Поскольку каждый модуль обладает стабильными электромагнитными характеристиками, на которые соседние модули не оказывают влияния, существует возможность поэтапного создания автоматизированной системы с большим количеством рабочих мест. При этом после каждого шага наращивания (подключения дополнительного модуля) специальные исследования по ТЗИ проводятся не для всей системы, а только для нового модуля.

Внедрение компанией ЕПОС модульного принципа при построении защищенных локальных сетей на базе ТК ОКИ в ряде организаций позволило снизить сроки ввода в эксплуатацию защищенных сетей, ограничить несанкционированный доступ к конфиденциальной информации и снизить эксплуатационные затраты. Такой принцип построения защищенных сетей с нашей точки зрения может явиться основой для разработки общепринятых методик построения и оценки уровня их защищенности в общегосударственном масштабе.

Поступила 26.03.2008г.

УДК 004.056:378(147)

М.Г.Коляда

ПРОГНОЗУВАННЯ ОБСЯГІВ ПЕРЕДАЧІ ЗАХИЩЕНОЇ ІНФОРМАЦІЇ ПО РАДІОКАНАЛАХ НА ОСНОВІ ТЕОРІЇ ГРИ З ПРИРОДОЮ

Вступ

Останнім часом затребуваність знань з теорії ігор у різних прикладних областях людської діяльності підсилюється

Теорія ігор усе ширше проникає в практику прогнозування економічних процесів. Її можна розглядати як інструмент, що допомагає підвищити ефективність планових і управлінських рішень. Вона знайшла широке застосування в області створення інтелектуальних ігрових та навчальних систем.

Однак при використанні теорії ігор, варто пам'ятати про особливості, які існують при застосуванні цієї теорії в області захисту інформації. Деякі автори [1] указують, що міні-максна теорія стратегічних ігор не завжди є найкращим підходом при моделюванні систем захисту. Як відомо міні-максна стратегія припускає, що функція $\varphi(p)$ супротивника -- протилежність вашої власної функції $\varphi(s)$. Таким чином, $\varphi(p) = -\varphi(s)$. В області економіки і менеджменту подібне допущення мало деякий успіх. Однак, в області побудови систем захисту інформації таке припущення не завжди справедливе, тому що мається ряд причин при яких $\varphi(s) \neq \varphi(p)$. Насамперед, зловмисник, цілком ймовірно, має мету відмінну від цілей і пріоритетів системи захисту. По-друге, далеко не завжди зловмисник має повну інформацію щодо конфігурації системи захисту, що значно ускладнює для нього можливість судити наскільки він близько знаходиться біля своїх цілей.

Іншою негативною стороною застосування теорії ігор в питаннях захисту інформації є те, що існують обмеження в можливостях автоматизованої розробки рівноважної (цільової) функції. У початковій стадії розвитку цієї ідеї було все добре; були розроблені методології для настроювання таких рівноважних функцій протягом гри. Найбільш яскравим прикладом, служить використання нейронних мереж у боротьбі з мережними атаками.

На відміну від експертних систем, які можуть дати користувачу визначену відповідь, чи відповідають чи ні поточні характеристики, еталонним характеристикам, які закладено у базу цих правил, нейромережа аналізує інформацію і оцінює, чи погодяться дані, які розглядаються з характеристиками, які вона повинна розпізнати. Відомо, що спочатку нейромережа сама навчається шляхом правильної ідентифікації попередньо обраних прикладів предметної області. Реакція

нейромережі аналізується і система настроюється таким чином, щоб досягти задовільних результатів. В додаток до первісного періоду свого навчання, нейромережа також набирається «досвіду» з часом, по мірі того, як вона проводить аналіз даних, пов'язаних із предметною областю.

Однак, спираючись на дані, які отримані від супротивника для навчання програми, ми піддаємося небезпеці, тому що зловмисник може створити дані, які навчать програму до неадекватної реакції і це буде використано в майбутньому для злому системи.

Інші автори [2] вважають, що теорію ігор можна застосувати при побудові неформальної моделі зловмисника (порушника), яка відбивала би причини і мотиви його дій, його можливості, апріорні знання, переслідувані цілі, пріоритетність для порушника, основні шляхи досягнення поставлених цілей – способи реалізації вихідних від нього погроз, місце і характер дії, можлива тактика і т.п. Найчастіше теоретично і застосовується теорія ігор, коли для створення захисної системи використовується *матриця погроз/засобів* захистів і *матриця ймовірностей* настання погроз. У зловмисника існує своя власна *матриця нападів* (цінностей), у загальному випадку ця матриця може не збігатися з матрицею сторони, яка захищається.

Але ніхто з перерахованих дослідників не приводить конкретні приклади використання елементів теорії стратегічних ігор, а тим більше, не вказує на технологічні кроки у втіленні своїх ідей. *Задача нашої статті* саме і полягає в тому, щоб на конкретному прикладі показати переконливість застосування концепцій, які лежать в основі теорії ігор.

Наявність невизначеностей значно ускладнює процес вибору ефективних (оптимальних) рішень і може привести до непередбачених результатів. Перед фахівцями в області захисту інформації встає задача прогнозування ефективних рішень без обліку неконтрольованих факторів, тобто в умовах невизначеності, коли зіштовхуються інтереси двох чи більш конкуруючих сторін, кожна з який переслідує свою мету, причому, результат будь-якого заходу кожної зі сторін залежить від того, які дії почне супротивник. Тому *актуальність* розробки даної *теми дослідження* дуже своєчасна і результати мають великі перспективи практичної реалізації.

ПРОГНОЗУВАННЯ ОБСЯГІВ ПЕРЕДАЧІ ЗАХИЩЕНОЇ ІНФОРМАЦІЇ ПО РАДІОКАНАЛАХ

При передачі захищеної інформації по радіоканалах, результат залежить від багатьох факторів (надійності роботи апаратури, розташування приймально-передавальних пристроїв, «шумового» фону і т.п.), але все-таки одним з головних залишається погодний фактор, який залежить у першу чергу від того, скільки водяної маси знаходиться в атмосфері.

Теорія ігор – це теорія математичних моделей прийняття оптимальних рішень в умовах невизначеності, протилежних інтересів різних сторін, конфлікту [3]. Теорія ігор умовно підрозділяється на *теорію стратегічних ігор* і *теорію статичних ігор*. Другий напрямок у теорії одержав назву *гри з природою*.

Відмінність ігор із природою від стратегічних ігор полягає в тому, що в них один з учасників протидіє супернику не усвідомлено. У стратегічних іграх антагоністичний характер для двох гравців: виграш одного дорівнює програшу іншого.

У статистичній грі природа не є розумним гравцем, який прагне вибрати для себе оптимальні стратегії. Цей гравець не зацікавлений у виграші. Інша справа людина, – вона має на меті виграти гру з уявлюваним супротивником, тобто з природою.

Гравець-природа не вибирає оптимальної стратегії, а людина прагне до визначення розподілу ймовірностей стану природи. Отже, основними відмінностями статистичної гри від стратегічної є: відсутність прагнення до виграшу в гравця-природи, тобто відсутність антагоністичного супротивника; можливість другого гравця – людини, провести статистичний експеримент для одержання додаткової інформації про стратегії природи.

При передачі захищеної інформації по каналах радіозв'язку, погодні фактори впливають на всі передавальні пристрої не конкретно, а одноманітно, подібно природі. Приведемо наступний приклад.

Радіопередавальний центр (перший гравець) може використовувати одну з трьох передавальних станцій, які позначимо через K_1, K_2, K_3. Їхні стратегії роботи позначимо через

S_1, S_2, S_3. Необхідно визначити, який із трьох передавачів необхідно задіяти в радіозв'язку, якщо за інших рівних умов, обсяги передавальної інформації залежать головним чином від погоди (другий гравець, стратегії – G_1, G_2, G_3) (див. табл.), а загальна кількість переданої захищеної інформації повинна бути максимальною.

Таблиця

Стратегія першого гравця (радіопередавальний центр)		**Стратегія другого гравця («погода»)**			**Умовна ціна якості захищеної інформації**
		дощова погода G_1	**нормальна погода G_2**	**суха погода G_3**	
Передавальне пристрій K_1	1	60	15	45	4
Передавальне пристрій K_2	2	22,5	37,5	15	8
Передавальне пристрій K_3	3	0	22,5	30	16

Якщо радіопередавальний центр має в своєму розпорядженню достовірні статистичні дані про погодні умови під час передбачуваного радіо сеансу, чи має надійний спосіб прогнозу погоди, то оптимальна кількість переданої захищеної інформації досить просто одержати, грунтуючись на максимізації математичного очікування. У противному випадку планування кількості переданої захищеної інформації здійснюється з обліком найбільш несприятливого стану погоди. Остання обставина допускає трактування даної радіопередавальної ситуації таким чином: з одного боку, радіопередавальний центр (ми назвемо його гравцем 1) зацікавлений у тому, щоб задіяти той передавальний пристрій (із трьох наявних), який дасть максимальну кількість переданої захищеної інформації, з іншого боку – природа (ми назвемо її гравцем 2), від якої залежать природні умови і яка тим самим може максимально нашкодити радіопередавальному центру, переслідує прямо протилежні інтереси. Прийняття природи за супротивника, що рівносильне плануванню використання передавальних пристроїв у найбільш несприятливих умовах, а якщо вони виявляться сприятливими, то отриманий вибір дасть можливість збільшити загальну кількість переданої захищеної інформації.

Таким чином, у наявності антагоністичний конфлікт ігрової ситуації. Які стратегії в даному конфлікті має природа? Число її стратегій (станів природи) варто вважати нескінченним. Однак, як це часто приймають, ми будемо «у першому наближенні» вважати, що під час радіо сеансу погода може бути *сухою, нормальною* (в міру вологою, тобто яка задовольняє нормам вологості для проходження радіосигналу) і з великими опадами (*дощовою*), тобто будемо вважати, що гравець 2 (природа) має тільки три стратегії. У радіопередавального центру маються також три стратегії: використовувати передавальний пристрій K_1, використовувати передавальний пристрій K_2, використовувати передавальний пристрій K_3 (з різними значеннями по обсягах передавальної інформації). Щоб представити описаний конфлікт у виді матричної гри, необхідно задати функцію корисності гравця 1 (цільову функцію). В якості функції корисності візьмемо функцію кількості переданої захищеної інформації радіопередавальним центром (тобто обсяг переданої інформації, помножений на умовну ціну якості захищеної інформації). Допустимо, що на підставі досвіду відомо, що при дощовій погоді обсяг переданої загальної інформації складає 60 гігабайт (Гб) для передавального пристрою K_1, при нормальної – 15 Гб, при сухій – 45 Гб, при умовній ціні якості захищеної інформації в 4 одиниці за 1 Гб, аналогічні дані маються по другому передавальному пристрою K_2 і третьому передавальному пристрою K_3 (див. табл.). Тоді, якщо зневажити іншими факторами, що впливають на радіопередачу інформації (сигналу), можна все це представити у виді ігрової матриці.

Перший рядок: 60 * 4 = 240; 15 * 4 = 60; 45 * 4 = 180.

Другий рядок: 22,5 * 8 = 180; 37,5 * 8 = 300; 15 * 8 = 120.

Третій рядок: 0; 22,5 * 16 = 360; 30 * 16 = 480.

$$H = \begin{pmatrix} 240 & 60 & 180 \\ 180 & 300 & 120 \\ 0 & 360 & 480 \end{pmatrix}$$

Можна без труда написати ігрову матрицю загальної кількості переданої захищеної інформації радіопередавальним центром, яка буде враховувати як поглинання радіосигналу, наявності пилу в атмосфері та інших можливих факторів. Ми тут не робимо цього, щоб уникнути громіздкості.

Скоротимо елементи матриці на 6, одержимо матрицю виграшу першого гравця:

$$H = \begin{pmatrix} 40 & 10 & 30 \\ 30 & 50 & 20 \\ 0 & 60 & 80 \end{pmatrix}$$

Таким чином, кінцева антагоністична гра, що задається цією матрицею, є теоретико-ігровою моделлю описаного ігрового конфлікту.

Неважко знайти верхню і нижню ціну гри (див. [3]):

$$H = \begin{pmatrix} 40 & 10 & 30 \\ 30 & 50 & 20 \\ 0 & 60 & 80 \\ 40 & 60 & 80 \end{pmatrix} \begin{matrix} 10 \\ 20 \\ 0 \end{matrix}$$

$$\alpha = \max_{i \in S} \cdot \min_{j \in G} a_{ij} = \max\{10,20,0\} = 20$$

$$\beta = \min_{j \in G} \cdot \max_{i \in S} a_{ij} = \min\{40,60,80\} = 40$$

Оскільки $\alpha < \beta$, отже, гра не має сідловою точки, тому оптимальна стратегія гравця 1 – змішана. Для знаходження такої стратегії необхідно вирішити задачу лінійного програмування:

Цільова функція $Z = x_1 + x_2 + x_3 = \frac{1}{\nu} \to \min\limits_{x_1, x_2, x_3}$

З виконанням наступних умов:

$$40x_1 + 30x_2 \geq 1$$

$$10x_1 + 50x_2 + 60x_3 \geq 1$$

$$30x_1 + 20x_2 + 80x_3 \geq 1$$

$$x_1, x_2, x_3 \geq 0$$

де:

$$x_1 = \frac{P_1}{\nu}$$

$$x_2 = \frac{P_2}{\nu}$$

$$x_3 = \frac{P_3}{\nu}$$

$$x_1 + x_2 + x_3 = \frac{1}{\nu}$$

$$\nu \geq 20, \nu \leq 40$$

Вирішимо цю задачу, використовуючи механізм *Пошук рішення* табличного процесору Excel.

Відведемо чарунки B1:B3 під невідомі величини, які змінюються (x_1, x_2 x_3), чарунки F1:F3 під відповідні ймовірності (P_1, P_2 P_3):

=B1*B4
=B2*B4
=B3*B4,

а чарунок B4 під очікувану кількість переданої захищеної інформації (v).

В чарунках A5:A7 запишемо праві частини нерівностей:

=40*B1+30*B2
=10*B1+50*B2+60*B3
=30*B1+20*B2+80*B3,

а в чарунках C5:C7 – їхні ліві частини (вони усі дорівнюють одиниці).

Відповідно в чарунках A8:A9 укажемо значення очікуваної кількості переданої захищеної інформації (перепозначимо чарунок B4), а в чарунках C8:C9 їхні праві частини (більше або дорівнює 20, і менше або дорівнює 40 – це нижня і верхня ціна гри). В чарунок A10 укажемо ліву частину рівності:

=B1+B2+B3,

а в чарунок C10 – праву частину (вона дорівнює зворотній величині очікуваної кількості переданої захищеної інформації). Це саме і є значення чарунок D4, що виступає в ролі цільової функції (вона прагне до min, тому що сама очікувана кількість переданої захищеної інформації повинна прагнути до max). Усі представлені записи на робочому листі будуть розміщені так, як показано на рис. 1, а формули так, як показано на рис. 2.

D4 = =1/B4

	A	B	C	D	E	F
1	X1:	0			P1:	0
2	X2:	0			P2:	0
3	X3:	0			P3:	0
4	V:	20	Целевая:	0,05		
5	0	>=	1			
6	0	>=	1			
7	0	>=	1			
8	20	>=	20			
9	20	<=	40			
10	0	"="	0,05			

Рис. 1

D4 = =1/B4

	A	B	C	D	E	F
1	X1:				P1:	=B1*B4
2	X2:				P2:	=B2*B4
3	X3:				P3:	=B3*B4
4	V:	20	Целевая:	=1/B4		
5	=40*B1+30*B2	>=	1			
6	=10*B1+50*B2+60*B3	>=	1			
7	=30*B1+20*B2+80*B3	>=	1			
8	=B4	>=	20			
9	=B4	<=	40			
10	=B1+B2+B3	"="	=1/B4			

Рис. 2

Спочатку чарунок очікуваної кількості переданої захищеної інформації заповнимо числом 20 (нижня ціна гри), щоб в чарунках зворотних величин не виникала помилка розподілу на нуль.

Запустимо механізм знаходження мінімальної величини цільової чарунки. Заповнимо всі перераховані обмеження, плюс обмеження додатності в чарунках, які змінюються (див. рис. 3).

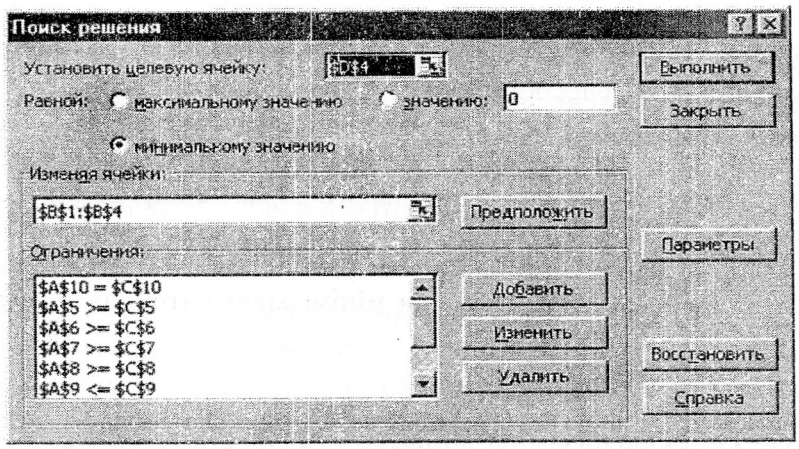

Рис. 3

Рис. 4

Одержали результат:

$$P = (0{,}49;0{,}40;0{,}11)$$

$$\nu = 31{,}56$$

Змішана стратегія задає ймовірності, з якими гравець 1 вибирає чисту стратегію гри. У даному прикладі радіопередавальний центр з ймовірністю 0,49 повинний використовувати передавальний пристрій $К_1$, з ймовірністю 0,40 – передавальний пристрій $К_2$, і з ймовірністю 0,11 – передавальний пристрій $К_3$.(рис. 4). Для визначення конкретного передавального пристрою з таблиці випадкових чисел випадковим образом вибирається число. Якщо воно виявиться в межах від 0 до 21, то використовувати треба передавальний пристрій $К_1$; якщо воно попадає в діапазон від 22 до 39, то вибирається передавальний пристрій $К_2$; і нарешті, якщо це число дорівнює від 40 до 44, то використовується передавальний пристрій $К_3$; якщо ж число знаходиться в межах від 45 до 99, то воно відкидається і з таблиці вибирається наступне число (чи вище, чи нижче першого, в відповідності з заздалегідь прийнятою умовою).

Реалізація вирішення побудови гри за допомогою фізичної суміші стратегій полягає в тому, що випадковий вибір однієї з трьох чистих стратегій гравця 1 заміняється застосуванням іншої стратегії – треба використовувати всі три передавальні пристрої одночасно – 49% першим передавальним пристроєм, 40% – другим, 11% – третім, тобто у відношенні 22:18:5, що дасть одержання гарантованої кількості переданої захищеної інформації при всіх погодних умовах не менше як 31,56 Гб.

Висновки

Застосування теорії гри з природою для прогнозування обсягів передачі захищеної інформації по радіоканалах має практичне втілення.

Використання теоретичних основ даної теорії можна застосовувати не тільки в тих областях захисту інформації, що безпосередньо залежать від погодних факторів. Наприклад, для організації безпеки даних в інформаційній базі використовується комбінація декількох методів і механізмів. Вибір способів захисту інформації в інформаційній базі – складна оптимізаційна задача, при вирішенні якої потрібно враховувати ймовірності різних погроз інформації, вартість реалізації різних способів захисту і наявність різних зацікавлених сторін. У загальному випадку для знаходження оптимального варіанта вирішення такої задачі необхідно використання теорії ігор, зокрема теорії *біматричних ігор з ненульовою сумою* [4], яка б дозволила вибрати таку сукупність засобів захисту, яка б забезпечувала б максимізацію ступеня безпеки інформації при заданих витратах, чи мінімізацію витрат при заданому рівні безпеки інформації.

Список літератури

1. Чибиров М.О. Об одной проблеме, возникающей при использовании теории игр в области защиты информации [Электронный ресурс] // Проблемы информационной безопасности в системе высшей школы. Московский инженерно-физический институт (государственный университет). – Режим доступа: http://library.mephi.ru/data/scientific-sessions/2005/vnpk/0-1-43.doc. – Заголовок с экрана.

2. Мельников Ю, Теренин А. Возможности нападения на информационные системы банка из Интернета и некоторые способы отражения этих атак [Электронный ресурс] // Банковские технологии. – 2007 – № 2 – Режим доступа: http://www.cryptography.ru. – Заголовок с экрана.

3. Шапкин А.С., Мазаев Н.П. Математические методы и модели исследования операций: Учебник. – М.: Издательско-торговая корпорация «Дашков и К^0», 2004. – 400 с.

4. Проектирование системы защиты данных в информационной базе [Электронный ресурс] // Режим доступа: http://www.kgau.ru/istiki/umk/pis/l26.htm. – Заголовок с экрана.

Надійшла 14.02.2008р.

УДК 537.87: 621.371

А.А.Стрельницкий,
А.Е.Стрельницкий, А.И.Цопа, В.М. Шокало

ВАРИАНТ МОДЕЛИ ЗАТУХАНИЯ ШИРОКОПОЛОСНОГО СИГНАЛА В РАДИОЛИНИИ ПРИ РАСЧЕТЕ ЗАЩИЩЕННОСТИ ЛОКАЛЬНОЙ СЕТИ СВЯЗИ

Введение

В период развития аналоговых систем связи модели распространения радиоволн (РРВ) все время усложнялись в связи с необходимостью более точного учета влияния многолучевости при расчете защищенности систем связи. В итоге это привело к огромным вычислительным затратам при расчетах радиолиний. В современных цифровых системах передачи информации (ЦСПИ) используются широкополосные сигналы. За счет этого в них достигается более слабая чувствительность к замираниям в условиях многолучевого приема, чем в аналоговых системах связи [1]. Это обстоятельство дает право сделать допущение о возможности использования упрощенных моделей расчета ослабления радиоволн в радиолиниях ЦСПИ.

Влияние отражающих поверхностей рассмотрено во многих работах по распространению радиоволн для случая дальней зоны, когда от точки передачи в точку приема лучи приходят параллельно. Особенность локальных ЦСПИ состоит в том, что зачастую передача