УДК 004.942

В.В. Глушак, О.М. Новіков

МЕТОД ПРОЕКТУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ДЕТЕРМІНОВАНОЇ ГРИ "ЗАХИСНИК–ЗЛОВМИСНИК"

This study describes the approach to solving the problem of creating a system of information protection with limited resources. The problem is solved using the game theory, notably a formal apparatus which allows taking into account the conflict relationships between an attacker and a defender. In terms of the game theory, the attacker's reward is the damage inflicted on the victim, while the defender aims to minimize the risk and ensure the stable system operation. Solving the described problem, we obtain the optimal set of security measures that provides the maximum level of protection under the given constraints.

Вступ

У процесі проектування системи захисту інформації (СЗІ) особлива увага приділяється розробленню політики безпеки [1]. Це зумовлюється тим, що від коректності формування вимог, правил, обмежень і рекомендацій з обробки інформації залежить ефективність розроблення та функціонування інформаційної системи в цілому. Вхідними даними для формування політики безпеки є модель зловмисника та загроз, особливості обчислювального середовища, технологія обробки інформації й інші чинники. Розроблення політики безпеки передбачає ретельний аналіз вказаних вхідних даних для формування порядку та правил обробки інформації.

На підставі цих даних систему обробки інформації розділяють на компоненти (вузли), для яких доцільно розробляти свої власні політики безпеки. Для кожного компонента формується необхідний набір механізмів (послуг) захисту від несприятливих дій зловмисника [2]. Завдання проектування системи захисту інформації зводиться до вибору функціонального профілю захищеності (оптимальної структури механізмів захисту) з множини доступних. Використання стандартних функціональних профілів для реалізації вимог із захисту інформації рекомендують в нормативних документах України, де їх пропонується ціла низка [3].

Зазвичай проектування системи захисту інформації здійснюється з використанням емпіричного підходу методом спроб і помилок або формальних математичних методів. При цьому через недоліки емпіричного підходу, навіть за участі досвідченого проектувальника, міцність спроектованої системи захисту буває або недостатньою, або такою, що перевищує необхідний рівень вимог. Використання методів формального математичного апарату через формалізацію процедури проектування дає можливість зменшити вказані недоліки. Разом з тим рівень формальних методів проектування систем захисту на сьогодні недостатній і потребує подальшого розвитку.

Під час проектування інформаційних систем, в тому числі систем захисту інформації, використовується низка формальних методів, серед яких можна зазначити такі: методи математичного програмування, теорія ігор, методи системного аналізу тощо [4–6]. Процедура розв'язання задач проектування базується на використанні формальних моделей предметної галузі, таких як моделі теорії надійності, нечіткої логіки, ймовірнісні та статистичні моделі, імітаційне моделювання тощо [7–9].

При зіткненні інтересів сторін за відсутності інформації про поведінку зловмисника математичні методи оптимізації для проектування систем захисту втрачають свою ефективність [10]. У цьому випадку активно використовуються методи управління конфліктними ситуаціями на основі теорії ігор. Залежно від особливостей конфліктних ситуацій в теорії ігор розглядаються різні класи задач, в тому числі ігри двох осіб з нульовою сумою, ігри з досконалою інформацією, ігри з лідером та веденим, оптимальність за Парето, рівновага за Нешем, ієрархічний розв'язок тощо [11].

У практиці побудови захищених інформаційних систем є низка актуальних задач, в яких зловмисник і захисник знають доступні стратегії поведінки один одного. Наприклад, при використанні певної операційної системи є ряд відомих вразливостей та підходів до їх використання, які відомі як захиснику, так і зловмиснику. Ще одним важливим прикладом є задача, за умовою якої зловмиснику вже відомо або він може дізнатися про застосовані заходи та за-

соби захисту. Наприклад, спостерігаючи за роботою невідомої системи, зловмисник може виявити встановлені механізми захисту й вибрати стратегію нападу таким чином, щоб уникнути їх.

Наведені приклади задач можуть бути формалізовані як клас задач теорії ігор, а саме гра лідера та веденого з прозорою інформацією. Г. фон Штакельберг запропонував метод розв'язання таких задач та першим виділив їх як самостійний клас [11].

Зазначений клас задач застосовується при плануванні захисту функціонування критичної інфраструктури, зокрема в електричних і трубопровідних мережах, метрополітенах, аеропортах тощо [8, 12–14]. Використання теорії ігор для вирішення задач планування захищених інформаційних систем є актуальним.

Постановка задачі

Мета – розробити підхід для проектування захищених інформаційних систем, який базується на методі теорії ігор з двома сторонами "зловмисник–захисник" (за умови прозорості інформації між цими сторонами) і відрізняється можливістю передбачати негативні дії зловмисника та вибирати необхідні механізми захисту.

Поставлено такі завдання:

- вибрати й обгрунтувати модель "захисник–зловмисник" для системи обробки інформації, яка вразлива до негативного впливу зловмисника. Перший етап передбачає формалізацію взаємовідносин між зловмисником і захисником в інформаційній системі та формулювання платіжної функції. Формалізація відносин реалізується завдяки розробленню економічної моделі системи в контексті теорії ігор, що оперує фінансовими надходженнями від функціонування системи та втратами внаслідок негативних дій зловмисника. Основними параметрами моделі є цінність елементів системи для її власника та вартість застосування заходів захисту до елементів системи. Цінність компонента системи відображає економічну вигоду від функціонування вузла в інформаційній системі. Використовуючи знання про інформаційну систему, що потребує захисту, аналізується список загроз та визначаються можливі стратегії нападу;
- синтезувати структуру системи захисту, тобто знайти екстремум цільової функції, а саме оптимальний набір профілів захищеності для автоматизованої системи. Пошук оптимального значення критерію виконується через застосування математичних методів оптимізації до моделі "захисник–зловмисник", розробленої на першому етапі.

Визначення та формалізація об'єкта дослідження

Як об'єкт дослідження розглядається розподілена інформаційна система S, яка використовується уповноваженими користувачами в межах їх привілеїв. Інформаційно-телекомунікаційна система складається з набору вузлів $j \in S$, що беруть участь в обробці інформації. Кожен вузол (компонент) характеризується унікальним набором параметрів, серед яких операційне середовище, технології обробки інформації, інтенсивність використання і т.д. Вказані характеристики вузлів становлять їх цінність для системи в цілому, яка буде позначатися через C_j. Для кількісного розрахунку цінність системи можна розглядати як сукупність власної вартості вузла, складності відновлення після атаки зловмисника та критичності для виконання системою своєї функції з обробки інформації.

Цінність компонентів системи є основним вхідним параметром для моделі захисник–зловмисник. Аналіз і точний розрахунок цінності кожного з вузлів для функціонування системи гарантує коректність вирішення завдання розподілу ресурсів на побудову системи захисту в цілому. Завищена цінність вузла призведе до встановлення додаткових, практично не потрібних, засобів захисту цього вузла, які могли бути використані ефективніше в іншому місці. В той же час недооцінений вузол залишиться без критично важливих механізмів захисту інформації, а тому буде вразливим до атак зловмисника.

За відсутності достатніх статистичних даних цінність вузла може розраховуватися з використанням методів експертної оцінки. Для коректного розрахунку цінності знадобляться емпіричні знання операторів, адміністраторів, власників, користувачів та інших знавців системи про принципи й особливості роботи системи та її компонентів. Ефективно розрахувати цінність компонентів системи на основі експертних оцінок можна за допомогою методу аналізу ієрархій (MAI) з використанням зазначених вище критеріїв [9].

Формалізація взаємовідносин зловмисника та захисника

Залежно від вразливостей компонентів системи, а також можливих загроз зі сторони зловмисника, засоби та заходи захисту можуть бути розподілені між компонентами в різний спосіб. Конфліктну ситуацію, яка виникає між сторонами, можна описати з використанням теорії ігор, причому розподілом механізмів захисту є стратегії захисника в грі "захисник–зловмисник". Гра захисника направлена на реалізацію захищеного середовища з протидії зловмиснику, метою якого є завдання максимального збитку.

Створення захищеного обчислювального середовища реалізується через вибір механізмів захисту для побудови комплексної системи захисту інформації. Разом з тим формально гарантувати безпеку інформаційної системи неможливо, оскільки згідно з теоремою М. Харрісона, В. Руззо, Дж. Ульмана не можна розв'язати задачу забезпечення безпеки довільної системи з відкритою архітектурою [1]. Для вирішення проблеми гарантування необхідного рівня безпеки будемо спиратися на стандартні функціональні профілі захищеності як основні рішення із забезпечення захисту, запропоновані в [3]. Профілі захищеності являють собою перелік мінімально необхідних рівнів послуг (механізмів захисту), які необхідно реалізувати в обчислювальній системі, щоб задовольнити вимоги із захищеності інформації, яка обробляється у конкретній інформаційно-телекомунікаційній системі [3].

Таким чином, завдання захисника цієї системи зводиться до вибору функціональних профілів захищеності $p \in P$, $P = \{p_1, \ldots, p_m\}$ для кожного компонента системи, які сприятимуть мінімізації збитків від можливих дій зловмисника при існуючих загрозах та обмеженнях на реалізацію системи захисту. У зв'язку з тим, що ідеальну систему захисту побудувати неможливо, завжди залишається певна ймовірність реалізації несприятливої дії зловмисником [1].

Якісно обчислити ймовірність несприятливої події і можливий збиток від такої дії зловмисника можна завдяки аналізу ризиків. В інформаційній безпеці ризик R визначається як функція двох змінних: ймовірності існування загрози T та потенційного збитку Q. Для відображення впливу стратегій захисника на ризик в системі введемо додаткову змінну, яка буде характеризувати здатність системи захисту протистояти атаці V. Таким чином, $(1-V)$ можна інтерпретувати як існування незахищеної вразливості, яка може бути використана зловмисником. Тоді співвідношення ризику інформаційної безпеки набуде такого вигляду:

$$R = T\,Q\,(1 - V). \qquad (1)$$

Розглянемо кожну зі змінних, що бере участь у розрахунку ризику (1).

Сучасні апаратні та програмні засоби, які використовуються в інформаційних системах, з точки зору безпеки недосконалі, а тому вразливі до загроз зловмисника. Вразливість компонента системи до тієї чи іншої загрози залежить від технологій, апаратних і програмних засобів, що використовуються в ньому. Позначимо множину загроз, які можуть бути реалізовані в системі та нанести їй збиток через $a \in A$, $A = \{a_1, \ldots, a_n\}$. Список можливих загроз складається на основі існуючих вразливостей, які можуть бути використані зловмисниками різних типів (як зовнішніми, так і внутрішніми), з різними повноваженнями (від користувачів до адміністраторів), різним рівнем підготовки в сфері захисту інформації, різними теоретичними знаннями та практичними можливостями.

Кількісною оцінкою ризику є збиток Q, виражений у вигляді втрат і неотриманої вигоди. Таким чином, максимальним значенням збитку Q, спричиненого певному компоненту i системи, є значення цінності C_i цього компонента для функціонування системи в цілому. Надалі будемо використовувати саме розраховані значення цінності, маючи при цьому на увазі заподіяний збиток.

Як вже зазначалось, подолання потенційних атак буде здійснюватися з використанням функціональних профілів захищеності p. Кожен з профілів може подолати одну або більше загроз a із множини A. Тобто можна ввести матрицю захищеності $D = \{d_{ap}\}$, яка характеризує здатність певного профілю p протидіяти потенційній атаці a. Визначимо d_{ap} так:

$$d_{ap} = \begin{cases} 1, \text{ якщо профіль захищеності } p \text{ здатний} \\ \text{протидіяти атаці } a, \\ 0, \text{ в іншому випадку.} \end{cases}$$

Беручи до уваги профілі захищеності з різними рівнями гарантій елементи матриці D відображатимуть ймовірність нейтралізації загро-

зи вибраним профілем захищеності та набуватимуть значень від 0 до 1.

Стратегії вибору зловмисника включають можливість, використовуючи атаки із множини $a \in A$, завдати збитків одному із компонентів системи $i \in S$. Стратегії зловмисника можна подати у вигляді матриці $Y \in \{y_{ai}\}$, елементи якої набувають таких значень:

$$y_{ai} = \begin{cases} 1, \text{ якщо атака типу } a \text{ направлена проти} \\ \text{вузла } i, \\ 0, \text{ в іншому випадку.} \end{cases}$$

У системі існує певна статистична невизначеність, тобто відомо деякі ймовірності вибору захисником своїх стратегій. Позначимо ймовірність реалізації загрози a в компоненті i через h_{ai}.

Беручи до уваги той факт, що зловмисник намагається завдати максимальних втрат системі, його цільова функція набуде такого вигляду:

$$Z_{\text{зловмисника}} = \max_{y=\{0,1\}} \sum_a (h_{ia}\, y_{ai}) Q_i, \quad y \in Y,\ a \in A. \tag{2}$$

У цьому випадку співвідношення (2) відображає ризик інформаційної безпеки в системі за відсутності системи захисту інформації, яка здатна зупиняти атаки зловмисника та понижувати загальний ризик автоматизованої системи.

Реалізація системи захисту інформації зводиться до вибору профілів захищеності p для компонента системи i. Стратегії захисника можуть бути позначені, використовуючи матрицю $X = \{x_{pi}\}$, де

$$x_{pi} = \begin{cases} 1, \text{ якщо профіль захищеності } p \\ \text{встановлений у вузлі } j, \\ 0, \text{ в іншому випадку.} \end{cases}$$

Вплив захисника на стан безпеки системи можна описати за допомогою (3). Необхідно брати до уваги той факт, що захисник для кожного з компонентів i може вибрати тільки один профіль захищеності, тому $V_{ai} = \{1\}$, якщо вибраний профіль є ефективним проти атаки a, і $V_{ai} = \{0\}$ у протилежному випадку:

$$V_{ai} = \sum_p d_{ap}\, x_{pi}. \tag{3}$$

На основі впливів зловмисника (2) та захисника (3) на результат конфліктної ситуації, можна визначити функцію виграшів (4). Ця характеристична функція на основі вибраних стратегій зловмисника y_{ai} та захисника x_{pi} визначає загальний ризик, наявний у системі. Чим вище значення функції $R(x, y)$, тим більший ризик і, відповідно, більше збитків може нанести зловмисник внаслідок вибраної стратегії:

$$R(x, y) = \sum_i \sum_a (h_{ia}\, y_{ai}) Q_i \sum_a \left(1 - \sum_p d_{ap}\, x_{pi}\right). \tag{4}$$

Маючи інформацію про стратегії учасників гри та функцію виграшу можна записати основну модель конфліктної ситуації між зловмисником і захисником:

$$G(X, Y, R). \tag{5}$$

Модель конфліктної ситуації "захисник–зловмисник" записано в нормальній формі (5). Згідно з визначеною задачею, а саме побудовою системи захисту, яка мінімізує максимальний можливий збиток, який може завдати зловмисник, захисник вибирає стратегії x із множини X, а зловмисник – стратегії y із множини Y. Функція виграшу $R = R(x, y)$ відображає виграш зловмисника при застосуванні стратегії y.

Синтез структури системи безпеки

Згідно з формалізованими відносинами конфліктних сторін, зловмисник намагається нанести максимальний збиток, тобто максимізувати функцію $R(x, y)$, у той час як у захисника протилежна мета – через встановлення профілів захищеності уникнути значного ризику, мінімізувавши $R(x, y)$. Враховуючи це, критерій задачі можна записати у вигляді максиміну (6). Цей критерій можна інтерпретувати як мінімальний ризик з тих, які можуть бути досягнуті при прийнятті рішення в найгірших для захисника умовах, і отже, як гарантований виграш:

$$Z = \min_x \max_{y=\{0,1\}} \sum_a (h_{ia}\, y_{ai}) Q_i \left(1 - \sum_p d_{ap}\, x_{pi}\right), \quad \sum_{pi} w_p\, x_{pi} \le W, \quad \sum_a \sum_i y_{ai} \le L. \tag{6}$$

Як зазначалося вище, задача передбачає пошук консервативного рішення захисту, тобто побудову такої системи захисту $\{x_{pi}\}$ від потенційних атак зловмисника $\{y_{ai}\}$ при існуючих обмеженнях на ресурси W, яка забезпечить захист від множини найбільш руйнівних загроз. Таким чином, витрати на реалізацію профілів захищеності не можуть перевищувати доступних ресурсів W, де W_p – вартість реалізації функціонального профілю p-го типу. Крім того, загальна кількість атак від зловмисника не може перевищувати обмеження L.

Можна розв'язати цю задачу з використанням апарату теорії двоїстості, завдяки чому позбудемося нелінійності. Оптимальний розв'язок отриманої цілочисельної задачі знайдемо симплекс-методом (розкладання за Бендерсом). Розв'язок системи дасть оптимальну стратегію захисту x^*, зафіксувавши це значення і підставивши в (6), отримаємо вибрану стратегію зловмисника при вибраному плані захисту. В термінах теорії ігор вибрані стратегії будуть становити рівновагу за Нешем.

Контрольний приклад побудови комплексної системи захисту ІКС

Розглянемо застосування описаного методу на реальному прикладі. Припустимо, що в обласних державних адміністраціях України було прийнято рішення із впровадження системи електронного документообігу (СЕД). Центральне сховище документів має розташовуватися в м. Київ.

Для зменшення навантаження на основний сервер буде створено сховища регіонального значення в трьох обласних центрах (Харків, Одеса та Львів), завданням яких стане обслуговування роботи власних регіонів і взаємодія зі всією Україною через центральний сервер.

На створення описаної системи виділено державні кошти, в тому числі визначена сума з них може бути витрачена на побудову системи захисту інформації. Необхідно, за умови наявності виділених коштів на систему захисту, мінімізувати ризик від потенційних атак зловмисника. Оптимальне рішення будемо шукати з використанням формальних математичних методів, а саме гри "захисник–зловмисник", яка має забезпечити оптимальний вибір функціональних профілів захищеності (6).

На першому кроці вирішення поставленого завдання проводиться аналіз інформаційної системи S, яку необхідно захищати. Описана система складається із 27 підсистем j (24 областей України, АРК, Києва та Севастополя), що взаємодіють між собою. Таким чином, маємо складну розподілену систему з одним центральним компонентом в м. Київ та трьома проміжними в Харківській, Одеській та Львівській областях (рис. 1).

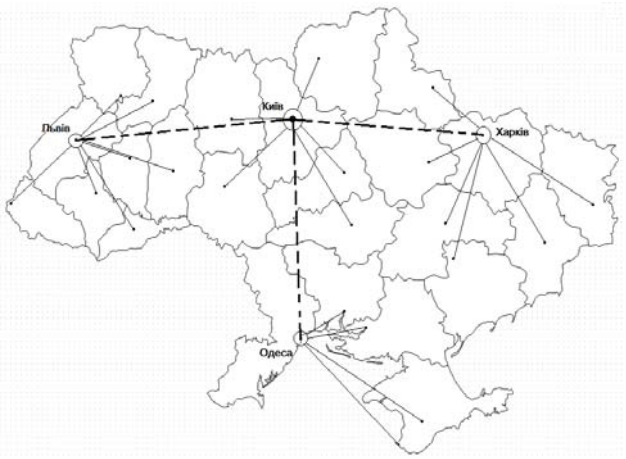

Рис. 1. Розподіл компонентів СЕД між регіонами з позначенням відповідних регіональних центрів

Для відображення збитку, який може бути завданий системі, необхідно здійснити оцінку цінностей вказаних компонентів системи. Цю характеристику C_j будемо вираховувати, використовуючи експертний метод аналізу ієрархій [9], на основі двох критеріїв: важливості вузла для функціонування системи в цілому (за шкалою від 1 до 10) та кількості користувачів відповідного вузла, яка пропорційна населенню в області, де розташовується відповідний вузол системи.

З усієї множини існуючих загроз T варто виділити такі, що за статистикою спричиняють найбільше збитків інформаційним системам S. Серед таких загроз визначимо неавторизований доступ, шкідливе програмне забезпечення, неправомірне використання ресурсів, відмова в обслуговуванні, підміна сервера тощо [5]. Оскільки список загроз, які слід врахувати при проектуванні системи захисту інформації, може бути досить великим, а кожна із загроз потребує ретельного експертного аналізу, в цьому прикладі згрупуємо всі загрози за певними ознаками. На практиці існує велика кількість класифікацій загроз інформаційної безпеки [1].

Використаємо класифікацію за властивостями інформації, які визначають її безпеку: конфіденційність, цілісність і доступність. Кожен з компонентів інформаційної системи *j*, яка розглядається, потребує захисту конфіденційності та цілісності інформації, а серверні компоненти потребують ще й забезпечення її доступності. Отже, в розглядуваній системі є три типи загроз на порушення: конфіденційності, цілісності чи доступності. Треба зазначити, що на практиці є загрози, які поєднують порушення відразу кількох властивостей інформації, в цьому випадку використовуються інші групування [1].

Після складання множини потенційних загроз, необхідно оцінити ймовірність реалізації h_a кожної з них. Експертним аналізом встановлено, що всі загрози є рівноймовірними.

Захист від вказаних загроз може бути забезпечений при використанні стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу, описаних у [3].

Для захисту інформації в розподілених системах необхідна реалізація одного з функціональних профілів захищеності *p*. Для АС класу 3 існує сім типів профілів захищеності, кожен з яких може бути реалізований з різним рівнем гарантій. Таким чином, при побудові системи захисту треба зробити вибір серед двадцяти восьми профілів захищеності. Реалізація кожного з профілів потребує певних ресурсів, які є обмеженими. Для всіх рівнів гарантій експертним шляхом було визначено вартість реалізації кожного функціонального профілю захищеності, яка пропорційна рівню захищеності, забезпеченого ним.

У зв'язку з тим, що витрати на реалізацію системи захисту обмежені, треба вибрати такий набір профілів, який створить необхідний та достатній рівень захисту для цієї системи. Після встановлення всіх обмежень і правил функціонування системи, можна переходити до розв'язання задачі побудови підсистеми захисту інформації. Отримані експертні дані є вхідними параметрами моделі "захисник–зловмисник".

Аналізуючи вихідні параметри за допомогою теоретико-ігрового підходу, розраховується оптимальна стратегія дій за наявних ресурсів захисника та з урахуванням можливостей зловмисника (6). Критерієм оптимальності є функція ризику, мінімізація якої і є основним завданням захисника.

Розв'язання задачі відбувається з використанням формального апарату цілочисельного програмування. Запрограмована в комп'ютерному математичному пакеті задача, наведена у співвідношенні (6), розв'язується існуючими математичними методами.

Було проведено низку експериментів для отримання значення ризику при різних вхідних параметрах. На рис. 2 показано зміну функції ризику залежно від виділених ресурсів на систему безпеки при різних типах зловмисника. Графік R1 описує зловмисника, котрий може проводити одночасно до чотирьох атак *L* (6), R2 – дві атаки, R3 – одна атака.

Значення ризику експоненційно спадає при збільшенні витрат на СЗІ. У разі витрати 600 умовних одиниць на побудову системи захисту значення ризику може бути зменшене до 9 % від початкового значення. У таблиці наведено набір профілів захисту, які забезпечують вказаний стан безпеки при різних витратах на реалізацію системи безпеки.

У результаті виконаної роботи отримано набір профілів захищеності інформації, які необхідно реалізувати у відповідних підсистемах для досягнення максимально можливого захисту. Профілі захищеності реалізуються за використанням функціональних послуг, які, в свою чергу, виконуються з використанням конкретних інженерних, технічних, організаційних, правових заходів і засобів.

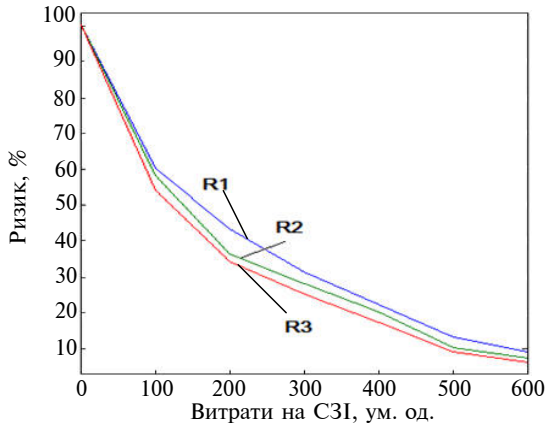

Рис. 2. Зміна функції ризику при зміні ресурсів захисника

Таблиця. Оптимальний набір профілів захисту x_{pi}

Компоненти	Реалізовані профілі захищеності						
м. Київ	Н/З	ЗКЦД4	ЗКЦД5	ЗКЦД5	ЗКЦД5	ЗКЦД5	ЗКЦД5
Київська область	Н/З	Н/З	ЗК1	ЗК1	ЗКЦ1	ЗКЦ1	ЗКЦ1
Вінницька область	Н/З	Н/З	ЗК1	ЗК1	ЗКЦ1	ЗКЦ1	ЗКЦ1
Черкаська область	Н/З	Н/З	Н/З	ЗК1	ЗКЦ1	ЗКЦ1	ЗКЦ1
Житомирська область	Н/З	Н/З	Н/З	ЗК1	ЗКЦ1	ЗКЦ1	ЗКЦ1
Чернігівська область	Н/З	Н/З	Н/З	ЗК1	ЗК1	ЗКЦ1	ЗКЦ1
Кіровоградська область	Н/З	Н/З	Н/З	ЗК1	ЗК1	ЗКЦ1	ЗКЦ1
Львівська область	Н/З	ЗКЦД1	ЗКЦД3	ЗКЦД4	ЗКЦД4	ЗКЦД4	ЗКЦД5
Івано-Франківська область	Н/З	Н/З	ЗК1	ЗК1	ЗКЦ1	ЗКЦ1	ЗКЦ1
Хмельницька область	Н/З	Н/З	Н/З	ЗК1	ЗКЦ1	ЗКЦ1	ЗКЦ1
Закарпатська область	Н/З	Н/З	Н/З	ЗК1	ЗКЦ1	ЗКЦ1	ЗКЦ1
Рівненська область	Н/З	Н/З	Н/З	ЗК1	ЗК1	ЗКЦ1	ЗКЦ1
Тернопільська область	Н/З	Н/З	Н/З	ЗК1	ЗК1	ЗКЦ1	ЗКЦ1
Волинська область	Н/З	Н/З	Н/З	ЗК1	ЗК1	ЗКЦ1	ЗКЦ1
Чернівецька область	Н/З	Н/З	Н/З	ЗК1	ЗК1	ЗКЦ1	ЗКЦ1
Харківська область	Н/З	ЗКЦД2	ЗКЦД3	ЗКЦД4	ЗКЦД5	ЗКЦД4	ЗКЦД5
Запорізька область	Н/З	Н/З	ЗК1	ЗКЦ1	ЗКЦ1	ЗКЦ1	ЗКЦ1
Донецька область	Н/З	Н/З	ЗКЦ1	ЗКЦ1	ЗКЦ1	ЗКЦ1	ЗКЦ6
Дніпропетровська область	Н/З	Н/З	ЗКЦ1	ЗКЦ1	ЗКЦ1	ЗКЦ1	ЗКЦ6
Луганська область	Н/З	Н/З	ЗЦ1	ЗКЦ1	ЗКЦ1	ЗКЦ1	ЗКЦ6
Запорізька область	Н/З	Н/З	ЗК1	ЗЦ1	ЗКЦ1	ЗКЦ1	ЗКЦ1
Полтавська область	Н/З	Н/З	ЗК1	ЗК1	ЗКЦ1	ЗКЦ1	ЗКЦ1
Сумська область	Н/З	Н/З	Н/З	ЗК1	ЗК1	ЗКЦ1	ЗКЦ1
Одеська область	Н/З	ЗК1	ЗКЦД2	ЗКЦД4	ЗКЦД4	ЗКЦД4	ЗКЦД5
АР Крим	Н/З	Н/З	ЗК1	ЗКЦ1	ЗКЦ1	ЗКЦ1	ЗКЦ6
Миколаївська область	Н/З	Н/З	Н/З	ЗК1	ЗК1	ЗКЦ1	ЗКЦ1
Херсонська область	Н/З	Н/З	Н/З	ЗК1	ЗК1	ЗКЦ1	ЗКЦ1
м. Севастополь	Н/З	Н/З	Н/З	Н/З	Н/З	ЗК1	ЗКЦ1
Витрати на систему захисту	0	100	200	300	400	500	600
Ризик	0,040	0,024	0,017	0,013	0,009	0,005	0,004
Ризик, %	100,000	60,212	43,077	31,526	22,063	13,582	9,701

Висновки

Проведений аналіз наявних підходів засвідчив необхідність використання формального математичного апарату для вирішення проблеми проектування систем захисту інформації. Запропонований у статті метод, який використовує формальний апарат теорії ігор і математичного програмування, має ряд особливостей, серед яких варто виділити врахування конфліктності інтересів зловмисника та захисника, а також постановка задачі за умов повноти інформації між сторонами. Вказані особливості реалізують більшу деталізацію моделі порівняно з аналогами.

Використовуючи розроблену модель, можна здійснити синтез структури системи захисту інформації та вибрати оптимальний набір функціональних профілів захищеності, що забезпечить максимальний рівень інформаційної безпеки. Гнучкість запропонованого підходу дає змогу використовувати його для широкого класу інформаційно-комунікаційних систем (з різною архітектурою, рівнем автоматизації, різного функціонального призначення, масштабу тощо). Розрахунки, проведені на прикладі роз-

поділеної інформаційної системи державного масштабу, показали адекватність, стійкість і математичну коректність прийнятої моделі.

Важливим нововведенням є підбір профілів захищеності окремо для кожного компонента системи, що дає можливість уникнути встановлення надлишкового, недоцільного захисту другорядних компонентів системи, в яких рівень важливості (секретності) оброблюваної інформації нижчий.

Подальший розвиток розробленого підходу передбачає побудову моделі з неповною інформацією, де зловмиснику невідомо про застосовані механізми захисту, а захиснику повністю або частково не відомі ймовірності реалізації загроз.

1. *Грайворонський М.В., Новіков О.М.* Безпека інформаційно-комунікаційних систем. – К.: ВНV, 2009. – 608 с.
2. *НД ТЗІ* 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 р., № 22.
3. *НД ТЗІ* 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 р., № 22.
4. *Зайченко Ю.П.* Дослідження операцій. – К.: Слово, 2003. – 688 с.
5. *Symantec* Global Internet Security Threat Report Trends for 2009 / Fossl M., Egan G., Haley K. et al. (eds) // Security-Shell. – **16**. – 2010. – P. 18.
6. *Антонов А.В.* Системный анализ: Учеб. – М.: Высш. шк., 2004. – 454 с.
7. *Ермаков А.А.* Основы надежности информационных систем: Учеб. пособие. – Иркутск: ИрГУПС, 2006. – 152 с.
8. *Brown G., Carlyle M., Salmeron J., Wood K.* Defending Critical Infrastructure // J. Interfaces. – **36**. – 2006. – P. 530–544.
9. *Тимошенко А.О.* Методи аналізу та проектування систем захисту інформації: Курс лекцій. – К.: Політехніка, 2007. – 174 с.
10. *Хэмди А. Таха.* Введение в исследование операций. – 7-е изд. / Пер. с англ. – М.: Вильямс, 2007. – 912 с.
11. *Шагин В.Л.* Теория игр с экономическими приложениями: Учеб. пособие. – М.: ГУ-ВШЭ, 2003. – 278 с.
12. *Cason A.K., Godfrey A.* Optimal Defense of Saudi Arabia's Pipelines Against Terrorist Attack. Red Team Report // Network Flows and Graphs. – 2003. – P. 18.
13. *Cormican I.A., Wood K.* Where to Install Contamination Detectors in a Subway System // Operation Research. – **16**. – 2005. – P. 71–92.
14. *Hakola B.M., Raffetto M., Yanik T.* Effects of Terrorist Attacks at U.S. Airports. Red Team Report // Network Flows and Graphs. – 2003. – P. 21.

Рекомендована Радою
Фізико-технічного інституту
НТУУ "КПІ"

Надійшла до редакції
23 лютого 2011 року