УДК 004

ПОБУДОВА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ЗАДАНОМУ РІВНІ ЗАХИЩЕНОСТІ ЗА ВИКОРИСТАННЯМ ТЕОРІЇ ІГОР

Глушак В. В., Новіков О. М.
Фізико-технічний інститут Національний Технічний Університет України «КПІ»
Кафедра інформаційної безпеки
e-mail: v.glushak@gmail.com

Анотація

Глушак В. В.,Новіков О. М. Побудова системи захисту інформації при заданому рівні захищеності за використанням теорії ігор. *В даній роботі пропонується розглянути підхід до побудови системи захисту інформації з використанням теорії ігор. Природньо, 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 ризику та забезпечення стабільної роботи системи. З математичної точки зору, конфліктна ситуація між зловмисником та захисником описується з використанням 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.*

Вступ

Сучасний етап розвитку цивілізації характеризується глобалізацією та інформатизацією суспільства. Більшість секторів економіки спираються на використаня інформаційних послуг та технологій, а інформаційні ресурси є важливим стратегічним товаром. Інформаційна складова стає базовою в національній безпеці, значним чином впливаючи на характер та направленість державної політики в будь якій важливій для держави сфері діяльності. Інтенсивний розвиток інформаційно-комунікаційних технологій створює нові можливості для реалізації загроз національної безпеки, пов'язаних з порушенням встановлених режимів використання інформації та комунікаційних систем. Регулярне удосконалення технологій обробки інформації потребує швидких та ефективних рішень в області інформаційної безпеки.

Ключовим етапом проектування систем захисту інформації є розробка політики безпеки, де приймаються рішення, щодо застосування тих чи інших механізмів захисту. Раціональний вибір засобів та заходів захисту досягається завдяки аналізу, попередній оцінці та визначенню ефективності кожного з них. Існує ряд підходів до оцінки захищеності та прийнятті рішень в інформаціній безпеці, що розділяються на емпіричні методи експертної оцінки (метод аналізу ієрархій) та формальні методи (логіко-ймовірнісний підхід, математичне програмування, нейронні мережі, генетичний алгоритм, теорія ігор та інші).

В даній роботі пропонується розглянути підхід до побудови системи захисту інформації з використанням теорії ігор. Можливість застосування теорії ігор до задач побудови системи захисту розглядається в ряді робіт, 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 задачі, 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. В арсеналі захисника є механізми захисту, ресурси на реалізацію яких обмежені. 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, який надасть можливість отримати оптимальний набір механізмів захисту, витрати не реалізацію яких будуть мінімальними, за необхідності відповідати заданому рівневі захищеності.

Формалізація гри

З математичної точки зору, конфліктна ситуація між зловмисником та захисником може бути описана з використанням максиміну.

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

В співвідношенні (1)x та y – це стратегії дій для захисника та зловмисника відповідно, які приймають булеві значення. Захисникобирає стратегії x, щодо реалізації механізмів захищеності $p \in P$, вартість створення кожного з яких відповідає w, намагаючись мінімізуватизагальні витратиZ.Матриця D відображає ефективність застосування механізму захисту проти тієї чи іншої загрози. Стратегії захисника x обмежені допустимим значенням ризику. Стратегії зловмисника y також обмежені певною множиною допустимих стратегій Y, що характеризується технічними можливостями зловмисника.

Ризик інформаційної безпеки може бути розрахований як добуток ймовірності реалізації загрози на потенційний збиток [3]. Враховуючи вказане, можна записати обмеження, згідно якого значення ризику не повинно перевищувати заданого.

$$Q * H * y * (1 - D * x) \prec R \qquad (2)$$

В співвідношенні (2)Qвиражає потенційний збиток, що може бути заподіяний зловмисником, H – апріорні ймовірності реалізації загрози, а R допустиме значення ризику або необхідний рівень захищеності якому повинна відповідати інформаційно-комунікаційна система. Q, H та 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 H можливо описавши модель загроз (зловмисника). Аналіз зловмисника та вразливостей системи дасть можливість скласти матрицю ефективності механізмів захисту, до подолання вказаних загроз 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 ієрархій[4], використовуючи ряд критеріїв, таких як вартість компоненту, складність відновлення, критичність для функціонування системи та інші.

В даній задачі приймемо, що атака зловмисника в разі успішності повність знищує атакований компонент. За даної умови цінність компоненту 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 $h_{ai} \in \mathrm{H}$ може бути проведена з використанням статистичних даних або методом експертної оцінки за їх відсутності.

Механізми захисту

Захисник володіючи інформацією щодо потенційних загроз A, захисник може проаналізувати вразливості системита 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 $d_{ap} \in \mathrm{D}$ матриці будуть виражати ймовірності нейтралізації потенційних загрозaта приймати значення від нуля до одиниці.

Синтез структури системи безпеки

Отримавши вихідні дані, можна переходити до розв’язання задачі (1), (2). Оптимальнерішеннядля обраної моделі може бути знайдене методом цілочисельного програмування. Отримане оптимальне значення $\mathrm{Z}(x, y)$ буде відображати мінімальні витрати на реалізацію системи захисту, за умови забезпечення необхідного рівня захищеності (допустимого значення ризику R). При цьому, стратегії захисника x в даній грі будуть складати оптимальний набір механізмів захисту враховуючи заданий критерій.

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.

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.

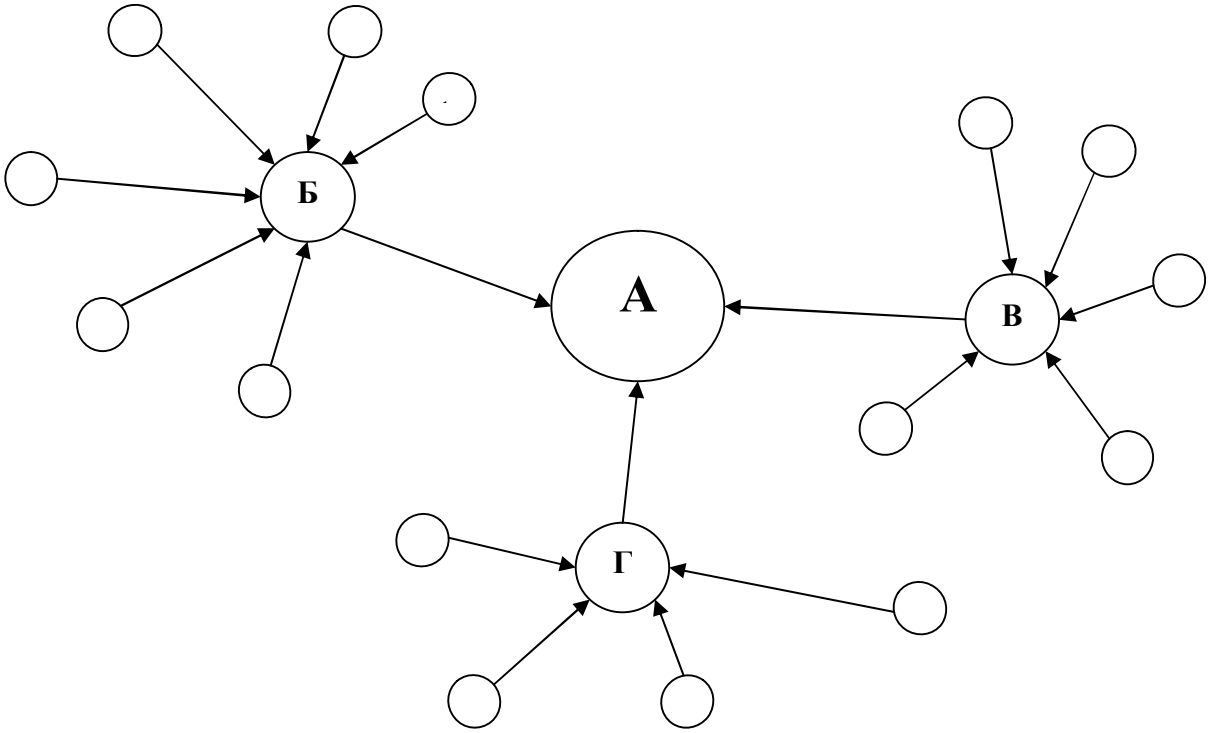

Рис 1. Структурна схема архітектури мережі оператора мобільного зв’язку

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
1. Розподілена відмова в обслуговуванні	0,6	0,3	0,3	0,3	0,1
2. Підбір паролів	0,2	0,3	0,3	0,3	0,2

3. Шкідливе програмне забезпечення	0,3	0,6	0,6	0,6	0,8
4. Віддалене проникнення	0,7	0,4	0,3	0,3	0,1
5. Модифікація даних	0,7	0,5	0,4	0,3	0,1
6. Підміна мережевих об’єктів	0,4	0,4	0,4	0,4	0,4
7. 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.

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

	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

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.

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 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

В роботі пропонується підхід до вирішення проблеми побудови оптимальної системи захисті інформації при заданих вимогах до рівня ризику. В якості формального апарату для розв'язання задачі пошуку оптимального рішення обрана теорія ігор, в термінах якої запропонована модель взаємодії захисника та зловмисника.Розв'язання описаної задачі надає оптимальний набір механізмів захисту, що забезпечить необхідний рівень ризику інформаційної безпеки, при цьому мінімізувавши витрати на створення системи захисту. В порівнянні з існуючими методами, в тому числі методами, в яких рішення приймають експерти, використання формального підходу гарантує оптимальність отриманого розв'язку.

Працездатність описаного методу доведено на прикладі інформаційно комунікаційної мережі мобільного оператора. Розв'язавши описаний приклад, було отримано набір механізмів захисту, що забезпечує необхідний рівень захищеності системи.

Література

1. Jorma Jormakka, Jarmo V. E. Molsa «Modelling Information Warfare as a Game», Journal of Information Warfare, 2005 4(2): 12-25.
2. Brown G., CarlyleM., SalmeronJ., WoodK. Defending critical infrastructure. Interfaces. 2006 p., 36, cc. 530-544.
3. Качинський А. Б.Безпека, загрози і ризик: наукові концепції та математичні методи. - К., 2003. - 472 с.
4. ТимошенкоА.О. Методи аналізу та проектування систем захисту інформації: Курс лекцій. – К.: Політехніка, 2007. – 174 с.
5. ГрайворонськийМ. В., НовіковО. М. «Безпека інформаційно-комунікаційних систем» - К., 2007