УДК 004.942

СИНТЕЗ СТРУКТУРИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ПОЗИЦІЙНОЇ ГРИ ЗАХИСНИКА ТА ЗЛОВМИСНИКА

В.В. ГЛУШАК, О.М. НОВІКОВ

Запропоновано підхід до вирішення задачі зі створенню системи захисту інформації за умови комплексного характеру атак зловмисника та обмеженості ресурсів захисника на побудову системи захисту. У термінах теорії ігор, побудовано модель в основі якої є формула ризику інформаційної безпеки та конфліктні взаємовідносини між зловмисником та захисником. За розробленою моделлю сформовано оптимізаційну задачу по зменьшенню витрат на побудову системи захисту за умови наявності інформації про зловмисника та наявних у системі вразливостях. Розроблено алгоритм розв'язання поставленої проблеми на основі методів експертної оцінки для отримання вихідних даних, теорії ігор та математичного програмування. Результатом розв'язання поставленої задачі є оптимальний набір механізмів захисту, що забезпечать максимальний рівень захищеності (мінімальне значення ризику інформаційної безпеки) за умови встановлених обмеженнь. На розподіленій інформаційно комунікаційній системі проведено розрахунок оптимального розміщення механізмів захисту для досягнення мінімального значення ризику та доведено практичну придатність розробленого підходу.

ВСТУП

Сучасні інформаційно-комунікаційні системи (ІКС) потребують захисту від атак зловмисників. Забезпечення безпеки інформації може бути досягнуто завдяки побудові системи захисту інформації (СЗІ), що представляє собою комплекс організаційних заходів, технічних і технологічних засобів, які перешкоджають несанкціонованому (незаконному) доступу до інформації. Під час побудови СЗІ необхідно враховувати дії зловмисника, який реалізує загрози активам ІКС, шляхом організації атак: простих (одноетапних) або комплексних, що складаються з набору взаємозв'язаних етапів. Комплексну атаку можна розділити на 3 етапи: розвідка, проникнення (безпосередньо атака) та зачищення слідів атаки [1].

Побудова системи захисту інформації (СЗІ) для протидії протиправним діям зловмисника — це складна процедура, яка може проводитись на основі формального або неформального підходів. На сьогодні розроблено ряд емпіричних та формальних методів, що вирішують поставлену задачу синтезу (побудови) СЗІ, метою якої є забезпечення ефективного захисту від зловмисника. Серед формальних методів забезпечення захисту структурно-складних систем широке застосування отримав логіко-ймовірнісний підхід, розроблений та розвинутий у роботах О.С. Можаєва, І.А. Рябініна, Г.М. Черкасова, Є.Д. Солженцева та інших [2]. Результати використання даного підходу для задач інформаційної безпеки наведено в роботах О.М. Новікова, А.М. Родіонова, А.О. Тимошенко та інших [3–5].

© *В.В. Глушак, О.М. Новіков*, 2013

Метою процедури побудови СЗІ є формування набору механізмів захисту, що відповідають заданим вимогам до ефективності протидії зловмиснику. Ця процедура складається з етапів аналізу системи, вибору механізмів захисту та оцінки ефективності. Якщо на етапі оцінки СЗІ виявлено її недостатню ефективність, процес вибору механізмів повторюється поки не буде вирішено поставленої задачі.

Якість синтезу структури СЗІ залежить від кваліфікованості розробника. Для мінімізації впливу розробника застосовуються підходи, що базуються на формальних методах синтезу, зокрема, математичному програмуванні та дослідженні операцій [1–4].

При зіткненні інтересів захисника та зловмисника, сторони намагаються досягти протилежних цілей маючи у своєму арсеналі певні набори альтернативних рішень, щодо впливу на ІКС. Формалізовані конфліктні ситуації представляють собою математичну модель (гру), синтез якої доцільно проводити з використанням апарату теорії ігор та методів математичного програмування, який забезпечить оптимальність отриманого рішення з гарантованим рівнем надійності.

Існуючі формальні підходи до моделювання та синтезу систем інформаційної безпеки присвячені розгляду переважно статичних випадків цих задач, які враховують прості (одноетапні) атаки [1]. Зважаючи на те, що атака зловмисника зазвичай комплексна, актуальною є задача протидії зловмиснику в умовах таких атак.

Існує велика кількість методів для моделювання динамічних систем та процесів, що в них відбуваються. Вибір тих чи інших методів залежить від повноти інформації про систему та її складність. Традиційним є підхід, що передбачає представлення системи у вигляді диференціальних рівнянь, які описують закони функціонування системи. У такому випадку задачею моделювання є визначення стану системи за відомих параметрів та впливах на цю систему [6–7]. Побудова такої моделі потребує повну інформацію щодо функціонування ІКС та процесів в ній, у тому числі опис СЗІ. Проте під час побудови систем захисту інформації доводиться діяти в умовах невизначеності, де вихідні дані задаються набором ймовірностей здійснення тих чи інших подій.

Побудова СЗІ передбачає прийняття рішень в умовах невизначеності, враховуючи конфліктні взаємовідносини суб'єктів системи, за наявності інформації про стани системи, можливі рішення (стратегії) та «виграші» від обраних рішень. Моделювання описаних процесів та пошук оптимальних рішень доцільно проводити з використанням математичного апарату теорії ігор. Один із класів ігр, що описують конфліктні ситуації, динаміка який впливає на поведінку гравців, є позиційні ігри [7]. Процес гри представляє собою перехід від одного стану гри до іншого, що відбувається шляхом вибору гравцями дії із множини доступних альтернатив. Для описаних задач, теорія ігор знайшла широке практичне застосування в різних сферах народного господарства, у тому числі в економіці, інформаційних технологіях, промисловості та військовій справі [8–9].

Актуальною задачею є мінімізація витрат на побудову СЗІ, за необхідності забезпечити необхідний рівень захищеності. Зазначений критерій може бути виведено із розробленої в термінах теорії ігор моделі.

Мета роботи — розробка підходу до синтезу структури системи захисту інформації в ІКС із використанням теорії ігор та забезпечення необхідного рівня захищеності із використанням мінімуму витрат на СЗІ, за умови комплексного характеру атак зловмисника.

ОПИС СИСТЕМИ

Об'єктом дослідження є розподілена ІКС із відкритою архітектурою, яка складається із C взаємодіючих компонентів, що приймають участь в обробці інформації. Кожен компонент описується набором характеристик, серед яких технологія обробки інформації, операційне середовище та інші. Вказані параметри компонентів складають їх цінність для системи, яка буде позначатися через q_c.

Враховуючи особливості обчислювального середовища, кожен із компонентів є вразливим до певних загроз із A допустимих загроз. Будемо допускати, що інформація про архітектуру ІКС є відкритою та відомою учасникам конфлікту. Крім того, задана ймовірність успішної реалізації загрози a проти компоненту системи c, а також ймовірність нейтралізації загрози, встановленням механізмів захисту p. Таким чином, на ефективність прийнятих зловмисником чи захисником рішення впливають випадкові фактори, що необхідно врахувати при моделюванні.

ПОЗИЦІЙНА ГРА «ЗАХИСНИК–ЗЛОВМИСНИК»

Побудова СЗІ розглядається як антагоністична гра двох гравців із повною інформацією, при чому сторони діють в умовах ризику. У такій грі ходи можуть бути детермінованими та випадковими. Детерміновані ходи є свідомим вибором стратегії дій гравців серед наявних альтернатив (варіантів рішень).

Рішення зловмисника визначає, яку розвідку чи загрозу a йому реалізовувати проти якого із компонентів c. Набір альтернатив можна представити у вигляді матриці $Y = \{y_{ac}\}$, що складається із булевих елементів, причому $y_{ac} = 1$ означає рішення, щодо реалізації загрози a проти компоненту c.

Вибір стратегії захисника передбачає встановлення механізму захисту $p = 1,2,...,P$ у компоненті c. Набір його альтернатив будемо описувати матрицею булевих елементів $X = \{x_{cp}\}$, причому $x_{cp} = 1$ означає рішення, щодо встановлення механізму захисту p у компоненті c.

Випадковий хід представляє собою вибір, що здійснюється під впливом випадкових факторів, а не конкретним гравцем. Набір таких факторів у теорії ігор називають «природою» — додатковим гравцем, що робить свої ходи випадково. Наприклад, під час перебору паролів існує не нульова ймовірність підбору правильного пароля або з іншої сторони, під час встановлення системи виявлення вторгнень існує ненульова ймовірність виявлення протиправних розвідувальних дій зловмисника (як то сканування портів). При цьому для кожного стохастичного ходу задається розподіл ймовірностей на множині всіх альтернатив «природи».

Будемо вважати, що «природа» впливає на рішення, які прийняв як зловмисник так і захисник. Позначимо через h_{ac} ймовірність успіху зловмисника під час розвідки або реалізації загрози a проти компоненту ІКС c. Тоді через d_{ap} позначимо ймовірність виявлення або нейтралізацію загрози a, під час встановлення механізму захисту p.

Ситуація, в якій опиняються гравці в результаті своїх ходів, називається позицією. Множину всіх позицій можна розбити на такі підмножини:

- позиції, що належать зловмиснику, в кожній із яких він робить вибір однієї із альтернатив, що доступні йому;
- позиції, що належать захиснику, в кожній із яких він робить вибір серед доступних йому альтернатив.

У теорії окремо виділяють позиції із випадковими ходами, проте в запропонованій моделі випадкові ходи «природи» безпосередньо пов'язані з детермінованими ходами обох гравців і будуть розглядатися разом. Таким чином, застосовуючи кожну із стратегій чи то зловмисником чи захисником існує ненульова ймовірність успіху (провалу) обраної стратегії в обраному обчислювальному середовищі, за заданої апріорної ймовірності успіху обраної події.

ЦІЛЬОВА ФУНКЦІЯ

Відносини між захисником та зловмисником можуть бути формалізовані з використанням функції ризику. Зловмисник завдаючи збитків системі намагається максимізувати ризик. У той же час, захисник, протидіючи зловмиснику, встановлює механізми захисту, прагнучи зменьшити ризик до нуля. В умовах обмеженості фінансових та технічних ресурсів, за заданої моделі зловмисника, захиснику необхідно розподілити засоби та заходи захисту, таким чином щоб ризик в ІКС був мінімальним. У термінах теорії ігор функція ризику виступає платіжною функцією.

Кількісною величиною для оцінки ризиків є завданий збиток Q_c, що виражається у вигляді витрат та неотриманої вигоди. Таким чином значення збитку Q_c спричинене певному компоненту c еквівалентне цінності цього компонента q_c для функціонування системи вцілому. У подальшому будемо вважати ці величини тотожніми.

У загальному вигляді співвідношення для функції ризику інформаційної безпеки R_{ac} можна записати як добуток ймовірності $P_{ac}^{\sim}$ реалізації загрози a та завданому збитку за реалізації цієї загрози Q_c. Також введемо змінну V_{ac}, що описує ймовірність нейтралізації загрози з використанням встановлених додаткових механізмів захисту [4]:

$$R_{ac} = P_{ac}^{\sim} * Q_c * (1 - V_{ac}). \quad (1)$$

Однією із особливостей протистояння між захисником та зловмисником є динамічний характер, так як атаці зазвичай передує спостереження за

системою та розвідка, які необхідно враховувати в моделі. Таким чином стан конфліктної ситуації може змінюватися з часом.

Приймемо, що атака зловмисника складається з K етапів, причому збиток буде завданий, якщо всі етапи завершено успішно. У такому випадку, ймовірність реалізації загрози можна представити як добуток ймовірностей успішної реалізації кожного з етапів $P_{ac}^{k\sim}$. Тоді, відповідно, співвідношення ризику має враховувати ймовірності реалізації загрози на кожному з етапів:

$$R^{\sim}{}_{ac} = \prod_{k=1}^{K} P_{ac}^{k\sim} * Q_c * (1 - V_{ac}). \qquad (2)$$

Співвідношення (2) відображає динамічний характер поведінки системи, стан якої змінюється під дією кожної із сторін. Враховуючи поетапність проведення атаки, відносини захисника та зловмисника будемо описувати із використанням позиційної гри, в якій учасники роблять по черзі ходи, намагаючись досягнути максимальної для себе вигоди. У відповідності до етапів комплексної атаки, можна виділити такі кроки позиційної гри:

- Зловмисник проводить розвідку. Метою даного етапу є аналіз, вивчення та пошук вразливостей в системі захисту для проведення атаки. Пошук вразливостей може здійснюватися пасивними або активними методами. Під час активного пошуку, зловмисник ризикує бути виявленим (етап 2), оскільки він впливає на діяльність системи (наприклад сканування портів, підбір пароля). Пасивний пошук є меньш ефективним, проте більш безпечним для зловмисника, оскільки при цьому відбувається збір інформації без втручання в роботу системи (прослуховування мережі по UDP протоколу). Задачею захисника на цьому етапі є попередити можливу атаку, шляхом нейтралізації вразливостей та виявленню зловмисника.
- Зловмисник проводить атаку. Використовуючи виявлену вразливість, зловмисник знешкоджує систему захисту та проводить безпосередню атаку (третій етап). На цьому етапі порушується одна або декілька фундаментальних властивостей інформації (конфіденційність, цілісність, доступність). Захисник застосовує наявні заходи та засоби захисту для нейтралізації небажаних дій.
- Зловмисник приховує сліди. Завершальним етапом атаки є знищення слідів, що можуть викрити зловмисника (зачищення журналів реєстрації подій, видалення тимчасових даних, тощо).

Гра може завершитися на одному із ранніх етапів, якщо захиснику вдасться виявити та знешкодити зловмисника, або на останньому етапі, якщо атаку проведено успішно. Таким чином апріорні ймовірності, щодо реалізації загроз h_{ac}^{k} та їх нейтралізації d_{ap}^{k} можуть змінюватися з часом, і тому мають бути задані для кожного з етапів k.

Як було зазначено, платіжна (цільова) функція виражається через ризик інформаційної безпеки, що зловмисник намагається збільшити, а захисник зменьшити. Зловмисник обираючи стратегію дій оперує ймовірністю реалізації загроз: $P_{ac}^{\sim k} = h_{ac}^{k} * y_{ac}^{k}$ та потенційним збитком $Q_c = q_c$ при технічних обмеженнях на кількість одночасно реалізованих загроз L. Захисник може

зменьшити ризик завдяки встановленню додаткових механізмів захисту: $V_{ac} = \sum_{p} d_{ap}^{k} * x_{cp}^{k}$. Якщо $V_{ac} = 1,$ то компонент c повністю захищений від загрози a, тому щоб не допустити встановлення надлишкових засобів та заходів захисту вводиться обмеження $V_{ac} \le 1.$ Крім того, у захисника обмежені ресурси W на реалізацію механізмів захисту p, вартість кожного з яких дорівнює w_p.

Підставивши визначені змінні в (2) та врахувавши мету захисника та зловмисника можна записати цільову функцію:

$$R = \min_{x} \max_{y} \prod_{k=1}^{K} \sum_{a=1}^{A} \sum_{c=1}^{C} \left\{ h_{ac}^{k} * y_{ac}^{k} * q_c * \left[1 - \sum_{p=1}^{P} d_{ap}^{k} * x_{cp}^{k} \right] \right\}. \qquad (3)$$

За наступних обмежень:

$$\sum_{a,c,k} y_{ac}^{k} \le L, \quad \sum_{c,p,k} w_p * x_{cp}^{k} \le W, \quad \sum_{p} d_{ap}^{k} * x_{cp}^{k} \le 1,$$

$$x_{cp}^{k} = \{0,1\}, \; y_{ac}^{k} = \{0,1\}.$$

Безкоаліційну гру зловмисника та захисника можна записати в нормальній формі як:

$$G^{\sim} \left\langle I = \{1,2\}; \; S = \{X, Y\}; R \right\rangle, \qquad (4)$$

де I — множина номерів гравців, S — множина допустимих стратегій гравців, а R — критерій виграшу.

За умови скінченної кількості етапів позиційна гра зловмисника та захисника розглядається як статична задача. Першим кроком розв'язання нелінійної задачі (3) передбачається перехід до двоїстої, шляхом введення змінної θ та зафіксувавши значення стратегій захисника x:

$$R = \min_{\theta} \prod_{k} \sum_{ac} \theta_{ac}^{k},$$

$$\theta_{ac}^{k} \ge h_{ac}^{k} * q_c * \left[1 - \sum_{p} d_{ap}^{k} * x_{cp}^{k} \right],$$

$$\sum_{c,p,k} w_p * x_{cp}^{k} \le W, \; \sum_{p} d_{ap}^{k} * x_{cp}^{k} \le 1, \quad \theta_{ac}^{k} \ge 0. \qquad (5)$$

Подальший розв'язок задачі (5) відбувається з використанням методу гілок та границь [11]. У результаті розв'язання отримуємо оптимальний набір рішень захисника $x_{cp}^{k\,*}$ та зловмисника $y_{ac}^{k^*}$, які в теорії ігор складають рівновагу за Нешем.

АЛГОРИТМ

Таким чином побудову СЗІ згідно розробленого підходу можна розділити на такі кроки:

1. Збір та аналіз вихідної інформації з використанням методів експертної оцінки.

- Аналіз структури ІКС, визначення кількості її компонентів c та інформаційних потоків між ними, оцінка цінності компонентів для функціонування системи. Результатом даного етапу є вектор цінностей q_c, який виражає потенційні збитки для кожного із компонент системи.
- Аналіз вразливостей, що характерні для систем із обраною архітектурою та технологіями.
- Аналіз загроз, що можуть бути реалізовані використовуючи наявні вразливості. При складанні моделі загроз необхідно врахувати, що зловмисник проводить комплексну атаку, виявляючи слабкі місця для нанесення максимального збитку. Результатом даного етапу є набір ймовірностей h_{ac}^k.
- Визначення релевантних механізмів захисту p та ймовірність нейтралізації загроз a з їх використанням d_{ap}^k.

2. Синтез структури системи захисту інформації. Підставляємо отримані на першому кроці вихідні дані в модель (3). У результаті розв'язання одержаної задачі з використанням симплекс методу, отримаємо відносне значення ризику R, а також набір механізмів захисту, що буде оптимальним під час протистояння.

ПРИКЛАД ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Розглянемо розподілену ІКС банку, що забезпечує передачу, обробку та збереження фінансових та персональних даних клієнтів. Припустимо, що банк діє на території Київської області та має представництва c у всіх районних центрах, а також у містах обласного підпорядкування. Центральне відділення, що координує роботу всієї установи знаходиться у столиці. Таким чином, система складається із $c = 1,2,...,30$ компонентів, які взаємодіють між собою.

Задача полягає в побудові системи захисту інформації для описаної ІКС, які забезпечить конфіденційність, цілісність та доступність даних. Допускається, що інформація про технології обробки інформації та обчислювальне середовище є доступною і може потрапити до зловмисника. Крім того, важливою вимогою є врахування характеру зловмисника, що може проводити атаки у декілька етапів.

Для вирішення поставленої задачі необхідно формалізувати систему, що підлягає захисту, в тому числі:

- провести оцінку потенційних втрат для кожного сегмента системи q_c;
- провести аналіз та створити модель порушника та атак, з урахуванням зазначених вимог, що буде включати можливі загрози a та ймовірність їх реалізації h_{ac};
- провести аналіз та реалізувати модель захисту де будуть обрані механізми захисту здатні протистояти зловмисникові.

Основні рішення, щодо побудови системи захисту, приймаються на етапі розробки політики безпеки. Саме тоді проводиться аналіз загроз та

вразливостей, складається модель порушника та обираються механізми, що забезпечать захист від нього. Під час обрання засобів та заходів захисту доцільно використовувати математичні засоби для синтезу структури системи захисту таким чином, щоб досягнути мінімального ризику. Результатом розробки політики безпеки є формалізована модель зловмисника та сформовані вимоги до СЗІ, в тому числі обрані механізми захисту.

ВИЗНАЧЕННЯ ЦІННОСТЕЙ КОМПОНЕНТ СИСТЕМИ

На першому етапі побудови СЗІ проводимо аналіз системи та виділяємо її компоненти c. Необхідно визначити цінність q_c компонентів системи c, яка в подальшому буде використовуватися для оцінки можливих збитків. Успішна реалізація загрози проти одного із компонентів системи призведе до фінансових втрат, що еквівалентні цінності цього компонента для функціонування системи вцілому. За відсутності статистичних даних та фінансових звітів, припустимо, що завданий збиток q_c пропорційний кількості клієнтів (населенню району) атакованої філії (табл. 1).

Таблиця 1. Компоненти системи c та їх цінності q_c

Філіал системи c	**Цінність** q_c
Київ	2799875
Баришівка	41287
Березань	17367
Біла Церква	255631
Богуслав	40602
Бориспіль	108633
Бородянка	57790
Бровари	163839
Васильків	70705
Васильків	39722
Вишгород	228015
Володарка	23384
Згурівка	22671
Іванків	35374
Ірпінь	101761
Кагарлик	37791
Красятичі	7567
Макарів	47915
Миронівка	40488
Обухів	71606
Переяслав-Хмельницький	67892
Ржищів	8447
Рокитне	36400
Сквира	44267
Славутич	24402
Ставище	28327
Тараща	36352
Тетіїв	37098
Фастів	88976
Яготин	40822

МОДЕЛЬ ПОРУШНИКА ТА ЗАГРОЗ

Невід'ємним етапом створення політики безпеки є формування моделі порушника. З огляду на поставлену задачу, необхідно передбачити захист від зовнішніх порушників з високою кваліфікацією, що оснащені необхідними програмними та апаратними засобами для віддаленої реалізації загроз ІБ та метою яких є: отримання доступу до конфіденційної інформації; отримання можливості вносити зміни в інформаційні потоки у відповідності зі своїми намірами; нанесення збитків шляхом знищення інформаційних цінностей.

Знаючи характерні ознаки порушника та його ціль, можна обрати типові загрози інформаційній безпеці a, використовуючи які, він зможе досягнути поставленої мети. Розроблений підхід розглядає атаку як динамічний процес, тому необхідно розділити загрози на етапи k у послідовності як вони будуть реалізовуватися порушником. Згідно вище зазначеного підходу розділимо процес реалізації загрози на 3 етапи (табл. 2).

Таблиця 2. Загрози інформаційній безпеці a та ймовірності їх виникнення h_a

Етап k	**№**	**Загрози** a	**Ймовірності реалізації** h_a
1		**Розвідка**	
	1	Сканування мережі	0,6
	2	Використання сканерів вразливості	0,7
	3	Аналіз протоколів	0,3
2		**Проникнення**	
	4	Віддалене проникнення	0,4
	5	Підбір паролів	0,6
	6	«Троянський кінь»	0,8
	7	Підміна об’єкта	0,9
3		**Реалізація мети**	
	8	Модифікація даних	0,9
	9	Відмова від авторства	0,7
	10	Розголошення інформації	0,5
	11	Відмова в обслуговуванні	0,9
	12	Підвищення привілеїв	0,8

Зазвичай розглядається також етап зачищення слідів, проте в рамках цього прикладу він розглядатися не буде, оскільки успішність його не впливає на збиток нанесений системі, проте є актуальним під час реагування на інцидент інформаційної безпеки та виявленню зловмисника.

Допускається, що в кожному із компонентів системи c використовуються однакові технології обробки інформації, а значить є вразливості до вказаних загроз інформації, причому ймовірність реалізації загрози проти кожного з компонентів однакова $\forall a, \forall c \Rightarrow h_{ac} = h_a$. Для простоти приймаємо, що ймовірність реалізації загрози залежить безпосередньо від виду загрози, проте не залежить від особливостей компоненту системи, принаймні поки не буде реалізована СЗІ.

МОДЕЛЬ ЗАХИСТУ

Наступним етапом розробки політики безпеки є обрання механізмів захисту, орієнтуючись на модель загроз та архітектуру обчислювального середови-

ща. Методом експертної оцінки визначається ефективність d_{ap} кожного із механізмів захисту p проти наявних загроз a в системі, а також вартість їх реалізації w_p (табл. 3). Кожен із механізмів захисту p забезпечує певний рівень захищеності.

Таблиця 3. Ймовірності d_{ap} нейтралізації загрози a механізмом захисту p та вартість реалізації даного механізму w_p

№	Механізми захисту p	Індекси загроз інформаційній безпеці a												Вартість w_p
		1	2	3	4	5	6	7	8	9	10	11	12	
1	Розмежування доступу	0,3	0,3	0,1	0,7	0,2	0,1	0,1	0,1	0,1	0,1	0,1	0,9	15
2	Ідентифікація та автентифікація	0,4	0,1	0,1	0,2	0,8	0,1	0,1	0,1	0,1	0,1	0,2	0,1	10
3	Криптографічні функції	0,3	0,2	0,1	0,1	0,3	0,2	0,1	0,7	0,7	0,8	0,1	0,1	20
4	Забезпечення цілісності	0,1	0,3	0,1	0,2	0,1	0,1	0,2	0,9	0,9	0,1	0,2	0,2	5
5	Антивірусний захист	0,1	0,4	0,1	0,1	0,1	0,8	0,1	0,1	0,2	0,1	0,1	0,1	10
6	Система виявлення вторгнень	0,7	0,9	0,3	0,2	0,1	0,3	0,8	0,1	0,3	0,1	0,7	0,1	30

СИНТЕЗ СТРУКТУРИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Зібравши необхідні дані, можна переходити до розв'язання поставленої задачі, а саме визначення структури системи захисту інформації, яка забезпечить мінімальне значення ризику інформаційної безпеки (2). Безпосередньо синтез СЗІ здійснюється з використанням співвідношення (3), результатом якого є набір механізмів захисту $\{p\}$ для кожного компоненту системи. Кількість можливих комбінацій, що аналізуються моделлю рівна $3*10^5$, тому, розв'язуючи цю задачу з експоненціальної складністю, використовувалися автоматизовані математичні пакети.

У табл. 4 надано рішення поставленої задачі для трьох різних випадків — за різних витрат на СЗІ W. У випадку витрат, що дорівнюють 600 одиниць, забезпечується зниження ризику до 17% від його значення за відсутності будь-якого захисту. У разі посилення системи захисту значення ризику знижується до 11% та 6% за витрат 800 та 1000 одиниць відповідно (табл. 5).

Для різних вихідних даних отримано набори механізмів захисту, що забезпечую мінімальний ризик при заданих обмеженнях (ресурси на побудову СЗІ).

Таким чином, на прикладі побудови СЗІ для ІКС фінансової установи показано практичну придатність розробленого підходу. Набір проведених експериментів показав, що запропонована модель є адекватною для синтезу

структури системи захисту інформації і може застосовуватися в системах підтримки прийняття рішень ІБ.

Таблиця 4. Встановлені механізми захисту

Компонент системи c	**Сукупність механізмів захисту** $\{x_{cp}\}$			**Компонент системи** c	**Сукупність механізмів захисту** $\{x_{cp}\}$		
Виділені ресурси (W)	600	800	1000	Виділені ресурси (W)	600	800	1000
Київ	12356	123456	123456	Богуслав	146	146	146
Біла Церква	1236	1236	12346	Миронівка	146	146	146
Вишгород	136	1236	12346	Васильків	126	146	126
Бровари	136	1236	12346	Кагарлик	126	146	126
Бориспіль	136	1236	1236	Тетіїв	126	146	126
Ірпінь	136	1236	1236	Рокитне	126	146	126
Фастів	136	136	1236	Тараща	126	126	126
Обухів	136	136	1236	Іванків	126	126	126
Васильків	136	136	1236	Ставище	126	126	126
Переяслав-Хмельницький	136	136	136	Славутич	126	125	126
Бородянка	146	136	136	Володарка	126	125	126
Макарів	146	136	136	Згурівка	25	125	123
Сквира	146	136	136	Березань	25	25	125
Баришівка	146	146	136	Ржищів	25	25	125
Яготин	146	146	146	Красятичі	24	25	25

Таблиця 5. Загальний ризик

Виділені ресурси (W)	600	800	1000
Загальний ризик ІБ (R)	0,17	0,11	0,06

ВИСНОВКИ

У статті запропоновано підхід до вирішення проблеми побудови системи захисту інформації за умови обмеженості ресурсів та розроблено алгоритм його реалізації на основі методів експертної оцінки, теорії ігор та математичного програмування. Ключовою відмінністю підходу є розгляд поставленої задачі за умов комплексної атаки зловмисника, тобто такої де його поведінка змінюється з часом. Використання математичного апарату теорії ігор, у тому числі максимінної стратегії, забезпечує отримання мінімального гарантованого значення ризику інформації, що відрізняє розроблений підхід від методів експертної оцінки.

Практичну придатність розробленого підходу було показано на прикладі побудови системи захисту для розподіленої інформаці комунікаційної системи. У результаті застосування розробленої моделі синтезовано

структуру СЗІ та отримано розподіл механізмів захисту між компонентами системи обробки фінансової інформації.

Розроблений підхід є гнучким, що дозволяє змоделювати поведінку порушників різного типу, а також для випадків, коли порушник циклічно повторює атаки.

Подальший розвиток підходу може бути направлений на аналіз ситуацій із неповною інформацією, для випадків коли одна або обидві конфліктуючі сторони не мають інформації про виконані ходи суперника.

ЛІТЕРАТУРА

1. *Грайворонський М.В., Новіков О.М.* Безпека інформаційно-комунікаційних систем. — К.: BHV, 2009. — 608 с.
2. *Рябинин И.А.* Научная Школа «Моделирование и Анализ Безопасности и Риска в Сложных Системах» и ее смысл // Труды четвертой Международной научной школы МА БР 2004, июнь 22–25, 2004. — 650 с.
3. *Родіонов А.М.* Логіко-імовірнісна модель захищеності компонентів інформаційно-комунікаційних систем // Інформаційні технології та комп'ютерна інженерія. — 2008. — № 1 (11). — С. 170–175.
4. *Глушак В.В., Новіков О.М.* Метод проектування систем захисту інформації з використанням детермінованої гри «захисник-зловмисник» // Наукові вісті НТУУ «КПІ». — 2011. — № 2. — С. 46–53.
5. *Архипов А.Е.* Технологии експертного оценивания в задачах защиты информации // Інформаційні технології та комп'ютерна інженерія: міжнар. наук.-техн. журн. — 2005. — № 1. — С. 89–94.
6. *Суздаль В.Г.* Теория игр для флота. — Москва.: Воениздат, 1976. — 317 с.
7. *Понтрягин Л.С.* Линейная дифференциальная игра убегания // Труды Математического института АН СССР, Т. 112. — 1971. — М.: Наука. — С. 30–63.
8. *Ishai Menache, Eitan Altmany* Battery-State Dependent Power Control as a Dynamic Game // Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops. — 2008. — WiOPT 2008. 6th International Symposium on. — Berlin. — P. 242–250.
9. *Мулен Э.* Теория игр с примерами из математической экономики. — Москва: Мир, 1985. — 200 с.
10. *Brown G., Carlyle M., Salmeron J., Wood K.* Defending critical infrastructure // Interfaces. J. — 2006. — **36**. — P. 530–544.
11. *Quesada I., Grossmann I.E.* An LP/NLP Based Branch and Bound Algorithm for Convex MINLP Optimization Problems // Computers Chem. Eng. — 1992.— 16 (10/11). — http://repository.cmu.edu/cgi/viewcotent.cgi? artcle=1176&context= cheme.

Надійшла 24.02.2012