doi: https://doi.org/10.15407/emodel.42.04.071
УДК 004.056

І.А. Пількевич, д-р техн. наук, **О.С. Бойченко**, канд. техн. наук,
І.В. Гуменюк, канд. техн. наук
Житомирський військовий інститут ім. С.П. Корольова
(Україна, 10004, Житомир, проспект Миру, 22,
тел. +38(067) 3978739, e-mail: igor.pilkevich@meta.ua;
тел. +38(068) 1702502, e-mail: bos_2006@ukr.net;
тел. +38(096) 8706003, e-mail: ig_gum@ukr.net)

Удосконалення методу розробки логіко-ймовірнісної моделі внутрішнього порушника

Проаналізовано сучасні методи розробки моделі внутрішнього порушника. Встановлено, що для отримання кількісних показників ймовірності реалізації загроз інформації в інформаційно-телекомунікаційній системі (ІТС) використовуються методи експертних оцінок та теорії ймовірності, які враховують лише факт виникнення події, а не ймовірність її виникнення. Запропоновано удосконалити метод розробки моделі внутрішнього порушника за допомогою логіко-ймовірнісної функції, яка складається з логічних змін, тобто подій. Апробація розробленого методу засвідчила, що його застосування дозволяє забезпечити підвищення точності оцінювання ймовірності реалізації загроз інформації в ІТС від внутрішнього порушника.

К л ю ч о в і с л о в а: внутрішній порушник, модель порушника, логіко-ймовірнісна модель, захист інформації, політика безпеки інформації.

Інформатизація суспільства, перехід на електронний документообіг усіх державних установ та інших організацій сприяють автоматизації процесу обміну інформацією між відповідними абонентами. З цією метою створюються, вводяться в експлуатацію та використовуються інформаційно-телекомунікаційні системи (ІТС). Однією з основних вимог, що висуваються до ІТС, є захист інформації. Для забезпечення захисту інформації в ІТС створено комплексну систему, призначену для захисту інформації від:

витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

несанкціонованих дій з інформацією, в тому числі з використанням комп'ютерних вірусів;

спеціального впливу на засоби обробки інформації, який здійснюється формуванням фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування [1].

Організація та проведення робіт із захисту інформації в ІТС здійснюється службою захисту інформації, яка забезпечує визначення вимог до захисту інформації в ІТС, проектування, розроблення і модернізацію системи захисту. Визначення вимог до захисту інформації полягає у розробці адекватних моделей загроз інформації в ІТС та порушника політики безпеки інформації в ІТС.

За допомогою моделі порушника політики безпеки інформації в ІТС є можливість у формалізованому вигляді описати дії порушника та визначити перспективні методи і способи захисту інформації в ІТС [2, 3].

Модель порушника політики безпеки інформації визначає:

- можливу мету порушника та її градацію за ступенями небезпечності для ІТС;
- категорії осіб, з числа яких може бути порушник;
- припущення про кваліфікацію порушника;
- припущення про характер його дій [3].

Визначення можливих порушників політики безпеки інформації та ймовірності досягнення їх мети у відповідності до розробленої моделі вимагає проведення наукових досліджень щодо аналізу їх поведінки та прогнозуванню рівня можливих збитків.

Отже, при розробці моделі порушника політики безпеки інформації за допомогою формалізованого опису дій порушника (моделі порушника) постає важливе науково-практичне завдання щодо оцінювання реалізації загроз від внутрішнього порушника з метою зменшення ймовірності реалізації загроз в ІТС. Це науково-практичне завдання обумовлено існуючим об'єктивним протиріччям між високими вимогами до забезпечення захисту інформації в ІТС та принциповою неможливістю мінімальних витрат на її захист з використанням існуючих моделей.

Аналіз літературних даних та постановка проблеми. Захист інформації в ІТС умовно поділяється на захист від зовнішніх та внутрішніх загроз. Захист інформації від зовнішніх загроз має потужний технічний інструментарій, який обґрунтовано науковими дослідженнями у сфері криптографічного та технічного захисту інформації. Захист інформації від внутрішніх загроз полягає в основному у виконанні організаційних заходів, які проводяться під час створення комплексної системи захисту інформації.

При захисті інформації від внутрішніх загроз розробляють модель внутрішнього порушника та модель загроз інформації в ІТС від внутрішнього порушника. Під внутрішнім порушником слід розуміти персонал установи, який може мати доступ до інформаційних ресурсів ІТС. Доступ може бути як санкціонований (користувачі ІТС), так і несанкціонований (технічний, обслуговуючий персонал). При розробці моделі внутрішнього порушника необхідно врахувати ці фактори та провести оцінку ймовірності виникнення загроз інформації в ІТС.

У роботі [4] наведено результати дослідження поведінки людини для можливості передбачення внутрішніх загроз від персоналу установи. Запропоновано враховувати психологічні та соціальні шаблони поведінки порушника політки безпеки інформації в ІТС. Але питанням кількісної оцінки впливу шаблонів на захищеність інформації в ІТС не приділено належної уваги. Результати роботи [5] вказують на необхідність врахування у мотиві поведінки внутрішнього порушника національного контексту. Питанням кількісної оцінки захищеності інформації також не приділено належної уваги. У роботі [6] запропоновано модель девіантної поведінки персонала установи на робочому місці. Застосування цієї моделі дозволяє визначити можливі загрози інформації, але кількісної оцінки ризиків не наведено.

Результатами роботи [7] є модель дослідження активності користувачів у мережі Інтернет та використання сервісу електронної пошти. Модель передбачає визначення розподілу загроз інформації за даними, отриманими під час моделювання активності користувачів. У роботі [8] описано загрози від внутрішніх порушників, які мають високу кваліфікацію та знання про склад ІТС. Для оцінки ризику несанкціонованого доступу до інформації користувачами ІТС у роботі [9] запропоновано програмне забезпечення, яке дозволяє досліджувати поведінку порушників. Модель внутрішнього порушника враховує й мотив поведінки.

У роботі [10] запропоновано метод розрахунку ймовірності реалізації загроз інформації з обмеженим доступом від внутрішнього порушника. Цей метод крім загальноприйнятої класифікації рівнів можливостей, використовуваних методів і способів здійснення дій та місця здійснення дій, враховує мотив неправомірних дій з боку внутрішнього порушника. Також реалізовано оцінку знань внутрішнього порушника щодо можливості реалізації загроз інформації з обмеженим доступом в ІТС.

У роботі [11] запропоновано формалізовану модель порушника, в якій враховується технологія обробки інформації, категорія персоналу та користувачів, кожен з яких має сукупність характеристик: мотив порушення, кваліфікація, можливості, час та місце дії. Ця сукупність характеристик визначає профіль можливостей порушників.

У роботі [12] описано модель імовірних деструктивних дій обслуговуючого персоналу автоматизованої системи управління технологічним процесом за умови наявності зовнішніх та(або) внутрішніх дестабілізуючих впливів. Застосування цієї моделі дозволяє проводити розрахунок імовірності здійснення індивідом (обслуговуючим персоналом) деструктивних дій, спрямованих на порушення інформаційної безпеки.

Результати досліджень, відображені у [4—12], свідчать про те, що ймовірність появи загрози інформації залежить лише від того, відбулась подія чи ні. Математичний апарат, застосований у зазначених наукових працях, оснований лише на статистичних даних і не враховує логічний взаємозв'язок між подіями.

Таким чином, у сучасних методах розробки моделі порушника для отримання кількісних показників ймовірності реалізації загроз інформації в ІТС використовуються лише методи експертних оцінок та теорії ймовірності. Одним із можливих способів отримання більш точних кількісних показників імовірності реалізації загроз інформації в ІТС є застосування логіко-ймовірнісного підходу, теоретичні основи якого наведено у роботі [13].

У роботі [14] застосовано логіко-ймовірнісний аналіз для оцінювання безпеки програмно-апаратних систем та безпеки інформації, а в роботі [15] наведено приклад застосування ймовірнісного підходу для моделювання невизначених логічних аргументів. У [15] показано розподіл ймовірностей на логічні події, тобто ймовірність появи події. У [16] наведено логіку створення переліку атак, які можуть бути реалізовані порушником. Відповідно до цього переліку проведено оцінку можливості здійснення стратегії нападу.

Дослідження, описані у [17], присвячені розробці математичної моделі на основі байєсовської мережі. Ця математична модель застосовується для раннього виявлення внутрішнього порушника інформаційної безпеки в ІТС.

Результати досліджень, наведені у роботах [13–17], свідчать про те, що використанню логіко-ймовірнісного методу для розробки моделі внутрішнього порушника у науковій літературі не приділено належної уваги, що дозволяє зробити висновок про доцільність проведення досліджень, присвячених удосконаленню методу розробки моделі порушника.

Отже, розглянемо удосконалення методу розробки моделі порушника за допомогою застосування логіко-ймовірнісних функцій. Для досягнення мети необхідно виконати такі завдання:

• визначити компетентність внутрішнього порушника за наступними критеріями: рівень можливостей, що надаються порушнику засобами

ІТС, рівень знань порушника про ІТС, методи і способи, що використовуються, місце дій порушника;

• розробити математичну модель розрахунку ймовірності реалізації загроз інформації від внутрішнього порушника в ІТС;

• провести апробацію розробленого методу для формування рейтингового списку співробітників установи, які можуть бути внутрішніми порушниками.

Визначення компетентності внутрішнього порушника. Відповідно до [3] модель порушника це є абстрактний формалізований або неформалізований опис дій, який відображає практичні та теоретичні можливості порушника, його апріорні знання, час та місце дій тощо. Для кожного конкретного випадку розробляється модель порушника, яка повинна бути адекватною реальному порушнику для даної ІТС.

Компетентність внутрішнього порушника визначається за допомогою логічних функцій, які відображають появу відповідної події. Під подією слід розуміти наявність або відсутність практичних та теоретичних можливостей, апріорних знань та місця дій.

Метод розробки логіко-ймовірнісної моделі внутрішнього порушника складається з наступних кроків:

1. Визначення рівня можливостей, що надаються порушнику засобами ІТС. Відповідно до [2] визначено чотири рівні можливостей. При цьому кожний вищий рівень має повний набір можливостей нижчого рівня. Визначення рівня можливостей, що надаються порушнику засобами ІТС, полягає у виникненні хоча б однієї з наступних подій:

l_1 — порушник отримав можливість фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

l_2 — порушник отримав можливість створення і запуску власних програм з новими функціями обробки інформації;

l_3 — порушник отримав можливість управління функціонуванням ІТС, тобто впливу на базове програмне забезпечення системи та на склад і конфігурацію її устаткування;

l_4 — порушник отримав повний обсяг можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення ІТС, аж до включення до складу ІТС власних засобів з новими функціями обробки інформації.

Рівні можливостей у даній ієрархічній класифікації визначаються як виникнення лише події $l_1 : l_1 \vee \overline{l_2} \vee \overline{l_3} \vee \overline{l_4}$, або виникнення події l_2, яка виникає у разі виконання події $l_1 : l_1 \vee l_2 \vee \overline{l_3} \vee \overline{l_4}$, або виникнення події l_3,

яка виникає у разі виконання події l_2, і так далі до виконання всіх подій. Всього таких комбінацій подій може бути п'ять.

2. Визначення рівня знань порушника про ІТС. Відповідно до [2] визначено чотири рівня знань порушника про ІТС. Визначення рівня знань порушника про ІТС полягає у виникненні хоча б однієї з наступних подій:

k_1 — порушник володіє інформацією про функціональні особливості ІТС, основні закономірності формування в ній масивів даних і потоків запитів до них та вміє користуватися штатними засобами ІТС;

k_2 — порушник володіє високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

k_3 — порушник володіє високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації ІТС;

k_4 — порушник володіє інформацією про функції та механізм дії засобів захисту.

Кожному наведеному рівню знань відповідає повна група несумісних подій. Тоді рівень знань порушника про ІТС може бути записаний як комбінація чотирьох несумісних подій. Наприклад запис у вигляді $k_1 \vee k_2 \vee k_3 \vee k_4$ означає, що порушник має знання про ІТС за всіма чотирма рівнями, а запис $k_1 \vee \overline{k_2} \vee \overline{k_3} \vee \overline{k_4}$ означає, що порушник має знання про ІТС лише за першим рівнем. Всього таких комбінацій може бути 16 .

3. Визначення методів і способів порушника, що використовуються. У [2] наведено методи і способи порушника, визначення яких полягає у виникненні хоча б однієї з наступних подій:

m_1 — порушник використовує виключно агентурні методи одержання відомостей;

m_2 — порушник використовує пасивні технічні засоби перехоплення інформаційних сигналів;

m_3 — порушник використовує виключно штатні засоби ІТС або недоліки проектування комплексної системи захисту інформації для реалізації спроб несанкціонованого доступу;

m_4 — порушник використовує засоби активного впливу на ІТС, які змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального програмного забезпечення тощо).

Кожному наведеному засобу порушника відповідає повна група несумісних подій. Тоді методи і способи порушника можуть бути записані як комбінація чотирьох несумісних подій. Наприклад запис у вигляді

$m_1 \vee m_2 \vee m_3 \vee m_4$ означає, що порушник використовує всі можливі методи, а запис $m_1 \vee \overline{m_2} \vee \overline{m_3} \vee \overline{m_4}$ — що порушник використовує лише агентурні методи одержання відомостей. Всього таких комбінацій може бути 16.

4. Визначення місця здійснення дій порушника. Відповідно до [2] наведено можливі місця здійснення дій порушника, визначення яких полягає у виникненні хоча б однієї з наступних подій:

p_1 — порушник здійснює дії без одержання доступу на контрольовану територію ІТС організації;

p_2 — порушник здійснює дії з одержанням доступу на контрольовану територію, але без доступу до технічних засобів ІТС;

p_3 — порушник здійснює дії з одержанням доступу до робочих місць кінцевих (у тому числі віддалених) користувачів ІТС;

p_4 — порушник здійснює дії з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів, автоматизованих робочих місць (АРМ) відповідних адміністраторів тощо);

p_5 — порушник здійснює дії з одержанням доступу до засобів адміністрування ІТС і засобів керування комплексної системи захисту інформації.

Для наведеної класифікації місць здійснення дій порушником існують лише дев'ять наступних комбінацій:

$$p_1 \vee \overline{p_2} \vee \overline{p_3} \vee \overline{p_4} \vee \overline{p_5};\ \overline{p_1} \vee p_2 \vee \overline{p_3} \vee \overline{p_4} \vee \overline{p_5};\ \overline{p_1} \vee \overline{p_2} \vee p_3 \vee \overline{p_4} \vee \overline{p_5};$$

$$\overline{p_1} \vee \overline{p_2} \vee p_3 \vee p_4 \vee \overline{p_5};\ \overline{p_1} \vee \overline{p_2} \vee p_3 \vee \overline{p_4} \vee p_5;\ \overline{p_1} \vee \overline{p_2} \vee p_3 \vee p_4 \vee p_5;$$

$$\overline{p_1} \vee \overline{p_2} \vee \overline{p_3} \vee p_4 \vee p_5;\ \overline{p_1} \vee \overline{p_2} \vee \overline{p_3} \vee p_4 \vee \overline{p_5};\ \overline{p_1} \vee \overline{p_2} \vee \overline{p_3} \vee \overline{p_4} \vee p_5.$$

Математична модель розрахунку ймовірності реалізації загроз інформації від внутрішнього порушника в ІТС. Модель порушника подамо за допомогою логічної функції, яка складається з логічних змін, тобто подій, описаних на попередніх етапах:

$$V = \sum_{i=1}^{N} \vee\, l_i \vee \sum_{j=1}^{S} \vee\, k_j \vee \sum_{x=1}^{D} \vee\, m_x \vee \sum_{y=1}^{Z} \vee\, p_y\,, \qquad (1)$$

де N — кількість рівнів можливостей, що надаються порушнику засобами ІТС; S — кількість рівнів знань порушника про ІТС; D — кількість методів і способів порушника; Z — кількість можливих місць здійснення дій порушника.

Розрахунок ймовірності реалізації загроз інформації в ІТС дорівнює відношенню суми кількості подій, які виникають при дії порушника, до загальної кількості подій, що можуть виникнути:

$$p_з = \frac{L + K + M + P}{N + S + D + Z}, \tag{2}$$

де L — кількість подій, при яких $l_i = 1$; K — кількість подій, при яких $k_i = 1$; M — кількість подій, при яких $m_i = 1$; P — кількість подій, при яких $p_i = 1$.

Для отримання арифметичного поліному ймовірнісної функції реалізації загроз інформації в ІТС до логічної функції (1) застосовано наступне відоме співвідношення:

$$A_1 \vee A_2 = A_1 + A_2 - A_1 A_2.$$

Враховуючи це співвідношення та логічну функцію (1), отримуємо ймовірнісну функцію

$$F(V) =$$

$$= \sum_{i=1}^{N}\sum_{j=1}^{S}\sum_{x=1}^{D}\sum_{y=1}^{Z}\begin{pmatrix} p_{l_i} + p_{k_j} + p_{m_x} + p_{p_y} - p_{l_i}p_{k_j} - p_{l_i}p_{m_x} - p_{l_i}p_{p_y} - p_{k_j}p_{m_x} - \\ - p_{k_j}p_{p_y} - p_{m_x}p_{p_y} + p_{l_i}p_{k_j}p_{m_x} + p_{l_i}p_{k_j}p_{p_y} + p_{l_i}p_{m_x}p_{p_y} + \\ + p_{k_j}p_{m_x}p_{p_y} - p_{l_i}p_{k_j}p_{m_x}p_{p_y} \end{pmatrix}, \tag{3}$$

де p_{li} — ймовірність виникнення події при визначенні рівня можливостей, що надаються порушнику засобами ІТС; p_{kj} — ймовірність виникнення події при визначенні рівня знань порушника про ІТС; p_{mx} — ймовірність виникнення події при визначенні використовуваних методів і способів порушника; p_{py} — ймовірність виникнення події при визначенні місця здійснення дій порушника.

Імовірність реалізації загроз інформації в ІТС з урахуванням виразу (3) має вигляд

$$p_з = \frac{\sum_{i=1}^{N}\sum_{j=1}^{S}\sum_{x=1}^{D}\sum_{y=1}^{Z}\begin{pmatrix} p_{l_i} + p_{k_j} + p_{m_x} + p_{p_y} - p_{l_i}p_{k_j} - p_{l_i}p_{m_x} - p_{l_i}p_{p_y} - \\ - p_{k_j}p_{m_x} - p_{k_j}p_{p_y} - p_{m_x}p_{p_y} + p_{l_i}p_{k_j}p_{m_x} + \\ + p_{l_i}p_{k_j}p_{p_y} + p_{l_i}p_{m_x}p_{p_y} + p_{k_j}p_{m_x}p_{p_y} - p_{l_i}p_{k_j}p_{m_x}p_{p_y} \end{pmatrix}}{N + S + D + Z}. \tag{4}$$

Отриманий арифметичний поліном ймовірнісної функції реалізації загроз інформації в ІТС характеризує не тільки факт появи подій, але й імовірності їх виникнення.

Апробація методу побудови логіко-ймовірнісної моделі внутрішнього порушника здійснювалася за допомогою побудови логіко-ймовірнісної моделі для внутрішніх порушників, які є співробітниками установи:

1. Користувачі ІТС.

1.1. Адміністратор безпеки.

1.2. Адміністратор обчислювальної мережі.

1.3. Системний адміністратор.

1.4. Адміністратори баз даних.

1.5. Оператори АРМ.

1.6. Керівники структурних підрозділів.

1.7. Інші співробітники установи.

2. Співробітники установи:

2.1. Технічні співробітники, які забезпечують експлуатацію ІТС (технік-монтажник, інженер з телекомунікацій, електрик та ін.).

2.2. Технічні співробітники (прибиральниці, сантехніки та ін.).

2.3. Інші співробітники установи (кухар, медична сестра та ін.).

Метою внутрішнього порушника є реалізація загроз інформації в ІТС (витік інформації, несанкціонований доступ до інформації, несанкціонована модифікація інформації). У табл. 1 наведено параметри моделі внутрішнього порушника, які є логічними змінними у логічній функції (1).

Відповідно до даних, наведених у табл. 1, логічна функція для адміністратора безпеки матиме наступний вигляд:

$$V = (l_1 \vee l_2 \vee l_3 \vee l_4) \vee (k_1 \vee k_2 \vee k_3 \vee k_4) \vee$$
$$\vee (\overline{m}_1 \vee \overline{m}_2 \vee m_3 \vee m_4) \vee (\overline{p}_1 \vee \overline{p}_2 \vee p_3 \vee p_4 \vee p_5).$$

Розраховану ймовірність реалізації загроз інформації в ІТС за виразом (2) наведено у табл. 2.

Для розрахунку ймовірності реалізації загроз інформації в ІТС за виразом (4) спочатку необхідно визначити будь-яким відомим методом ймовірності виникнення подій p_{li}, p_{kj}, p_{mx}, p_{py} як вхідних параметрів. Потім сформувати таблицю, аналогічну за структурою до табл. 1, в якій замість подій записати ймовірності їх виникнення.

Значення ймовірності реалізації загроз інформації в ІТС, наведені в табл. 2, близькі до одиниці. Це свідчить про те, що удосконалений метод має більшу точність визначення ймовірності реалізації загроз інформації в ІТС у порівнянні з методом, який використано в моделі порушника на основі логічної функції. Результати розрахунку ймовірності реалізації загроз інформації в ІТС (див. табл. 1) свідчать про те, що співробітники

Таблиця 1

Внутрішній порушник	Кількість подій, які виникають внаслідок дій порушника																	Ймовірність реалізації загроз
	l_1	l_2	l_3	l_4	k_1	k_2	k_3	k_4	m_1	m_2	m_3	m_4	p_1	p_2	p_3	p_4	p_5	
1. Користувачі ІТС																		
1.1	1	1	1	1	1	1	1	1	0	0	1	1	0	0	1	1	1	0,765
1.2	1	1	1	1	1	1	1	1	0	0	1	1	0	0	1	1	0	0,706
1.3	1	1	1	1	1	1	1	1	0	0	1	0	0	0	1	1	0	0,647
1.4	1	1	1	1	1	1	1	0	0	0	1	0	0	0	1	1	0	0,588
1.5	1	0	0	0	1	1	0	0	0	0	1	0	0	0	1	1	0	0,353
1.6	1	0	0	0	1	0	0	0	0	0	1	0	0	0	1	0	0	0,235
1.7	1	0	0	0	1	0	0	0	0	0	1	0	0	0	1	0	0	0,235
2. Співробітники установи																		
2.1	0	0	0	0	1	0	0	0	1	1	0	0	0	1	0	0	0	0,294
2.2	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	0	0,177
2.3	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	0	0	0,177

Таблиця 2

Внутрішній порушник	Ймовірність виникнення подій																	Ймовірність реалізації загроз
	p_{l_1}	p_{l_2}	p_{l_3}	p_{l_4}	p_{k_1}	p_{k_2}	p_{k_3}	p_{k_4}	p_{m_1}	p_{m_2}	p_{m_3}	p_{m_4}	p_{p_1}	p_{p_2}	p_{p_3}	p_{p_4}	p_{p_5}	
1. Користувачі ІТС																		
1.1	0,9	0,8	0,7	0,7	0,9	0,8	0,7	0,7	0	0	0,5	0,8	0	0	0,9	0,9	0,7	0,99999
1.2	0,9	0,8	0,7	0,5	0,9	0,8	0,7	0,5	0	0	0,5	0,5	0	0	0,9	0,9	0	0,99999
1.3	0,9	0,8	0,7	0,4	0,9	0,8	0,7	0,5	0	0	0,5	0,5	0	0	0,9	0,9	0	0,99999
1.4	0,9	0,8	0,6	0,3	0,9	0,8	0,7	0,4	0	0	0,5	0,5	0	0	0,9	0,8	0	0,99999
1.5	0,9	0	0	0	0,9	0,8	0	0	0	0	0,5	0,3	0	0	0,9	0,4	0	0,99996
1.6	0,9	0	0	0	0,9	0	0	0	0	0	0,8	0	0	0	0,9	0	0	0,9998
1.7	0,9	0	0	0	0,9	0	0	0	0	0	0,8	0	0	0	0,9	0	0	0,9998
2. Співробітники установи																		
2.1	0	0	0	0	0,5	0	0	0	0,5	0,7	0	0	0	0,8	0	0	0	0,985
2.2	0	0	0	0	0	0	0	0	0,5	0,5	0	0	0	0,7	0	0	0	0,925
2.3	0	0	0	0	0	0	0	0	0,5	0,5	0	0	0,5	0	0	0	0	0,875

установи не розглядались як можливі внутрішні порушники політики безпеки інформації в ІТС. Вважалось що вони не мають можливості здійснити:

несанкціоноване ознайомлення з інформацією на робочому місці користувача ІТС;

закладку пасивних технічних засобів перехоплення інформаційних сигналів;

активний вплив на ІТС, що змінить її конфігурацію.

Застосування моделі внутрішнього порушника дозволить враховувати загрози, що можуть виникнути від співробітників установи, які не розглядаються як потенційно можливі порушники. До таких порушників відносяться співробітники установи, які

не мають можливостей, що надаються засобами ІТС;

не мають знань про структуру та порядок роботи ІТС;

мають доступ на контрольовану територію, де розміщуються засоби ІТС;

мають можливість використовувати засоби активного впливу на ІТС.

Недоліком розробленого методу є використання числових значень ймовірності виникнення подій, отриманих від експертів.

Подальші наукові дослідження будуть спрямовані на розробку математичної моделі оцінювання компетентності внутрішнього порушника з використанням методів теорії тестів.

Висновки

Застосування до логічної функції, яка описує модель поведінки внутрішнього порушника, відомого співвідношення дозволило отримати арифметичний поліном імовірнісної функції реалізації загроз інформації в ІТС. За допомогою цього полінома отримано вираз для розрахунку ймовірності реалізації загроз інформації в ІТС.

Результати апробації методу розробки логіко-ймовірнісної моделі внутрішнього порушника свідчать про те, що при застосуванні розробленого методу підвищується точність оцінювання ймовірності реалізації загроз інформації в ІТС від внутрішнього порушника.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Postanova* Kabinetu ministriv Ukrayiny № 373 vid 29.03.2006 “Pro zatverdzhennya pravyl zabezpechennya zakhystu informatsiyi v informatsiynykh, telekomunikatsiynykh ta informatsino-telekomunikatsiynykh systemakh”. [Elektronnyy resurs] Rezhym dostupu: http://www.zakon.rada.gov.ua/laws/show/373-2006-p. Data zvernennya: 28 travnya, 2020.
2. *Наказ* Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України № 215 від 25.11.2015 “Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-05”. [Електронний ресурс] Режим доступу: http://www. dsszzi.gov.ua/control/uk/publish/article?art_id=46074. Дата звернення: 28 травня, 2020.
3. *Наказ* Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України № 53 від 04.12.2000 “Типове положення про службу захисту інформації в автоматизованій системі. НД ТЗІ 1.4-001-2000”. [Електронний ресурс] Режим доступу: http://www.tzi.com.ua/downloads/1.4-001-2000.pdf. Дата звернення: 28 травня, 2020.
4. *Greitzer F.L., Hohimer R.E.* Modeling Human Behavior to Anticipate Insider Attacks // Journal of Strategic Security, 2011, Vol. 4, № 2, p. 25–48. Doi: http://dx.doi.org/10.5038/1944-0472.4.2.2.
5. *Frącik K.* Insider attacks as one of the main threats to resolute support personnel in Afghanistan // Security and Defence Quarterly, 2016, 12(3), p 3–18. Doi: https://doi.org/10.35467/sdq/103234.
6. *Green D.* Insider threats and employee deviance: developing an updated typology of deviant workplace behaviors // Issues in Information Systems, 2014, 15 (2), p. 185–189.
7. *Kim Park, Kim Cho, & Kang.* Insider Threat Detection Based on User Behavior Modeling and Anomaly Detection Algorithms // Applied Sciences, 2019, 9(19), 4018. Doi: https://doi.org/10.3390/app9194018.
8. *Teng Hu, Weina Niu, Xiaosong Zhang et al.* An Insider Threat Detection Approach Based on Mouse Dynamics and Deep Learning // Security and Communication Networks, 2019, Vol. 2019, Article ID 3898951. Doi: https://doi.org/10.1155/2019/3898951.
9. *Бойченко О.С., Гуменюк І.В., Гладич Р.І.* Математична модель оцінки ризику несанкціонованого доступу до інформації користувачами інформаційно-телекомунікаційної системи // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: Зб. наук. праць, 2019, № 16, с. 124–135.
10. *Бойченко О.С., Зюбіна Р.В.* Метод розрахунку ймовірності реалізації загроз інформації з обмеженим доступом від внутрішнього порушника // Безпека інформаційних систем та технологій, 2019, № 1(1), с 19–26. Doi: https://doi.org/10.17721/ISTS.2019.1.19-26.
11. *Комаров М.Ю., Ониськова А.В., Гончар С.Ф.* Аналіз і дослідження моделі порушника безпеки інформації для захищеного вузла інтернет доступу // Вчені записки ТНУ ім. В.І. Вернадського. Серія: Технічні науки, 2018, **29** (68), ч. 1 №5, с. 138–142.
12. *Гончар С.Ф.* Аналіз ймовірності реалізації загроз захисту інформації в автоматизованих системах управління технологічним процесом // Захист інформації, 2014, **16**, № 1, с. 40–46.
13. *Рябинин И.А.* Надежность и безопасность структурно-сложных систем. Второе изд. СПб.: Изд-во СПбГУ, 2007, 276 с.
14. *Зеленов С.В., Зеленова С.А.* Моделирование программно-аппаратных систем и анализ их безопасности // Труды Института системного программирования РАН, 2017, № 5, с. 257–282. Doi: https://doi.org/10.15514/ISPRAS-2017-29(5)-13.

15. *Hunter A.* A probabilistic approach to modelling uncertain logical arguments // International Journal of Approximate Reasoning, 2013, № 1 (54), p. 47–81. Doi: https://doi.org/10.1016/j.ijar.2012.08.003.
16. *Лукинова О.В.* Компьютерное формирование целей и стратегий нарушителя безопасности информационной системы // Открытое образование, 2013, № 4(99), с. 83–90. Doi: https://doi.org/10.21686/1818-4243-2013-4(99)-83-90.
17. *Михалькова А.П., Зайцев А.С.* Применение байесовского подхода для раннего обнаружения внутренних нарушителей информационной безопасности // Безопасность информационных технологий, 2013, № 3, с. 103–108.

Отримано 17.06.20

REFERENCES

1. Kabinet ministriv Ukrayiny. (2006), Resolution No.373, “Pro zatverdzhennya pravyl zabezpechennya zakhystu informatsiyi v informatsiynykh, telekomunikatsiynykh ta informatsino-telekomunikatsiynykh systemakh”, available at: http://www.zakon.rada.gov.ua/laws/show/373-2006-p (accessed August 3, 2020).
2. Department of Special Telecommunication Systems and Information Protection. Security Service of Ukraine. (2015), Order No.215, “The procedure for creating a comprehensive information protection system in the information and telecommunications system. Sun TZI 3.7-003-05”.
3. Nakaz Departamentu spetsialnykh telekomunikatsiynykh system ta zakhystu informatsiyi Sluzhby bezpeky Ukrayiny № 53 vid 04.12.2000 “Typove polozhennya pro sluzhbu zakhystu informatsiyi v avtomatyzovaniy systemi. ND TZI 1.4-001-2000”. [Elektronnyy resurs] Rezhym dostupu: http://www.tzi.com.ua/downloads/1.4-001-2000.pdf. Data zvernennya: 28 travnya, 2020.
4. Greitzer, F.L. and Hohimer, R.E. (2011), “Modeling Human Behavior to Anticipate Insider Attacks”, *Journal of Strategic Security*, Vol. 4, no. 2, pp. 25-48. DOI: http://dx.doi.org/10.5038/1944-0472.4.2.2.
5. Frącik, K. (2016), “Insider attacks as one of the main threats to resolute support personnel in Afghanistan”, *Security and Defence Quarterly*, Vol. 12, no. 3, pp. 3-18. DOI: https://doi.org/10.35467/sdq/103234.
6. Green, D. (2014), “Insider threats and employee deviance: developing an updated typology of deviant workplace behaviors”, *Issues in Information Systems*, Vol. 15, no. 2, pp. 185-189.
7. Kim, P., Kim, C. and Kim, K. (2019), “Insider Threat Detection Based on User Behavior Modeling and Anomaly Detection Algorithms”, *Applied Sciences*, Vol. 9, no. 19. DOI: https:// doi.org/10.3390/app9194018.
8. Teng, H., Weina, N., Xiaosong, Z., Xiaolei, L., Jiazhong, L. and Yuan, L. (2019), “An Insider Threat Detection Approach Based on Mouse Dynamics and Deep Learning”, *Security and Communication Networks*, Vol. 2019. DOI: https://doi.org/ 10.1155/2019/3898951.
9. Boychenko, O.S., Humenyuk, I.V. and Hladych, R.I. (2019), “Mathematical model for risk assessment of unauthorized access to information by users of information and telecommunication system”, *Problemy stvorennya, vyprobuvannya, zastosuvannya ta ekspluatatsiyi skladnykh informatsiynykh system: zbirnyk naukovykh prats'*, no. 16, pp. 124-135.
10. Boychenko, O.S. and Zyubina, R.V. (2019), “Method of calculating the probability of realization of threats of information with limited access from an internal violator”, *Bezpeka informatsiynykh system ta tekhnolohiy*, Vol. 1, no. 1, pp. 19-26. DOI: https://doi.org/10.17721/ISTS.2019.1.19-26.
11. Komarov, M.Yu., Onys′kova, A.V. and Honchar, S.F. (2018), “Analysis and research of the information security violator model for a secure Internet access node”, *Vcheni zapysky*

TNU imeni V.I. Vernads'koho. Seriya: tekhnichni nauky, Vol. 29, no. 68, pp. 138-142, available at: http://www.tech.vernadskyjournals.in.ua/journals/2018/5_2018/ part_1/26.pdf (accessed August 3, 2020).
12. Honchar, S.F. (2014), *"*Analysis of the probability of realization of information security threats in automated process control systems", *Zakhyst informatsiyi*, Vol. 16, no. 1, pp. 40-46.
13. Ryabinin, I.A. (2007), *Nadezhnost' i bezopasnost' strukturno-slozhnykh sistem. 2-ye izd* [Reliability and safety of structurally complex systems. Second ed], Izd-vo SPbGU.
14. Zelenov S.V. and Zelenova S.A. (2017), "Modeling of software and hardware systems and analysis of their security", *Trudy Instituta sistemnogo programmirovaniya RAN*, no. 5, pp. 257-282. DOI: https://doi.org/10.15514/ISPRAS-2017-29(5)-13.
15. Hunter, A. (2013), "A probabilistic approach to modelling uncertain logical arguments", *International Journal of Approximate Reasoning*, Vol. 1, no. 54, pp. 47-81. DOI: https://doi.org/ 10.1016/j.ijar.2012.08.003.
16. Lukinova, O.V. (2013), "Computer formation of goals and strategies of an information system security intruder", *Otkrytoye obrazovaniye*, Vol. 4, no. 99, pp. 83-90.
17. Mikhal'kova, A.P. and Zaytsev, A.S. (2013), "Applying a Bayesian Approach to Early Detection of Internal Information Security Offenders", *Bezopasnost' informatsionnykh tekhnologiy*, no. 3, pp. 103-108.

Received 17.06.20

И.А. Пилькевич, А.С. Бойченко, И.В. Гуменюк

УСОВЕРШЕНСТВОВАНИЕ МЕТОДА РАЗРАБОТКИ
ЛОГИКО-ВЕРОЯТНОСТНОЙ МОДЕЛИ ВНУТРЕННЕГО НАРУШИТЕЛЯ

Проанализированы современные методы разработки модели внутреннего нарушителя. Установлено, что для получения количественных показателей вероятности реализации угроз информации в информационно-телекоммуникационной системе (ИТС) используются методы экспертных оценок и теории вероятности, учитывающие только факт возникновения события, а не вероятность ее возникновения. Предложено усовершенствовать метод разработки модели внутреннего нарушителя с помощью логико-вероятностной функции, которая состоит из логических переменных, т.е. событий. Апробация разработанного метода свидетельствует о том, что его применение позволяет обеспечить повышение точности оценивания вероятности реализации угроз информации в ИТС от внутреннего нарушителя.

К л ю ч е в ы е с л о в а: внутренний нарушитель, модель нарушителя, логико-вероятностная модель, защита информации, политика безопасности информации.

I.A. Pilkevych, O.S. Boychenko, I.V. Humeniuk

IMPROVIMG THE METHOD OF DEVELOPING A
LOGIC-PROBABILISTIC MODEL OF AN INTERNAL VIOLATOR

The modern approaches to the development of a model of an internal violator are analyzed. It is established that to obtain quantitative indicators of the probability of the implementation of information threats in the information and telecommunication system, methods of expert estimates and probability theory are used that take into account only the fact of the occurrence of the event, and not the probability of its occurrence. It is proposed to improve the method of developing an internal violator model by creating an internal violator model using a logical-

probabilistic function, which consists of logical variables-events. Testing of the developed method showed that its application allows to increase the accuracy of assessing the probability of the implementation of information threats in the information and telecommunication system from an internal violator.

K e y w o r d s: internal violator, violator model, logical-probabilistic model, information protection, information security policy.

ПІЛЬКЕВИЧ Ігор Анатолійович, д-р техн. наук, професор, професор кафедри комп'ютерних інформаційних технологій Житомирського військового інституту ім. С.П. Корольова. У 1982 р. закінчив Житомирське військове училище радіоелектроніки ППО. Область наукових досліджень — математичне моделювання складних систем, інформаційна безпека.

БОЙЧЕНКО Олег Сергійович, канд. техн. наук, начальник науково-дослідної лабораторії наукового центру Житомирського військового інституту ім. С.П. Корольова, який закінчив у 2004 р. Область наукових досліджень — захист інформації, моделювання інформаційно-телекомунікаційних систем.

ГУМЕНЮК Ігор Володимирович, канд. техн. наук, ст. викладач кафедри захисту інформації та кібербезпеки Житомирського військового інституту ім. С.П. Корольова. У 2010 р. закінчив Житомирський військовий інститут Національного авіаційного університету. Область наукових досліджень — захист інформації, моделювання інформаційно-комунікаційних систем.