УДК 004.3

В.В. Глушак, О.М. Новіков
Фізико-технічний інститут Національного Технічного Університету України «КПІ»
Кафедра інформаційної безпеки
v.glushak@gmail.com

Побудова системи захисту інформації заданого рівня захищеності з використанням теорії ігор

В роботі пропонується розглянути підхід до побудови системи захисту інформації заданого рівня захищеності з використанням теорії ігор. Природно, моделювати інформаційне протистояння як статичну гру двох осіб: зловмисника та захисника. Нагородою зловмисника є збиток завданий жертві, в той час як метою захисника є мінімізація витрат на систему захисту за умови забезпечення стабільної роботи системи. З математичної точки зору, конфліктна ситуація між зловмисником та захисником описується з використанням критерію максиміну. Розв'язавши описану задачу, ми отримаємо оптимальний набір механізмів захисту, що забезпечать необхідний рівень захищеності, при обраній моделі зловмисника та встановлених обмеженнях на реалізацію системи захисту.

Система захисту інформації, теорія ігор, модель захисника і зловмисника

Вступ

Створення системи захисту інформації складний та довготривалий процес, одним із найважливіших етапів є розробка політики безпеки. На цьому етапі приймаються рішення, щодо застосування тих чи інших механізмів захисту. Раціональний вибір засобів та заходів захисту досягається завдяки проведенню аналізу системи, вразливостей та потенційних загроз. Використовуючи отримані дані, можна визначити ефективності кожного з механізмів захисту та обрати найбільш ефективні. Існує ряд формальних підходів до оцінки захищеності в інформаційній безпеці, що поділяються на емпіричні методи експертної оцінки (метод аналізу ієрархій, метод Дельфі та інші) та формальні математичні методи (логіко–ймовірнісний підхід, математичне програмування, нейронні мережі, генетичний алгоритм, теорія ігор та інші).

В статті пропонується розглянути підхід до побудови системи захисту інформації з використанням теорії ігор. Можливість застосування теорії ігор до задач побудови системи захисту обгрунтовано в роботах багатьох дослідників, в тому числі для захисту об'єктів критичної інфраструктури та протидії терористичній діяльності [1,2].

Актуальною проблемою створення системи захисту – є мінімізація витрат на її реалізацію за необхідності досягнення заданого рівня захищеності. В такій постановці, природньо моделювати інформаційне протистояння як статичну гру двох осіб: зловмисника та захисника. Очікується, що обидва гравці ведуть себе раціонально, тобто намагаються отримати максимальну вигоду для себе. Таким чином, нагородою зловмисника є збиток завданий жертві, в той час як метою захисника є забезпечення стабільної роботи системи. Маючи відомості про інформаційно–комунікаційну систему (задача з прозорою інформацією), зловмисник оперує загрозами, намагаючись завдати максимального збитку. Захиснику необхідно розподілити засоби та заходи захисту таким чином, щоб забезпечити необхідний рівень захищеності інформаційної системи, мінімізувавши витрати на реалізацію системи захисту інформації.

Постановка задачі

Метою роботи є розробка підходу до проектування систем захисту інформації заданого рівня захищеності, який надасть можливість визначати набір механізмів захисту з оптимальним розташуванням, витрати на реалізацію яких будуть мінімальними.

Формалізація гри

Гра зловмисника та захисника відноситься до класу ігор двох конфліктуючих сторін з нульовою сумою та повною інформацією. Характеристикою стану є ризик інформаційної безпеки, а критерієм оптимізації мінімізація витрати на систему захисту, при максимізації ризику зловмисником.

З математичної точки зору, дана задача може бути описана з використанням критерію максиміну.

$$\mathbb{Z}(x, y) = \max_{y \in Y} \min_{x} (w * \mathbb{D} * x) \qquad (1)$$

В співвідношенні (1) x та y – це стратегії дій для захисника та зловмисника відповідно, які приймають булеві значення. Захисник обирає стратегії x, щодо реалізації механізмів захищеності $p \in P$, вартість створення кожного з яких дорівнює w, намагаючись мінімізувати загальні витрати $\mathbb{Z}$. Матриця $\mathbb{D} = \{d_{ap}\}$ відображає ефективність застосування механізму захисту p проти загрози a. Стратегії захисника x обмежені допустимим значенням ризику. Стратегії зловмисника y також обмежені певною множиною допустимих стратегій Y, що характеризується технічними можливостями зловмисника до проведення атаки.

Ризик інформаційної безпеки може бути розрахований як добуток ймовірності реалізації загрози та потенційного збитку [3].

$$Q * H < R \qquad (2)$$

Враховуючи вказане, можна записати обмеження, згідно якого значення ризику не повинно перевищувати заданого.

$$\sum_{a,i,p} q_i * h_{ia} * y_{ia} * (1 - d_{ap} * x_{pi}) < R \quad (3)$$

В співвідношеннях (2) та (3) $Q = \{q_i\}$ виражає потенційний збиток, що може бути заподіяний зловмисником компоненту системи i, $\mathbb{H} = \{h_{ia}\}$ – апріорні ймовірності реалізації загрози a проти компонента i, а скаляр R – це допустиме значення ризику або необхідний рівень захищеності якому повинна відповідати інформаційно–комунікаційна система.

Необхідно зауважити, що загроза a проти компонента i вважається реалізованою, якщо зловмисник обрав стратегію $y_{ia} = 1$, і тим самим збільшив загальний ризик. В той же час, загроза a проти компонента i вважається нейтралізованою, якщо захисник встановив механізм захисту p для атакованого компонента i, тобто $x_{pi} = 1$, причому даний механізм захисту p здатен протидіяти вказаній загрозі a, $d_{ap} = 1$.

Матриці Q, $\mathbb{H}$ та $\mathbb{D}$ є вихідними даними до описаної моделі, що потребують попереднього розрахунку. Шляхом аналізу та оцінки інформаційно–комунікаційної системи, можуть бути отримані значення поненційного збитку Q. Отримати ймовірності реалізації загроз $\mathbb{H}$ можливо описавши модель загроз (зловмисника). Аналіз зловмисника та вразливостей системи дасть можливість скласти матрицю ефективності механізмів захисту, до подолання вказаних загроз $\mathbb{D}$.

Аналіз та оцінка системи

В якості об'єкта дослідження розглядається гетерогенна розподілена система, що складається з множини компонентів $i \in S$, що взаємодіють між собою.

Кожен з компонентів має певну цінність для функціонування системи вцілому. За відсутності статистичних даних, цінність може бути розрахована методом аналізу їєрархій [4], використовуючи ряд критеріїв, таких як вартість компоненту, складність відновлення, критичність для функціонування системи та інші.

В даній задачі приймемо, що реалізована загроза зловмисника в разі успішності повністю виводить з ладу атакований компонент. За даної умови цінність компонента i буде еквівалентною потенційному збитку q_i.

Модель зловмисника (загроз)

Маючи інформацію про систему, її архітектуру, особливості обчислювального середовища, технології обробки інформації можна скласти множину потенційних загроз інформації $a \in A$.

Оцінка ймовірностей реалізації кожної із загроз проти кожного з компонентів $h_{ia} \in \mathbb{H}$ може бути проведена з використанням статистичних даних або методом експертної оцінки за їх відсутності.

Механізми захисту

Захисник володіючи інформацією щодо потенційних загроз A, може проаналізувати вразливості системи та скласти множину засобів та заходів захисту $p \in P$, що здатні подолати вказані атаки. Необхідно врахувати, що існує ймовірність неподолання механізмом захисту певної атаки. З урахуванням вказаного, елементи $d_{ap} \in \mathbb{D}$ матриці будуть виражати ймовірності нейтралізації потенційних загроз a та приймати дійсні значення від нуля до одиниці.

Синтез структури системи безпеки

Отримавши вихідні дані, можна переходити до розв'язання задачі (1), (3). Першим кроком розв'язання є позбавлення від нелінійності шляхом переходу від прямої задачі max-min до двоїстої задачі мінімізації по змінній x.

Оптимальне рішення отриманої задачі може бути знайдене одним із методів цілочисельного програмування, наприклад

методом гілок та границь, при цьому буде знайдено оптимальний набір механізмів захисту (стратегій захисника по встановленню систем захисту) x^*.

Зафіксувавши значення x як константу, можна повернутися до початкової задачі та знайти суму витрат на систему захисту, а також відшукати оптимальний набір стратегій зловмисника, щодо реалізації загроз.

Обрання механізмів захисту для інформаційно–комунікаційної мережі

Розглянемо можливість застосування обраного підходу на прикладі побудови системи захисту для інформаційно–комунікаційної мережі мобільного оператора. Основною задачею мережі є маршрутизація повідомлень, що надходять від користувачів послуг мобільного оператора.

Нехай, перед оператором мобільного зв'язку, що забезпечує покриття певного регіону постала задача побудови системи захисту інформації. Основною вимогою до системи захисту є гарантоване забезпечення роботи 75 (90, 95 та 99) відсотків користувачів.

Схематично архітектура мережі зображена на рисунку 1 і представляє собою розподілену мережу, що складається з 15 клієнтських компонентів, що є вихідними точками для подачі повідомлення; 3х маршрутизуючих компонент, що об'єднують територіально розподілені клієнтські компоненти; та центрального компоненту, що виконує функцію маршрутизації повідомлення до отримувача.

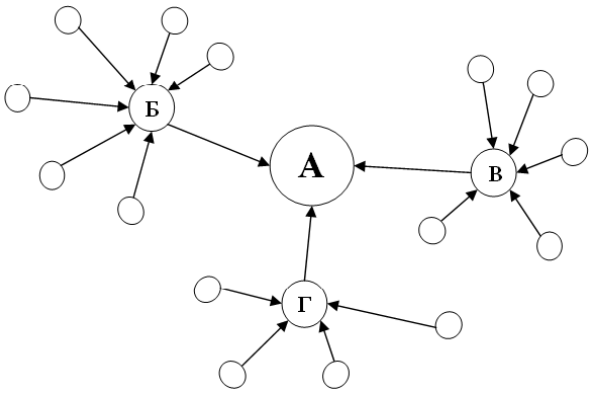

Рисунок 1 - Структурна схема архітектури мережі оператора мобільного зв'язку

Вирішення даної задачі будемо шукати з використанням моделі теорії ігор. Знаючи значення допустимого ризику, що пропорційне вимогам до надійності системи, необхідно розподілити механізми захисту, при цьому мінімізувавши витрати на їх реалізацію.

Першим етапом моделювання є збір вихідних даних. Як зазначалось раніше, отримати значення потенційного збитку Q можна шляхом аналізу цінностей компонентів системи.

В таблиці 1 подані значення цінностей кожного з компонентів, отримані методом аналізу ієрархій шляхом проведення експертної оцінки системи. У зв'язку з тим що клієнтські компоненти є рівнозначними, при аналізі системи та розрахунку вихідних даних ми їх будемо зображувати як один компонент.

Таблиця 1. Цінність компонентів системи

Компонент i	Оцінка Q_i
А	0,25
Б	0,15
В	0,125
Г	0,1
1..15	0,025

Маючи відомості про систему, можна провести аналіз та отримати множину потенційних загроз, щодо яких в даній системі є вразливості. Ми будемо розглядати набільш загальні загрози, які за статистикою спричиняють найбільших збитків [5]. В таблиці 2 подані такі загрози, а також ймовірність їх реалізації проти кожного з компонентів. Як і при оцінці потенційних збитків, ймовірності реалізації загроз h_{ai} були отримані експертним методом.

Таблиця 2. Загрози інформації

Загроза a	Ймовірність реалізації $h_{ai} \in H$				
	А	Б	В	Г	1–15
Розподілена відмова в обслуговуванні	0,6	0,3	0,3	0,3	0,1
Підбір паролів	0,2	0,3	0,3	0,3	0,2
Шкідливе програмне забезпечення	0,3	0,6	0,6	0,6	0,8
Віддалене проникнення	0,7	0,4	0,3	0,3	0,1
Модифікація даних	0,7	0,5	0,4	0,3	0,1
Підміна мережевих об'єктів	0,4	0,4	0,4	0,4	0,4
Аналіз протоколів	0,7	0,7	0,7	0,7	0,4

Протидіяти описаним загрозам можна шляхом використання засобів за заходів захисту. Провівши аналіз особливостей побудови системи та моделі зловмисника, можна скласти множину механізмів захисту, що здатні протидіяти описаним загрозам. В таблиці 3 наведені

механізми захисту, а також ефективність їх використання для подолання загроз.

Маючи необхідні вихідні дані можна розрахувати оптимальну стратегію розміщення механізмів захисту. Підставивши вихідні дані в описану модель (1) та (2), необхідно розв'язати отриману задачу цілочисельного програмування.

Оптимальне рішення було знайдено шляхом запрограмування даної задачі в математичному пакеті matlab(R). Програма, використовуючи вихідні данні, надає оптимальний набір стратегій захисника за різних значеннях допустимого ризику. Результати роботи програми наведені в таблиці 4, де для кожного компоненту пропонується певний набір механізмів захисту p, при різних значеннях ризику R.

Таблиця 3. Матриця застосування механізмів захисту $d_{ap} \in D$

	Загрози a						
Механізми захисту p	1	2	3	4	5	6	7
Антивірус (А)	0	0	0,9	0	0,2	0,2	0,1
Файрвол (Ф)	0,9	0,7	0,1	0,9	0,4	0,1	0,9
Система виявлення вторгнень (С)	0,9	0,9	0,4	0,3	0,7	0,6	0,7

Таблиця 4. Оптимальний набір механізмів захисту

	Вимоги значення ризику			
Компоненти	0,75	0,90	0,95	0,99
А	ФС	АФС	АФС	АФС
Б	ФС	АФС	АФС	АФС
В	ФС	ФС	АФС	АФС
Г	ФС	ФС	АФС	АФС
1	Ф	Ф	ФС	АФС
2	Ф	ФС	ФС	АФС
3	Ф	Ф	ФС	ФС
4	Ф	ФС	ФС	ФС
5	Ф	Ф	Ф	ФС
6	Ф	ФС	ФС	ФС
7	Ф	Ф	Ф	ФС
8	Ф	ФС	ФС	ФС
9	Ф	Ф	Ф	ФС
10	Ф	Ф	Ф	ФС
11	Ф	Ф	Ф	ФС
12	Ф	Ф	ФС	ФС
13	Ф	Ф	Ф	ФС
14	Ф	Ф	Ф	ФС
15	Ф	Ф	Ф	ФС

Як бачимо, серверні компоненти А,Б,В та Г потребують більшого захисту, як більш цінні та бажані для атак зловмисника.

Висновки

Задача забезпечення заданого рівня захищеності є актуальною для більшості установ та організацій, де обробляється інформація з обмеженим доступом. Запропонований в статті підхід вирішує проблему побудови оптимальної системи захисту інформації заданого рівня захищеності, де показником захищеності виступає ризик інформаційної безпеки. Як результат вирішення задачі оптимізації отримуємо мінімальну суму витрат на побудову СЗІ, а також структуру механізмів захисту для протидії обраному (змодельованому) зловмиснику.

Формулювання конфліктної ситуації між захисником та зловмисником з використанням формального апарату теорії ігор та математичного програмування гарантує оптимальність отриманого розв'язку. Це відрізняє розроблений підхід від методів, що беруть за основу рішення експертів, оптимальність результатів роботи яких не може бути математично доведена.

Практична придатність розробленого підходу була показана на прикладі побудови системи захисту для інформаційно-комунікаційної мережі мобільного оператора. Як результат проведеного моделювання, отримана сума витрат на набір механізмів захисту, що забезпечать захист від можливих загроз, таким чином, що ризик інформаційної безпеки не буде перевищувати заданого значення.

Список літератури

1. Jorma Jormakka Modelling Information Warfare as a Game / Jormakka Jorma, V. E. Jarmo // Journal of Information Warfare. – 2005. – 4(2). – P. 12–25.

2. Defending critical infrastructure / G. Brown, M. Carlyle, J. Salmeron, K. Wood // Interfaces. J. – 2006. – 36. – P. 530–544.

3. Качинський А.Б. Безпека, загрози і ризик: наукові концепції та математичні методи / А.Б. Качинський. – К., 2003. – 472 с.

4. Тимошенко А.О. Методи аналізу та проектування систем захисту інформації: курс лекцій / А.О. Тимошенко. – К.: Політехніка, 2007. – 174 с.

5. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков. – К.: BHV, 2009. – 608 с.

Надійшла до редколегії 21.03.2011

В.В. ГЛУШАК, А.Н. НОВИКОВ
Физико-технический институт Национального технического университета Украины «КПИ»

Построение системы защиты информации заданного уровня защищенности с использованием теории игр

В работе предлагается рассмотреть подход к построению систем защиты информации заданного уровня защищенности с использованием теории игр. Естественно, моделировать информационное противостояние как статическую игру двух лиц: злоумышленника и защитника. Наградой злоумышленника является ущерб нанесенный жертве, в то время как целью защитника является минимизация затрат на систему защиты при условии обеспечения стабильной работы системы. С математической точки зрения, конфликтная ситуация между злоумышленником и защитником описывается с использованием критерия максимина. Решив описанную задачу, мы получим оптимальный набор механизмов защиты, которые обеспечат необходимый уровень защищенности, при выбранной модели злоумышленника и установленных ограничениях на реализацию системы защиты.

Система защиты информации, теория игр, модель защитника и злоумышленника

V. GLUSHAK, A. NOVIKOV
Institute of Physics and Technology, National Technical University of Ukraine "Kyiv Politechnic Institute"

Development of Security System with Given Protection Level Using Game Theory

There an approach for building the information security system with given protection level by using game theory was introduced. Usually information warfare could be modeled as a static game with two players: attacker and defender. Attacker try to damage information system with an maximum losses for system's owner, while the defender is pretend to minimize the cost of security system but ensure stable system operation. From a mathematical point of view, conflicts between attacker and defender is described using the criteria max-min. Solving the described problem, we obtain the optimal set of protection mechanisms that ensure the necessary level of security.

Information security system, game theory, attacker – defender model