УДК 004.621.3

С.Ж. Піскун[1]

[1]Інституту спеціального зв'язку та захисту інформації НТУУ "КПІ", м. Київ

ОБҐРУНТУВАННЯ ТА ВИЗНАЧЕННЯ НЕОБХІДНОГО РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ СФЕРИ ДЕРЖАВИ

У статті визначені пріоритети у формуванні поліпшення забезпечення безпеки інформаційної сфери держави. На основі цього сформульовані та обґрунтовані методичні основи забезпечення безпеки у будь-який конкретній ситуації при атаці на інформаційну сферу держави.

Ключові слова: захист інформації, системи захисту інформації, засоби контролю, системи технічного захисту об'єктів.

Вступ

Заходи, спрямовані на підвищення інформаційної безпеки, як правило мають комплексний фактор, оскільки охоплюють одночасно політичну, воєнну, економічну, соціальну та інші сфери діяльності держави. При цьому кожна конкретна ситуація потребує своїх пріоритетів у формуванні політики забезпечення безпеки інформаційної сфери держави. Визначення цих пріоритетів є складним і відповідальним завданням державної політики, оскільки помилки, здатні привести до безрезультатності зусиль забезпечення воєнної безпеки держави. Вихідні аксіоматичні положення, на основі яких доцільно вирішувати це завдання, можна визначити наступними так:

визначення основних напрямів забезпечення безпеки інформаційної сфери держави має здійснюватися в інтересах найбільшої ефективності заходів, що вживаються, при мінімальних витратах часових, фінансових матеріальних і людських ресурсів;

заходи, спрямовані на протидію атаці на інформаційну сферу (інформацію, знаходиться у ній) та на підготовку до її відбиття.

Магістральними шляхами забезпечення безпеки інформаційної сфери держави є відвернення впливу на інформацію, протидія впливу на інформацію або відбиття можливої атаки на кожному з цих шляхів відповідними зусиллями створюються необхідні передумови для того, щоб втручання на відбулося або хоча б не призвело до тяжких наслідків.

Основна частина

Проведений аналіз стану безпеки інформаційної сфери України дає змогу прийти до розробки методичних основ обґрунтування пріоритетних заходів щодо забезпечення безпеки у будь-якій конкретній ситуації. Вихідними даними для вирішення цього завдання є:

досягнутий рівень безпеки інформаційної сфери держави;

кількісні показники стану міждержавних відносин в інформаційній сфері та величини, що їх визначають;

приріст індексу безпеки інформаційної сфери держави, необхідний для приведення його до такого значення, яке відповідає потрібному рівню інформаційної безпеки;

перелік можливих заходів в області відвернення потенційного інформаційного впливу або підготовки до його відбиття із зазначенням у тій або іншій формі необхідних для їх здійснення витрат часу, фінансових, матеріальних та людських ресурсів.

Після підготовки необхідних вихідних даних порядок обґрунтування пріоритетних заходів щодо забезпечення інформаційної сфери держави може бути таким.

1. Визначаються прирости індексу безпеки інформаційної сфери держави для кожного з можливих заходів, спрямованих на підвищення рівня інформаційної безпеки, за формулою:

$$\Delta P_{ІБ}^{i} = P_{ІБ}^{i} - P_{ІБ}^{t} \tag{1}$$

де $\Delta P_{ІБ}^{i}$ - приріст індексу безпеки інформаційної сфери для і-го заходу, стосовно наперед складного переліку;

$P_{ІБ}^{i}$ - нове значення індексу безпеки інформаційної сфери, одержане за умов виконання і-го заходу;

$P_{ІБ}^{t}$ - поточне значення індексу безпеки інформаційної сфери (до виконання і-го заходу).

Одержаний ряд приростів безпеки інформаційної сфери держави дає змогу після його ранжування за абсолютною величенною виділити заходи, здійснення яких надаватиме найбільший ефект, щодо підвищення рівня інформаційної безпеки.

2. Визначаються коефіцієнти переваги для кожного і-го заходу за формулою:

$$K_{4}^{i} = \frac{\Delta P_{ІБ}^{i}}{R_i} \tag{2}$$

$$K_{t}^{i} = \frac{\Delta P_{ІБ}^{i}}{T_i} \tag{3}$$

$$K_{4t}^{i} = \frac{\Delta P_{ІБ}^{i}}{R_i + T_i} \tag{4}$$

де K_{4}^{i} - коефіцієнт переваги і-го заходу за критерієм матеріальних і фінансових витрат;

K_{t}^{i} - коефіцієнт переваги і-го заходу за критерієм часових витрат;

K_{4t}^{i} - коефіцієнт переваги і-го заходу за критерієм загальних, виличночасових витрат;

R_i - приведений до тієї або іншої умовної шкали рівень необхідних витрат часу для реалізації і-го заходу;

T_i - приведений до тієї або іншої умовної шкали рівень необхідних витрат часу для реалізації і-го заходу.

3. Найбільш складним і відповідальним є етап прийняття рішення щодо заходів, які слід планувати і використовувати в першу чергу. Для обґрунтування такого рішення можуть бути використані такі методичні рекомендації:

- за умов критичного рівня безпеки інформаційної сфери держави на перший план виходить принцип “безпека будь-якою ціною”. У цьому випадку поперше черговими слід вважати ті заходи, які дають змогу в найкоротший термін добитися помітного або

радикального покращення ситуації, тобто заходи, для яких коефіцієнт переваги за критерієм часових витрат (K_t^i) є найбільшим;

- за умов підвищення рівня безпеки інформаційної сфери держави доцільно здійснювати вибір першочергових заходів, виходячи з значень коефіцієнта переваги за критерієм загальних витрат (K_{4t}^i);

- за умов низького рівня інформаційної небезпеки держави найбільш раціональним буде рішення, прийняте на основі розгляду коефіцієнтів переваги за критерієм матеріальних та фінансових витрат (K_4^i).

4. Після вибору першочергових заходів необхідно, виходячи з умови їх здійснення, розрахувати нове поточне значення індексу безпеки інформаційної сфери держави і уточнити весь комплекс вихідних даних.

5. Визначення подальших заходів, спрямованих на підвищення рівня безпеки інформаційної сфери держави здійснюється встановленим вище порядком на основі уточнених вихідних даних.

Оскільки спілкування інформаційної сфери з навколишнім середовищем здійснюється безпосередньо або через систему захисту об'єктів сфери, то будь яка атака на сферу або систему захисту виражається в дії на них, відповідні атакованим засобам захисту, і моделюється за допомогою зменшення значень діагональних елементів матриці суміжності графа-моделі (вагових коефіцієнтів).

При повному виведені з ладу атакованого засобу відповідальний діагональний елемент матриці суміжності обнуляється. Таке обнулення на матричному рівні еквівалентно відніманню з $\overline{MS}$ позитивно напіввизначеної діагональної матриці, єдиний нульовий елемент, який відповідає валовому коефіцієнту вузла, відповідного до "постраждалого" елементу інформаційної сфері або засобу захисту.

Матриця $\overline{MS}$ по побудові є не негативною і нерозкладною, тобто симетричної перестановками рядків і стовпчиків вона не може бути приведена до вигляду [1].

$$A = \begin{bmatrix} B0 \\ 0C \end{bmatrix} \tag{5}$$

Дійсно, якби таке було можливе то відповідне граф складався би із двох компонентів зв'язності, що не відповідає істині. Виходячи із теореми Фробеніуса [2], матриця з такими властивостями завжди має позитивне λ_{max}, яке являється коренем пряжності 1 характерного рівня, а модулі усіх інших елементів сфери не перевищувати λ_{max}. Якщо зіставити це немою 2, то звідси безпосередньо буде витікати, що навіть при можливому перехрещенні кіл Чернегоріна $\overline{B(m_{11},0)}$ і $\overline{B(m_{22},R_2)}$ після збільшення їх радіусів за рахунок введення зв'язку <1,2>, ми не отримаємо пряжності максимального захисту. Система захисту λ_{max} відповідає власному значенню, всі координати якому відзначенні від нуля і одного знаку. Крім того із початкового результату Вейля про монотонність, якщо $\overline{MS} = \overline{\overline{MS}} + \gamma$, де γ і $\overline{\overline{MS}}$ – симетричні матриці, при чому γ – позитивно полувизначена, то захист матриці $\overline{\overline{MS}}$ не перевертають відповідні засоби захисту $\overline{MS}$.

Зі сказаного витікає, що результатом будь якої атаки, що виводить з ладу деякий засіб захисту або елемент сфери, буде цілком певне обурення системи захисту (СЗ) матриці $\overline{MS}$: вони не збільшаться. Через це формальним проявом відповіді інформаційної сфери на атаку повинно стати не менше СЗ обуренної матриці $\overline{MS}$. Цього можна добитися відповідно до "постраждалої" $\overline{MS}$ діагональної матриці з непозитивними елемен-

тами (позитивно напіввизначеною), що відповідає збільшенню вагових коефіцієнтів для деяких вузлів, тобто збільшенню реальної цінності для роботи сукопної системи деяких із засобів захисту або елементів сфери, що залишилися незайманими. Визначимо, якою повинна бути необхідна відповідь на атаку.

Через властивості матриці $\overline{MS}$ усі її СЗ позитивні. Обнулення діагонального елементу, що відбувається при моделюванні атаки, відповідно до теореми 1 приведе до того, що найменше обурення матриці $\overline{MS}$ стане негативним.

Для оцінки чутливості інформації має сенс аналізувати атаку більше на власний вектор при атаці на інформацію матриці основного повідомлення.

Теорема 1. Достатньою умовою забезпечення малої чутливості інформації до інформаційної атаки є відповідна атака при атаці на інформацію основного повідомлення власних векторів його матриці А власним значенням матриці, що мають великі абсолютні віддаленості.

Доведення. При атаці на інформацію деякі власні вектори матриці А основного повідомлення отримають атаку, відхилившись від первинного положення на деякі кути.

Це відбудеться завжди, якщо тільки алгоритм перетворення додаткової інформації не базується на безпосередній модифікації лише власного значення матриці основного повідомлення. Сукупність атак власного вектора є уявленням для додаткової інформації. Таким чином, чутливість отримання інформації визначається чутливістю атак при атаці на інформацію власного вектора матриці А. Очевидно, щоб зберегти незмінною по перетворенню додаткову інформацію при атакуючих діях на інформацію, відключення власного вектора, що виникають в результаті атаки на інформацію, повинні залишатися незмінними.

Нормальне спектральне розкладання матриці інформації $\bar{A}$ у відповідності з [2] $F = U\Lambda U^T$ представляється у вигляді: $\bar{A} = \overline{U\Lambda U^T}$ нехай Е матриця атак $\bar{A}$. Тоді нормальне спектральне розкладання симетричної матриці $\bar{A} + E$ визначається як $\bar{A} + E = \overline{U\Lambda U^T}$. Нехай $\overline{u_i}$, $\overline{\overline{u_j}}$, які відповідають і-му захисту, θ_i - кут між ними. У відповідності з [2]

$$SinU_i \le \frac{2\left\|\Delta A\right\|_2}{gap_{abs}(i, A)}$$

де власний вектор, отримав атаку при атаці на інформацію, а значить і інформації в цілому буде нечутливий і інформаційна атака, якщо відповідні власні значення матриці $\bar{A}$ мають великі абсолютні значення, причому чим більше, тим менше чутливим до атак буде відповідний власному вектору.

З цього витикає теорема 2.

Теорема 2. Нехай матриця $\overline{MS}$ отримана з симетричної і позитивної певної матриці Т шляхом обнуління довільного єдиного діагонального елементу. Тоді інерція матриці $\overline{MS}$ визначається як (n-1, 1, 0).

Доведення. Аналогічно доведення теореми [2], тільки нулевий елемент шляхом перестановок (подібних перетворень) виводяться на місце (n, n).

Тема 1. Нехай матриця $\overline{MS}$ отримана з симетричної та позитивно визначеної матриці Т шляхом обнулення елементу, що стоїть на місці (n, n) тобто $\overline{m_{nn}} = 0$. Тоді іне-

рція [2] матриці $\overline{MS}$ визначається як (n-1, 1, 0), тобто вона матиме точно одне негативне значення.

Доведення. Оскільки матриця T є позитивно визначене, то вона автоматично задовольняє умовам теореми LU – розкладання [3]. Якщо $\overline{MS}^{(k)}$, $T^{(k)}$, $k=\overline{1,n}$ – головні підматриці матриці $\overline{MS}$ і T відповідно, то діагональні елементи U_{kk} верхньої трикутної матриці U для $\overline{MS}$ задовольняють

$$U_{kk}=\frac{\det\overline{MS}^{k}}{\det\overline{MS}^{(k-1)}}=\frac{\det\overline{T}^{(k)}}{\det\overline{T}^{(k-1)}}>0,\quad k=\overline{1,n-1} \tag{6}$$

Кількість негативних елементів в матриці, що отримується при трикутному LU – розкладання матриці, визначає кількість негативних СЗ матриці $\overline{MS}$. Із відношення (6) виходить, що кількість позитивних СЗ в $\overline{MS}$, а з теореми 2 витікає, що мінімальне СЗ $\overline{MS}$ негативне. В силу невиродженності матриці, негативне СЗ єдино.

Слідство 1. Якщо атака на сферу руйнування піддавався єдиний засіб захисту, то це приведе до появи єдиного негативного засобу захисту (мінімальної системи захисту) в матриці суміжності графа – моделі.

Таким чином, необхідна відповідь інформаційної сфери держави на будь яку атаку повинна привести до повернення найменшої СЗ матриці суміжності графа – моделі до вигляду, коли його значення можна буде нехтувати.

Тема 2. Формальне введення інформації в інформаційну сферу держави не зменшить найбільше СЗ MS.

Доведення. Матриця $\overline{MS}$ – не виродження і симетрична з елементами $\overline{m_{i,j}}, i,j=\overline{1,n}$, $\overline{m_{1,2}}\neq m_{1,2}=0$, для інших елементів матриці $\overline{MS}$ і MS, $\overline{m_{ij}}=m_{ij}$. Приведемо у вигляд:

$$\overline{MS}=\begin{bmatrix} HB^{T} \\ BU \end{bmatrix} \tag{7}$$

де $H=H^{T}$ m x m – матриця, СЗ якої $\theta\leq\ldots\leq\theta_m$ ($H=(\overline{m}_{11})$), має єдине значення СЗ $\theta_1=\overline{m}_{11}$; $B=((\overline{m}_{21},0,\ldots,0)^{T})$, а СЗ $\overline{MS}-\overline{\lambda}_1\leq\ldots\leq\overline{\lambda}_n$. Тоді теореми Коші про розділенні: $\overline{\lambda}_j\leq\theta_j\leq\lambda_{j+n-m}$, $\overline{V_j}=\overline{1,m}$ (*).

Перша частина (*) при $m=1, j=1: U_1\leq\overline{\lambda}_n$.

Теорема 3: Якщо хоча б один діагональний елемент не виродженої симетричної матриці А дорівнює нулю, то $\lambda_1<0$.

Доведення. Нехай $a_{kk} = 0,\ k \neq 1$. Нехай $P_{1,k}$ – матриця перестановок [4] ($P_{1,k}$ отримана з одиничної n x n – матриці шляхом перестановки першої і k-ої строки). Для $P_{1,k}$ справедливо співвідношення: $P_{1,k} = P_{1,k}{}^T$ і $P_{1,k}P_{1,k}{}^T = P_{1,k}{}^2 = 1$, тобто $P_{1,k}$ – ортогональна матриця. Нехай $B = P_{1,k}AP_{1,k}$, тобто матриця B отримана із A шляхом подібного перетворення, що не змінює спектр матриці [5], однак перестановки першої і k-ої строк і однойменних стовбців A, є результатом множення зліва і справа на $P_{1,k}$, виведуть нульовий елемент на місце (1,1) в матриці B. З наведеного, мінімальне B, а, значить, і A, негативне.

Висновки

Визначені пріоритети у формуванні поліпшення забезпечення безпеки інформаційної сфери держави. На основі цього сформульовані та обгрунтовані методичні основи забезпечення безпеки у будь-який конкретній ситуації при атаці на інформаційну сферу держави.

Література

1. Расторгуев С.П. Программные методи защиты информации в компьютерах и сетях / Расторгуев С.П. – М.: Агенство “Яхтсмен”, 1993. – 214 с.
2. Кобозева А.А. Анализ информационной безопасности / Кобозева А.А., Хорошко В.А. – К.: Издательство ГУНКТ, 2009. –251 с.
3. Калиткин Н.Н. Численные методы / Калиткин Н.Н. – М.: Наука, 1978. – 512 с.
4. Антушев Г.С. Методы переметрического синтеза сложности систем / Антушев Г.С. – М.: Наука, 1989. – 88 с.
5. Парлетт Б. Симметрическая проблема собственных значений. Численные методы / Парлетт Б. – М.: Мир, 1983. – 384 с.

Надійшла до редколегії 20.01.2013 р.

Рецензент: д.т.н., проф. Хорошко В.О.

Пискун С.Ж.

ОБОСНОВАНИЕ И ОПРЕДЕЛЕНИЕ НЕОБХОДИМОГО УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМЦИОННОЙ СФЕРЫ ГОСУДАРСТВА

В статье определены приоритеты в формировании улучшения обеспечения безопасности информационной сферы государства. На основе этого сформулированы и обоснованы методические основы обеспечения безопасности в любой конкретной ситуации при атаке на информационную сферу государства.

Ключевые слова: защита информации, системы защиты информации, средства контроля, системы технической защиты объектов.

Piskun S.Zh.

BACKGROUND AND DEFINITIONS REQUIRED LEVEL OF SECURITY OF INFORMATION OF STATES

The article defining priorities in shaping improving information security of the state. Based on this methodology formulated and substantiated basis for safety in any particular situation in an attack on the information of the state.

Keywords: information security, information security systems, controls, systems of technical protection facilities.