якого (0 або 1) визначає факт наявності/відсутності механізму захисту від i-ї загрози;

K_i – коефіцієнт міцності механізму захисту від *i*-ї загрози, що характеризує ступінь його надійності з погляду на запобігання загрозам безпеці системи.

Таким чином, в моделі, що розробляється, множина механізмів M має бути задана у вигляді $M = \{M_i\}, i \in \{1,...,L\}$, де M_i – цілочисельний параметр, значення якого (0 або 1) визначає факт наявності/відсутності механізму захисту від *i-ї* загрози; L – кількість виявлених загроз безпеці системи, внесених у множину загроз T. Крім того, як характеристики механізмів захисту в модель має бути введена множина коефіцієнтів міцності механізмів захисту $K = \{K_i\}$.

Множина коефіцієнтів визначається здатністю механізму захисту протидіяти певним способам реалізації загроз за умови використання даних механізмів. Наприклад, коефіцієнт міцності механізму захисту керування доступом визначається із врахуванням розрядності системи, коефіцієнт міцності криптографічного механізму захисту знаходиться із врахуванням довжини ключа шифрування.

Таким чином, модель оцінки ймовірності збереження безпечного стану P можна визначити як функцію множини загроз безпеці системи T, виражених показниками ефективності їх реалізації E і множини реалізованих у системі механізмів захисту M з коефіцієнтами міцності K:

$$P = f(E, M, K).$$

Даний підхід було запропоновано в [12].

Комплексний підхід до моделювання захищеності інформаційно-комунікаційних систем

Позначимо величини вимірювання показників захищеності системи, які залежать від реалізації загроз, спрямованих на окремі властивості інформації – конфіденційність, цілісність та доступність ймовірності – $P_к, P_ц, P_д$ і назвемо їх частковими показниками захищеності інформаційної системи. Для цього задамо систему координат, в якій координатними векторами будуть вектори, довжини яких відповідатимуть значенню даних часткових показників захищеності (рис. 2).

Розглянемо деякий комплексний показник захищеності інформації C, що буде результуючим вектором від векторів часткових показників захищеності інформаційної системи. Його евклідова норма залежатиме від $P_к, P_ц, P_д$ і характеризуватиме рівень захищеності інформації, що обробляється в інформаційно-комунікаційній системі:

$$|C| = \sqrt{(P_1^2 + P_2^2 + P_3^2)}.$$

Даний підхід традиційно використовується в моделях із комплексним показником стану систем різного класу, зокрема в задачах моделювання сталого розвитку [16].

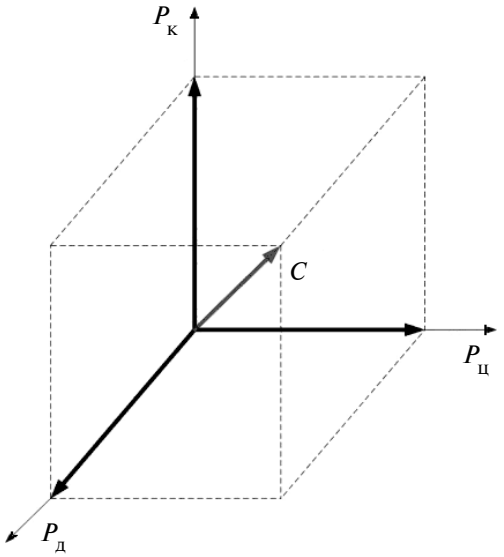

Рис. 2. Простір захищеності

Враховуючи сказане, визначимо характеристики часткових показників захищеності системи. Виокремивши властивості інформації та зробивши всі необхідні викладки і перетворення за допомогою логіко-ймовірнісного методу [12], отримаємо такі вирази ймовірностей реалізації НСС для кожної властивості системи окремо:

$$T_{i1}(M) = \sum_{j=1}^{N}\left(E_{j1}\prod_{k=1}^{j-1}(1 - E_{k1})\prod_{k=1}^{j}(1 - M_{k1}K_{k1})\right),$$

$$T_{i2}(M) = \sum_{j=1}^{N}\left(E_{j2}\prod_{k=1}^{j-1}(1 - E_{k2})\prod_{k=1}^{j}(1 - M_{k2}K_{k2})\right),$$

$$T_{i3}(M) = \sum_{j=1}^{N}\left(E_{j3}\prod_{k=1}^{j-1}(1 - E_{k3})\prod_{k=1}^{j}(1 - M_{k3}K_{k3})\right).$$

На основі отриманих значень визначимо вирази для ймовірнісних функцій оцінки захищеності при умові реалізації однієї j-ї загрози, що реалізується на i-му рівні стеку протоколів для кожної властивості системи окремо:

$$P_{i1}(M) = \prod_{j=1}^{N}(1 - E_{j1}) +$$

$$+\sum_{j=1}^{N}\left[E_{j1}\prod_{k=1}^{j-1}(1 - E_{k1})\left(\sum_{k=1}^{j} M_{k1}K_{k1}\prod_{l=k+1}^{j}(1 - M_{l1}K_{l1})\right)\right],$$

$$P_{i2}(M) = \prod_{j=1}^{N}(1 - E_{j2}) +$$

$$+\sum_{j=1}^{N}\left[E_{j2}\prod_{k=1}^{j-1}(1 - E_{k2})\left(\sum_{k=1}^{j} M_{k2}K_{k2}\prod_{l=k+1}^{j}(1 - M_{l2}K_{l2})\right)\right],$$

$$P_{i3}(M) = \prod_{j=1}^{N}(1 - E_{j3}) +$$

$$+\sum_{j=1}^{N}\left[E_{j3}\prod_{k=1}^{j-1}(1 - E_{k3})\left(\sum_{k=1}^{j} M_{k3}K_{k3}\prod_{l=k+1}^{j}(1 - M_{l3}K_{l3})\right)\right].$$

Враховуючи ж всю множину загроз, дані вирази перепишемо у вигляді

$$P_1(M) = \prod_{i=1}^{L_1}\left(\prod_{j=1}^{N}(1 - E_{ij1}) + \sum_{j=1}^{N}\left[E_{ij1}\prod_{k=1}^{j-1}(1 - E_{ik1}) \times \right.\right.$$

$$\left.\left. \times\left(\sum_{k=1}^{j} M_{ik1}K_{ik1}\prod_{l=k+1}^{j}(1 - M_{il1}K_{il1})\right)\right]\right), \qquad (2)$$

$$P_2(M) = \prod_{i=1}^{L_2}\left(\prod_{j=1}^{N}(1 - E_{ij2}) + \sum_{j=1}^{N}\left[E_{ij2}\prod_{k=1}^{j-1}(1 - E_{ik2}) \times \right.\right.$$

$$\left.\left. \times\left(\sum_{k=1}^{j} M_{ik2}K_{ik2}\prod_{l=k+1}^{j}(1 - M_{il2}K_{il2})\right)\right]\right), \qquad (3)$$

$$P_3(M) = \prod_{i=1}^{L_3}\left(\prod_{j=1}^{N}(1 - E_{ij3}) + \sum_{j=1}^{N}\left[E_{ij3}\prod_{k=1}^{j-1}(1 - E_{ik3}) \times \right.\right.$$

$$\left.\left. \times\left(\sum_{k=1}^{j} M_{ik3}K_{ik3}\prod_{l=k+1}^{j}(1 - M_{il3}K_{il3})\right)\right]\right), \qquad (4)$$

де L_1, L_2, L_3 – кількості загроз, внесених у множину T по кожній властивості інформації окремо; N – кількість рівнів стеку протоколів системи.

Запишемо норму вектора C із врахуванням розрахованих співвідношень інших векторів:

$$\|C\| = \sqrt{(P_1^2 + P_2^2 + P_3^2)}\,. \qquad (5)$$

Наближення значення норми вектора $\|C\|$ до значення норми "ідеального" вектора $\|1\| = \sqrt{(1^2 + 1^2 + 1^2)}$ характеризуватиме рівень захищеності інформації, що обробляється в інформаційно-комунікаційній системі.

Таким чином, у виразах (2)–(4) отримано співвідношення для визначення рівня захищеності інформації, що обробляється в інформаційно-комунікаційній системі, яка має три властивості L_1, L_2, L_3 загроз, спрямованих на окремі властивості інформації системи та N рівнів стеку протоколів. У виразі (5) знайдено співвідношення для визначення комплексного показника захищеності системи, що залежить від отриманих у (2)–(4) часткових показників захищеності інформації.

Для того щоб довести адекватність даної моделі, далі буде проведено її перевірку за допомогою обчислювального експерименту.

Обчислювальний експеримент

Для дослідження запропонованої моделі інформаційної безпеки було вибрано систему централізованого керування мережевими ресурсами, що призначена для керування інформаційними ресурсами сучасної компанії. Схему фізичної структури даної системи наведено на рис. 3, а схему логічної структури системи – на рис. 4. При проведенні обчислювального експерименту загрози вибиралися таким чином, щоб враховувалась топологія системи, показники ефективності загроз безпеці інформації розраховувалися за допомогою експертної оцінки з використанням методу аналізу ієрархій [17]. Розглядався чотирирівневий стек протоколів TCP/IP. Під час експертної оцінки загрози були розділені за впливом на інформаційні об'єкти в певних компонентах системи, з певними властивостями інформації та рівнями стеку протоколів. Коефіцієнти міцності механізмів захисту вибирались залежно від механізмів захисту, що використовуються в системі.

Метою даного експерименту було дослідити запропоновану модель, довести її адекватність та проаналізувати отримані показники. Експеримент проводився у спосіб розрахунку

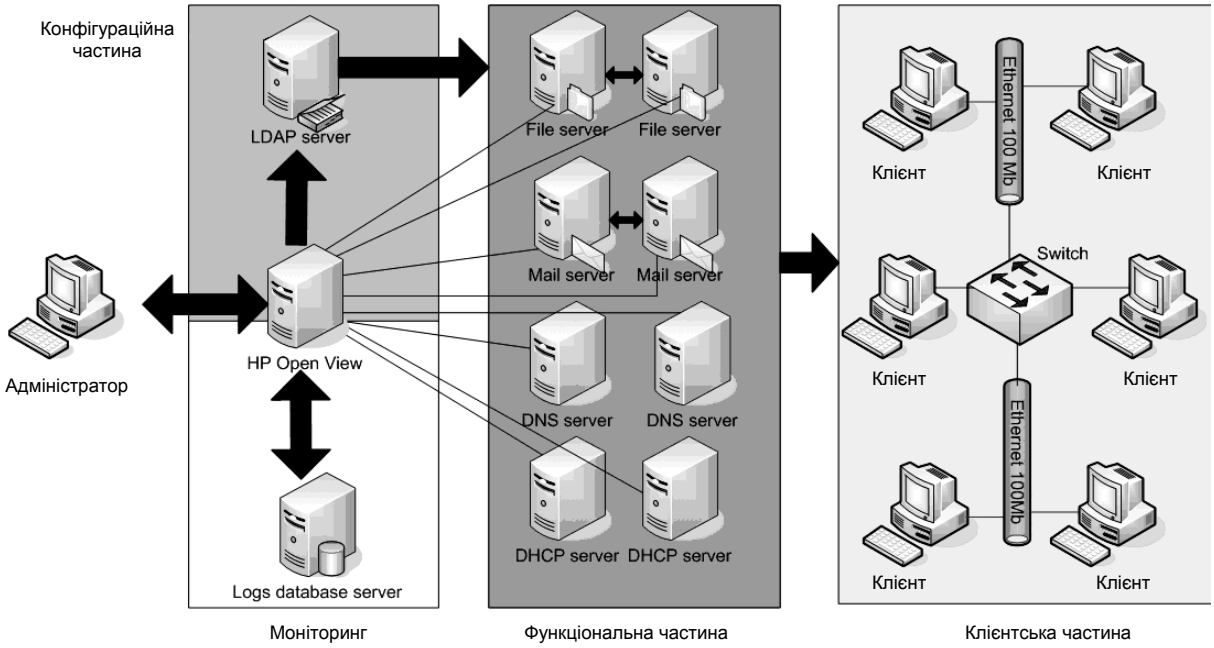

Рис. 3. Схема фізичної структури системи

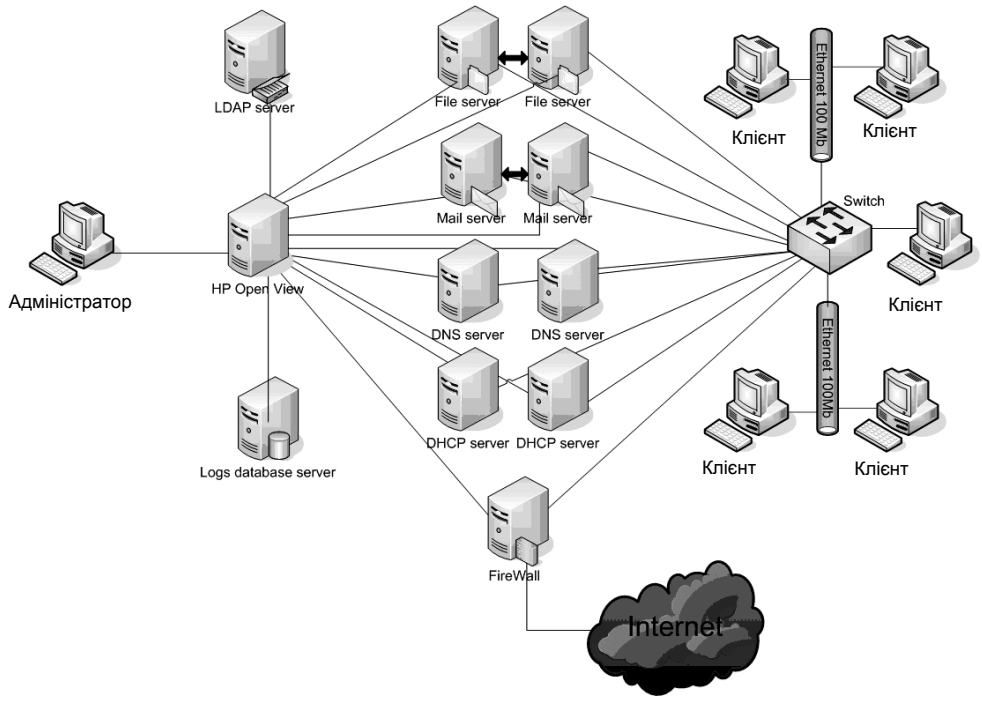

Рис. 4. Схема логічної структури системи

значень показників за допомогою розробленого програмного комплексу. Вхідними даними були розраховані експертами за співвідношенням (1) ймовірнісні характеристики загроз та механізмів захисту, спрямованих на нейтралізацію даних загроз. Приклад інтерпретації загроз для компонентів системи, таких, як сервер СУБД та клієнт СУБД наведено в табл. 1, а приклад механізмів захисту – в табл. 2.

Результуючими даними є часткові показники ймовірностей збереження системою захищеного стану, які залежать від реалізації загроз, спрямованих на окремі властивості інформації, комплексний показник захищеності інформації, що обробляється в інформаційно-комунікаційній системі, та інтегральний показник захищеності інформації, розрахований за методом, описаним у [12].

***Таблиця* 1**. Приклад загроз

Спосіб реалізації загроз, спрямованих на порушення захищеності клієнта СУБД	Мета дії			Рівень стеку TCP/IP			
	Конфіденційність	Цілісність	Доступність	Канальний	Мережевий	Транспортний	Прикладний
Несанкціоноване використання ресурсів БД	+	+	+				+
Несанкціонована модифікація запису БД		+					+
Несанкціоноване знищення запису БД		+					+
Несанкціонована зміна програмного забезпечення		+	+				+
Підбір/перехоплення паролів (даних аутентифікації)	+	+	+			+	+
Захоплення надмірного об'єму ресурсів			+				+
Відмова від факту введення/зміни інформації		+					+
Підміна довіреного сервера БД	+	+	+		+	+	+
Нав'язування помилкового сервера БД			+		+	+	+

***Таблиця* 2.** Приклад механізмів захисту

Опис механізму захисту	Рівень протоколу стеку TCP/IP, на якому повинен бути реалізований механізм			
	Канальний	Мережевий	Транспортний	Прикладний
Цифровий підпис повідомлень, оброблюваних на РС клієнта і ПС				+
Керування доступом до файлів даних, збереженим на РС клієнта				+
Використання засобів взаємної строгої автентифікації РС клієнта			+	
Забезпечення цілісності потоку даних, переданих між РС клієнта і ПС			+	
Забезпечення цілісності файлів даних, збережених на ПС				+
Використання засобів автентифікації користувачів ПС				+
Використання засобів взаємної строгої автентифікації ПС і РС ЛВС			+	
Керування доступом до файлів даних, збережених на ПС				+
Шифрування повідомлень, оброблюваних на РС клієнта і ПС				+

Для того щоб перевірити граничні значення комплексного показника захищеності, розглянемо два сценарії.

Сценарій 1. Зловмисник має доступ до всіх компонентів системи і ніщо не обмежує його дій. У даній ситуації ймовірнісні показники загроз дорівнюють 1.

Сценарій 2. Зловмисник не має жодного доступу, тобто система ізольована від зовнішньої мережі, ймовірнісні показники загроз дорівнюють 0.

Отримані під час розрахунку дані та дані кінцевих значень наведено в табл. 3.

У результаті перевірки даного методу було отримано інтегральний показник захищеності,

***Таблиця* 3.** Порівняння отриманих показників з їх кінцевими значеннями

Стан системи	P_1	P_2	P_3	C
Мінімально захищена система	0	0	0	0
Досліджувана система	0,999491	0,98215	0,753851	1,59119
Максимально захищена система	1	1	1	1,73205

який становить $P = 0,758318$. Цей показник дає можливість визначити рівень захищеності інформації, що обробляється в досліджуваній системі, і зробити висновок, що даний рівень є недостатнім. З іншого боку, отримані за допомогою розробленого підходу часткові показники ймовірностей збереження системою захищеного стану, які залежать від реалізації загроз, спрямованих на окремі властивості інформації, мають такі значення: $P_{к} = 0,999491$, $P_{ц} = 0,98215$, $P_{д} = 0,753851$. Комплексний показник захищеності інформації C дорівнює 1,59119. Якщо проаналізувати значення комплексного показника захищеності інформації, то отримані дані дають можливість впевнитись, що дана система є недостатньо захищеною, а якщо врахувати ще часткові показники ймовірностей збереження системою захищеного стану, які залежать від реалізації загроз, спрямованих на окремі властивості інформації, то можна точно визначити, які загрози, спрямовані на яку властивість інформації, впливають на отриманий рівень захищеності системи. Це дає змогу враховувати отримані значення під час проектування системи, щоб спрямувати всі зусилля на підвищення рівня захищеності тільки тих властивостей інформації, які є найбільш критичними для системи.

Інтерпретація результатів

Головним результатом проведеного експерименту є отримання комплексного показника C, який визначає рівень захищеності інформації, що обробляється в інформаційно-комунікаційній системі і є функцією від часткових показників ймовірностей збереження системою захищеного стану, які залежать від реалізації загроз, спрямованих на окремі властивості інформації – конфіденційність, цілісність та доступність. Як випливає з отриманих результатів, показник C залежить від цих окремих властивостей.

Аналізуючи отримані часткові показники захищеності, можна зробити висновок, що недостатній рівень захищеності такої властивості системи, як доступність, дуже істотно впливає на комплексний показник захищеності системи. Зважаючи на це, можна чітко визначити, яка саме властивість інформації потребує підвищення мір захисту та є найбільш критичною для даної системи, що підтверджує клас даної системи згідно з [13].

Ще одним результатом є можливість знаходження ваги k, m, n кожного показника захищеності P_1, P_2, P_3 при розкладі комплексного показника захищеності за базисом:

$$C = kP_1 + mP_2 + nP_3 .$$

Отриманий результат дає можливість коригувати комплексний показник захищеності за рахунок критичності для системи окремих властивостей інформації.

Висновки

Запропонований підхід на основі аналізу існуючих методів дослідження захищеності складних інформаційно-комунікаційних систем відрізняється від існуючого покомпонентним розділенням загроз захищеності системи з подальшою інтеграцією їх у складі єдиного комплексного показника захищеності. Це дає можливість підвищити якість аналізу захищеності системи та зменшити витрати на етапі проектування системи захисту інформації.

Цінність даного дослідження полягає в його спроможності бути використаним для аналізу безпеки структурно складних систем інших класів, що і планується перевірити в подальших дослідженнях.

А.М. Хныгичева, А.Н. Новиков, А.А. Тимошенко

МОДЕЛИРОВАНИЕ БЕЗОПАСНОСТИ СЛОЖНЫХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ЛОГИКО-ВЕРОЯТНОСТНОГО МЕТОДА

Представлен подход к моделированию безопасности сложных информационно-коммуникационных систем, который базируется на использова-

A.M. Khnygicheva, O.M. Novikov, A.O. Tymoshenko

ON MODELING OF COMPLEX INFORMATION AND COMMUNICATIONS SYSTEMS SECURITY USING THE LOGIC-PROBABILITY METHOD

This paper proposes the approach to modeling of complex information and communications systems security based on the logic-probability method. This approach relies on the component-specific division

нии логико-вероятностного метода и отличается покомпонентным разделением угроз безопасности системы с последующей интеграцией их в составе единого комплексного показателя безопасности. Разработанный подход был проверен с помощью вычислительного эксперимента. Полученные результаты подтвердили, что данный подход позволяет упростить процесс формирования модели угроз, а также уменьшить расходы на создание системы защиты информации.

of the system's security threats and their further integration into one complex security indicator. We also conduct the computing experiment to test the elaborated approach. The obtained results show that this approach allows simplifying the threats' model formation as well as reducing expenditures on developing the information security system.

1. *Закон* України "Про основи національної безпеки України" // Відомості Верховної Ради. – 2003. – № 39. – Ст. 351.
2. *Gordon E. Moore*. Cramming More Components Onto Integrated Circuits // Reprinted, with permission, from Electronics. – 1965. – **38**, N 8. – P. 114–117.
3. *FIPS PUB* 146-1, Federal Information Processing Standards Publication (Supersedes FIPS PUB 146-1988, August 24). U.S. Department of Commerce, National Institute of Standards and Technology (USA). April 1991.
4. *ISO/IEC* 7498-1:1994, Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model.
5. *Рябинин И.А.* Научная школа логико-вероятностных методов и концепция логико-вероятностной теории безопасности сложных систем / Под ред. И.А. Рябинина // Теория и информационная технология моделирования безопасности сложных систем / Препринт 101. – СПб.: ИПМАШ РАН, 1994. – Вып. 1. – С. 3–22.
6. *Можаев А.С.* Общий логико-вероятностный метод анализа надежности сложных систем: Учеб. пособ. – Л.: ВМА, 1988. – 68 с.
7. *Solojentsev E.D.* Peculiarities of Logic and Probabilistic Theory with groups of Incompatible Events // Automation and Remote Control. – 2003. – N 7. – P. 187–204.
8. *Bell D.E., La Padula L.J.* Security Computer System: Mathematical Foumdation // Mitre Techical Report 2547. – 1973. – **2**. – 35 p.
9. *Згуровский М.З., Панкратова Н.Д.* Системный анализ (проблемы, методология, приложения). – К.: Наук. думка, 2005. – 744 с.
10. *Панкратова Н.Д.* Системний аналіз в динаміці діагностування складних технічних систем // Системні дослідження та інформаційні технології. – 2008. – № 1. – С. 33–49.
11. *Качинський А.Б.* Засади системного аналізу безпеки складних систем / За заг. ред. В.П. Горбуліна. – К.: НВЦ "Євроатлантикінформ", 2006. – 336 с.
12. *Новіков О.М., Тимошенко А.О.* Побудова логіко-ймовірнісної моделі захищеної комп'ютерної системи // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – Вип. 3. – С. 101–105.
13. *НД ТЗІ* 3.7-003-05: Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Затверджено наказом ДСТСЗІ СБ України від 08.11.2005 р., № 125.
14. *Хофман Л.Дж.* Современные методы защиты информации / Пер. с англ. – М.: Сов. радио, 1980. – 264 с.
15. *Ховард М., Лебланк Д.* Защищенный код / Пер. с англ. – М.: Изд.-торговый дом "Русская редакция", 2003. – 704 с.
16. *Zgurovsky M.Z.* Sustainable development global simulation: Opportunities and treats to the planet // Russ. J. Earth Sci. – 2007. – **9**, N 2. – http://www.agu.org/WPS/rjes/abstract/v09/2007ES000273-abs.html
17. *Саати Т.* Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993. – 320 с.

Рекомендована Радою
Фізико-технічного інституту
НТУУ "КПІ"

Надійшла до редакції
7 липня 2010 року