УДК 004.621.396.1 **Шевченко А.С. (ВІТІ НТУУ «КПІ»)**

МОДЕЛЬ ЗАГРОЗ ДЛЯ ВІДОМЧИХ БЕЗПРОВОДОВИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ В УМОВАХ ІНФОРМАЦІЙНОЇ БОРОТЬБИ ПРИ ВПЛИВІ КОМПЛЕКСУ НАВМИСНИХ АТАК ПОРУШНИКА

Вступ

Інформаційні технології все більше інтегруються у сфери державного управління. Будь-яка атака на інформаційні активи в цих сферах може призвести до тяжких наслідків, паралізувати як ординарні, так і складні системи управління відомчими структурами, спровокувати руйнівні аварії на стратегічних об'єктах [1].

Особливу увагу слід приділити вирішенню проблем інформаційної безпеки в сучасних умовах глобалізації інформаційних процесів, а також в умовах бажання сильних держав досягти інформаційного домінування у світі. Наростання антагоністичного протистояння між конфліктуючими сторонами призводить до застосування ширшого арсеналу засобів та методів боротьби. Протягом останніх двох десятиліть протистояння плавно перейшли в інформаційну сферу. Виникли такі поняття, як «інформаційна боротьба», «інформаційні операції», «інформаційні війни» [2 – 6].

Розвиток концепцій інформаційної боротьби, засобів і методів їх реалізації був обумовлений стрімким розвитком інформаційно-комунікаційних систем (ІКС). Найбільш вразливими ІКС є безпроводові інформаційно-комунікаційні системи (БпІКС). Засоби захисту, які на сьогодні використовуються в БпІКС, не здатні повною мірою забезпечити їх захищеність при комплексному впливі порушників, які реалізують атаки згідно концепції інформаційної боротьби [5, 6]. Відповідно до цього, найбільш актуальними напрямками є оцінка захищеності БпІКС та впровадження механізмів захисту БпІКС, здатних протистояти порушнику в інформаційній боротьбі.

Аналіз останніх публікацій в галузі захисту інформації БпІКС показує, що розвиток механізмів захисту відбувається здебільшого для вищих рівнів моделі взаємодії відкритих систем [7 – 11]. Захист інформації в БпІКС традиційно обумовлений вдосконаленням криптографічних алгоритмів, автентифікації, розмежування доступу. Окремо розглядається радіоелектронна боротьба (РЕБ). В роботі [12] був дещо розширений перелік загроз для інформації БпІКС – введено такі загрози, як перехоплення по технічних каналах витоку інформації (ТКВІ), нав'язування хибної інформації, дезорганізація системи управління ІКС. Але при функціонуванні БпІКС під час інформаційної боротьби множина загроз збільшується.

Постановка завдання

Впровадженню механізмів захисту має передувати оцінка загроз для інформації БпІКС. Завданням цієї роботи є побудова математичної моделі загроз інформації, що передається БпІКС в умовах інформаційної боротьби, у відповідності до результатів отриманих в [13, 14].

В якості обмежень приймається розгляд штучних навмисних атак на перший і другий рівні БпІКС відповідно до моделі OSI. Кратність атак не вище одиниці.

Основна частина

Під інформаційною безпекою в системах безпроводового зв'язку будемо розуміти захищеність інформації, що циркулює в БпІКС, та самої БпІКС від навмисних або ненавмисних дій штучного та природного характеру відповідно, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, зокрема власникам і користувачам інформації і БпІКС.

В сучасних БпІКС основні механізми захисту інформації реалізуються на вищих рівнях моделі взаємодії відкритих систем [7 – 11]. Це пов'язано з швидким розвитком комп'ютерних технологій, мереж, Internet сервісів та ресурсів. Але найбільш вразливими, з точки зору інформаційної безпеки, є перші два рівні БпІКС: фізичний та канальний. Активом в БпІКС, на який направлений атаки порушника, якому він намагається завдати збитків є інформація.

Аналіз загроз інформації БпІКС [13] дав змогу побудувати функціональну модель [15] загроз для інформації в БпІКС в умовах інформаційної боротьби (рис. 1). Інформаційні загрози поділяться, відповідно до критеріїв безпеки [16, 17], на загрози конфіденційності, цілісності та доступності інформації. Крім того, ці загрози можна класифікувати за об'єктами впливу: загрози каналу зв'язку, загрози системам управління та захисту станцій і БпІКС, загрози безпосередньо БпІКС.

Функціонування БпІКС, в умовах відсутності штучних загроз, обумовлюється наявністю лише загроз природнього характеру: адитивних $\xi(t)$ і мультиплікативних $\mu(t)$ завад, часовою затримкою розповсюдження радіохвиль $\tau_з$ (характерна для систем дальнього короткохвильового зв'язку та супутникового зв'язку). Уникнути виникненню цих загроз неможливо. Єдиним виходом для запобігання їх шкідливого впливу є створення систем компенсації та іншого роду технічних рішень, направлених на мінімізацію шкідливого впливу. Впровадження цих технічних рішень здійснюється на етапі проектування засобів зв'язку.

З точки зору інформаційної безпеки більший інтерес представляють штучні навмисні загрози. В умовах інформаційної боротьби порушник вдається до реалізації наступних атак:

- перехоплення радіосигналу;
- придушення радіолінії;
- перехоплення інформації через ТКВІ;
- спотворення інформації;
- проникнення в систему;
- пошкодження системи управління;
- порушення системи захисту інформації;
- деструктивне пошкодження.

Перераховані загрози, максимально відображають можливі атаки порушника інформаційної безпеки БпІКС.

Найбільшу загрозу для БпІКС складає застосування порушником заходів РЕБ. До складових етапів РЕБ відносяться реалізація атак перехоплення радіосигналів та придушення радіолінії [18]. Перехоплення радіосигналу може здійснюватися в довільній точці зони його розповсюдження через канал перехоплення інформації $y(t)$ (рис. 1). Для здійснення перехоплення інформації через радіоканал, необхідно мати обладнання сумісне з тим, що використовується на передавальній стороні – приймач має приймати й обробляти радіосигнали з заданою поляризацією, видом модуляції, завадостійкого кодування, тощо.

Досить важливим аспектом є наявність механізмів захисту: аутентифікації, шифрування радіоінтерфейсів, ідентифікації абонентів. В даному випадку несанкціоноване ознайомлення з інформацією ускладнюється або стає неможливим.

Порушник при здійсненні перехоплення радіосигналів може переслідувати дві цілі: перша – перехоплення радіосигналу для отримання несанкціонованого доступу до інформації, друга – перехоплення радіосигналу з подальшим визначенням його параметрів та характеристик джерела радіовипромінювання (ДРВ). Перший вид атак перехоплення радіосигналів виконує радіорозвідка (РР), другий – радіотехнічна розвідка (РТР).

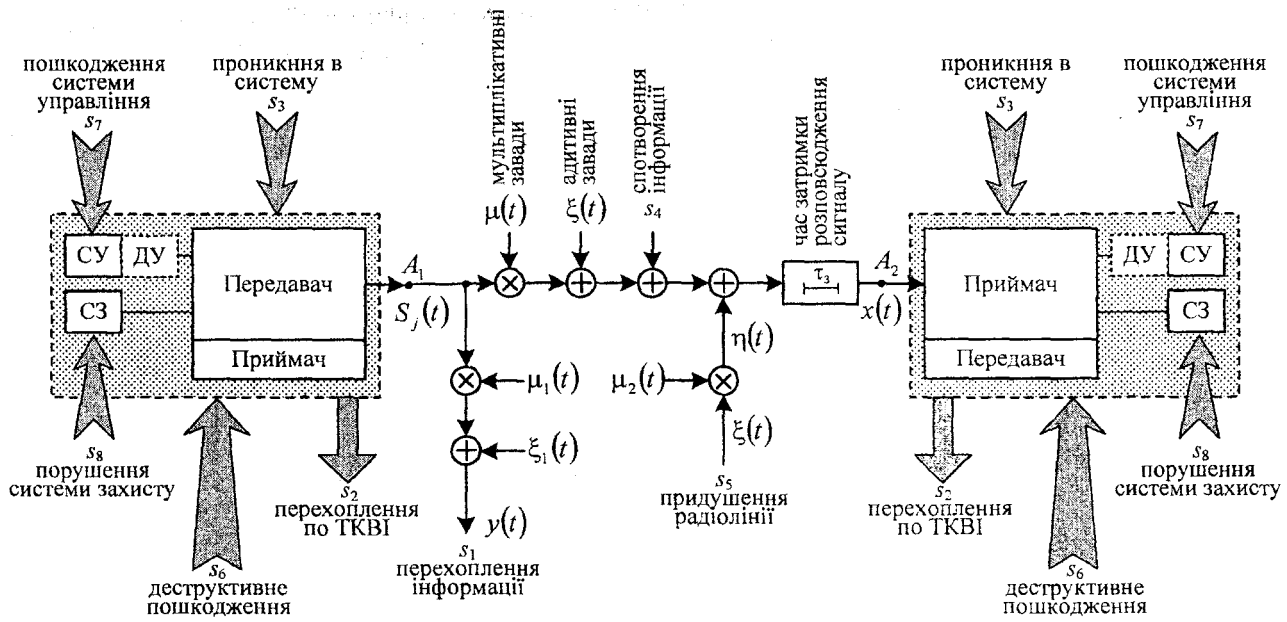

Рис. 1. Функціональна модель загроз інформації БпІКС в умовах інформаційної боротьби

Відповідно до останніх тенденцій [18] функції РР та РТР реалізуються однією станцією радіо/радіотехнічної розвідки (РРТР).

Після визначення параметрів ДРВ здійснюється вибір виду перешкоди та здійснюється придушення радіолінії, через канал придушення $\eta(t)$ [13]. Канал придушення складається з сукупності технічних засобів станції завад, приймального обладнання та середовища розповсюдження між ними.

На канали перехоплення і придушення діють адитивні і мультиплікативні завади. Таким параметром, як час затримки розповсюдження радіосигналу, від передавача до приймача РР та завадового сигналу від передавача станції завад до приймального пристрою кореспондента, можемо знехтувати. Це пов'язано з використанням станцій РРТР та станцій завад на незначній для розповсюдження радіохвиль відстані.

Інформація про ДРВ станціями управління комплексів РЕБ може передаватись для цілевказівки засобів деструктивного враження БпІКС. Тимчасове виведення з ладу, чи ураження БпІКС призводить до унеможливлення передачі ними інформації. Відповідно до цього доступ до інформації обмежується або інформація стає повністю недоступною для користувача.

Наступним видом атак є атаки спотворення інформації (дезінформації). Для її реалізації необхідне комплексне, скоординоване за часом здійснення перехоплення інформації, її аналіз та передача по радіоканалу, під виглядом кореспондента, хибної інформації, чи спотворення службової інформації (зміна заголовку IP пакету, флагів, тощо). Іншим шляхом є підміна передавача кореспондента на передавач порушника – введення хибної станції. В обох випадках до сеансу зв'язку, а відповідно і до інформації, порушник здійснює несанкціонований доступ (НСД).

Попереднім етапом для реалізації певних атак є проникнення в систему – НСД до БпІКС. Після здійснення НСД до БпІКС порушник має можливість здійснювати маніпулювання налаштуваннями станції (обладнання) БпІКС – загроза пошкодження системи управління, порушити систему захисту (відключення шифрування, аутентифікації, алгоритмів перевірки цілісності, тощо) – атака порушення системи захисту, отримує доступ в контрольовану зону для здійснення по перехопленню

інформації через ТКВІ. Сама по собі атака не представляє загрози для нанесення збитку у разі впливу на інформацію, але без її реалізації неможливо здійснити перераховані вище атаки, тому атака проникнення в систему розглядається в комплексі з іншими.

Великий клас атак порушника складає перехоплення інформації через ТКВІ. Порушник після здійснення несанкціонованого доступу до контрольованої зони, в якій розміщена стація БпІКС, може задіяти технічні засоби розвідки як для перехоплення інформації через побічні електромагнітні випромінювання і наведення, так і через візуальні і акустичні канали витоку інформації. Розгляд витоку через радіоканали витоку інформації розглядається в контексті РЕБ.

Функціональна модель загроз відображає лише перелік атак та взаємозв'язок з об'єктами впливу. Для відображення послідовності реалізації атак порушником, взаємозв'язків між етапами реалізації атак, у відповідності до семантичної моделі загроз інформації в БпІКС, побудуємо граф G. Він задається множиною вершин S і відповідностей Г, які показують як між собою пов'язані вершини графа. Граф в цьому випадку записується як $G = (S, Г)$ [19].

Вершинами графа є стани, кожний з яких відповідає спробі реалізації порушником певної атаки на інформацію БпІКС. Позначимо через N множину номерів загроз інформації. Для відображення початкового стану системи введемо стан системи s_0, тобто такий, при якому відсутні загрози інформації БпІКС. Кожний s_i ($i \in N$) стан відповідає спробі реалізації i-ї атаки. У випадку її успішної реалізації здійснюється перехід до наступного стану системи s_j ($j \in N$). При штатному реагуванні системи захисту інформації (СЗІ) здійснюється перехід до стану s_{n+1}, тобто порушник зазнає невдачі при спробі подолати СЗІ («невдача порушника»). Стан s_n є кінцевим і відповідає досягненню порушником мети нанесення збитку.

Дуги графа відображають напрями переходів між станами. Кожна дуга характеризується значенням імовірності переходу між станами системи. Пунктиром позначені дуги, що відповідають можливому переходу зі стану s_i в стан s_{n+1}.

Для відображення СЗІ, та наглядності процесу «атака-захист», в граф G включена множина псевдовершин Z, де кожна псевдовершина $z_i \in Z$ відображає засіб захисту від i-ї загрози, при реалізації атаки зі сторони порушника. Для захисту від i-ї загрози може використовуватись декілька засобів захисту z_i. Нехай їх кількість буде k, тоді множину засобів z_i, які потенційно можуть бути використані для протидії реалізації порушником i-ї загрози ($i = 1, 2, \ldots, n$) представимо як множину K. Множина K є підмножиною Z, тобто $K \subseteq Z$.

На i-у систему захисту може бути направлено декілька атак. Імовірність подолання системи захисту в цьому випадку є сумарною складовою імовірностей подолання. Але варто враховувати стійкість системи захисту. При реалізації однотипних атак, СЗІ може ефективно протистояти їм.

Для відображення однотипних атак, при реалізації деяких загроз, введемо вектор атак $\vec{s}_i$, що об'єднує m атак з множини $M \subseteq N$.

$$\vec{s}_i = \left\{ s_i^{\langle 1 \rangle}, s_i^{\langle 2 \rangle} \ldots, s_i^{\langle m \rangle} \right\},$$

де $s_i^{\langle m \rangle}$ – m-на атака з $\vec{s}_i$ вектору. Відповідно $z_i^{\langle m \rangle}$ є механізмом захисту від m-ї атаки з вектору $\vec{s}_i$.

Для опису взаємних переходів порушника, між етапами реалізації однієї атаки – досягнення успіху та реалізації іншої атаки, тобто перехід від стану s_i, що характеризує попередню атаку, до стану реалізації наступної атаки s_j, розпишемо відповідності $Г\{s_i\}$. Розгляд відповідностей вводиться у звязку з тим, що не зберігається равенство $j=i+1$.

Таким чином, маємо наступні відповідності $\Gamma\{s_i\}$ для кожної з вершин $s_i \in S$ графа $G = (S, \Gamma)$ [19]:

$$\Gamma\{s_0\} = \{s_1, s_2, s_3\};$$
$$\Gamma\{s_1^{(1)}\} = \{s_9 \vee s_{10}\},\ \Gamma\{s_1^{(2)}\} = \{s_4, s_{10}\},\ \Gamma\{s_1^{(3)}\} = \{s_5, s_{10}\},\ \Gamma\{s_1^{(4)}\} = \{s_6^{(1)}, s_{10}\};$$
$$\Gamma\{s_2^{(1)}\} = \{s_6^{(2)}, s_{10}\},\ \Gamma\{s_2^{(2)}\} = \{s_9 \vee s_{10}\},\ \Gamma\{s_2^{(3)}\} = \{s_9 \vee s_{10}\};$$
$$\Gamma\{s_3^{(1)}\} = \{s_2^{(3)}, s_{10}\},\ \Gamma\{s_3^{(2)}\} = \{s_7, s_{10}\},\ \Gamma\{s_3^{(3)}\} = \{s_8, s_{10}\};$$
$$\Gamma\{s_4\} = \Gamma\{s_5\} = \Gamma\{s_6\} = \Gamma\{s_7\} = \Gamma\{s_8\} = \{s_9 \vee s_{10}\};$$
$$\Gamma\{s_9\} = \Gamma\{s_{10}\} = \phi.$$

Таким чином, представляючи кожну загрозу як стан s_i і відобразивши послідовність дії порушника, як переходи між цими вершинами – дуги графа G, отримаємо орієнтований граф, зображений на рис. 2.

Вершини графа G відображають: s_1 – перехоплення радіосигналу; s_2 – перехоплення по ТКВІ; s_3 – проникнення в систему; s_4 – спотворення інформації; s_5 – придушення радіосигналу; s_6 – деструктивна атака; s_7 – порушення системи управління; s_8 – порушення системи захисту; s_9 – досягнення нанесення збитку активам; s_{10} – невдача порушника по нанесенню збитків активам

Приведений граф моделі загроз, відображає багаторубіжну систему захисту. Для досягнення успіху – стану s_n (s_9 відповідно до рис. 2), в нанесенні інформаційним активам збитку, порушнику необхідно подолати всі рубежі захисту. Не здолавши, хоча б один з механізмів захисту, порушник зазнає невдачі – стану s_{n+1} (s_{10} на рис. 2).

При розгляді моделі загроз основним допущенням приймемо те, що порушник реалізовує всі атаки – від s_1 до s_{10}. Кратність атак приймається за одиницю. У разі відсутності механізму захисту імовірність подолання його дорівнює одиниці.

Імовірність знаходження системи в j-му стані, при спробі реалізації порушником мети, визначається наступним чином:

$$P_j = p_i p_{ij},$$

де P_j – імовірність досягнення j-го стану, j – наступний стану реалізації атак порушником, $j \in N$; p_i – імовірність того, що порушник досягнув i-го стану, p_{ij} – імовірність переходу з i-го в j-й стан

Відповідно до цього, імовірність переходу із стану s_i в s_j визначається як:

$$p_{ij} = \rho_i g_{ij}^k,$$

де ρ_i – імовірність реалізації порушником i-ї (поточної) атаки для переходу в j-й (наступний) стан; g_{ij}^k – імовірність подолання i-го захисту при спробі досягнення порушником цілі;
k – кількість засобів захисту для i-ї загрози, $k \in K$.

Успіх подолання засобу захисту визначається вірогідністю g_{ij}^k. Вона залежить від того, як ефективно функціонує система захисту, чи дійсно перекриває вразливості БпІКС, і від того, як технічно оснащений і на скільки кваліфікований порушник [8].

$$g_{ij}^k = \left(1 - e^{-q\omega}\right) \prod_{k \in K} \left(1 - r_{ik}\beta_{ik}\right),$$

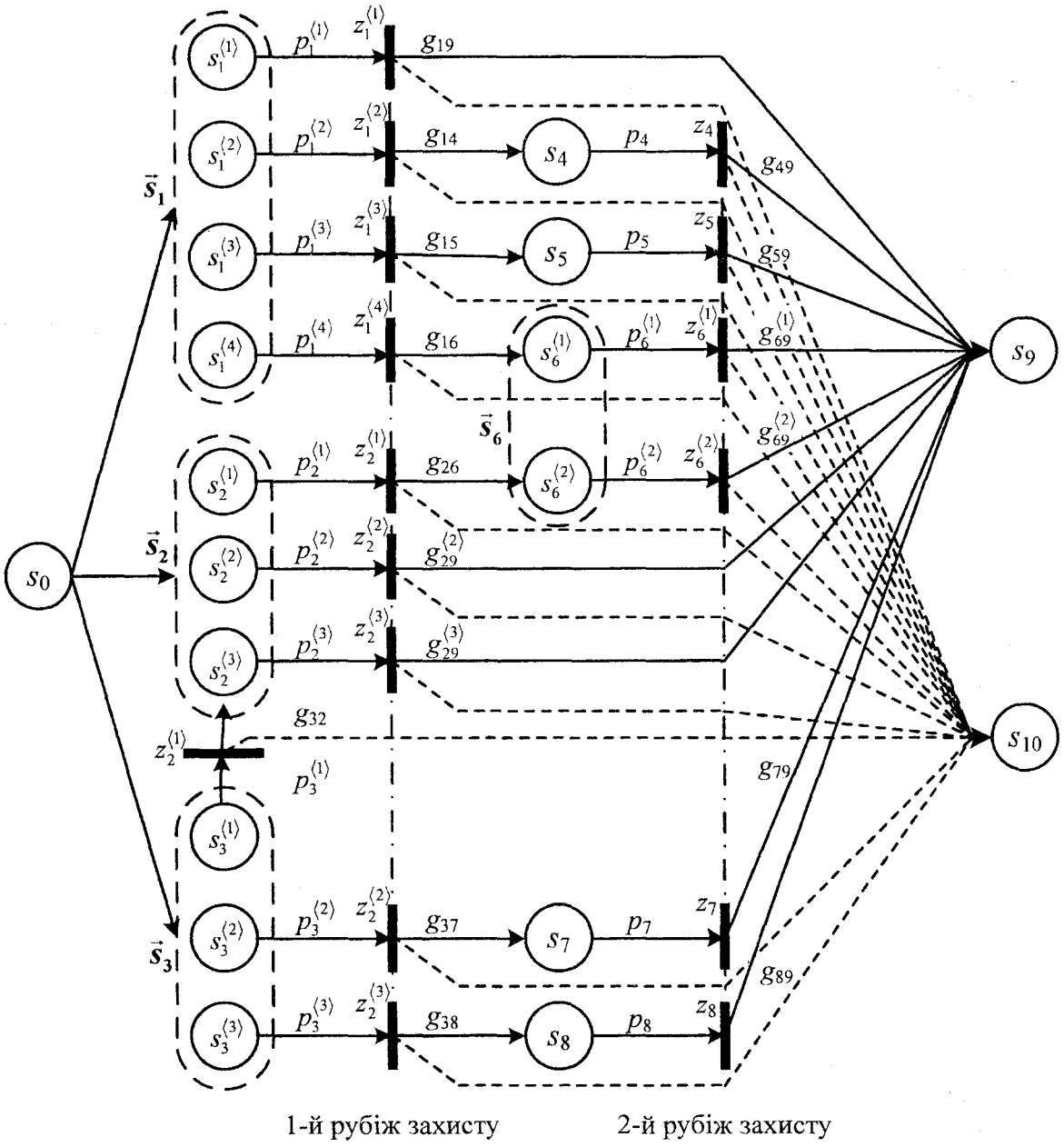

Рис. 2. Граф моделі загроз інформації в БпІКС при дії навмисних атак порушника в умовах інформаційної боротьби

де r_{ik} – імовірність успішного функціонування i-го засобу захисту по протидії реалізації порушником атаки для завдання збитків; q – коефіцієнт технічної оснащеності порушника; ω – рівень кваліфікації порушника при реалізації атаки; $\beta_{ik} = \{0, 1\}$, $\beta_{ik} = 1$, якщо i-й засіб захисту використовується для усунення i-ї загрози, $\beta_{ik} = 0$ – в гіршому випадку.

Момент часу, при якому порушник не здійснив ще жодної атаки – початковий момент, і на графі G представлений як стані s_0. Початковий момент часу характеризується такими значеннями:

$$P_0 = 1;\ P_n = 0;\ P_{n+1} = 0;\ \beta_{ik} = 0, \forall i, k.$$

Сума імовірностей переходу в стани s_n і s_{n+1} є імовірністю повної групи подій, і дорівнює одиниці: $p_n + p_{n+1} = 1$. Тоді імовірність захисту k-ю СЗІ від i-ої загрози (перехід в стан «невдача противника»):

$$p_{i,n+1} = 1 - g_{ij}.$$

Ефективність функціонування СЗІ БпІКС може бути визначена за допомогою наступних параметрів.

1. Середня величина інформаційних збитків в БпІКС від реалізації порушником атак:

$$C^{\text{р}} = \sum_{\substack{j \in N, \\ j \neq 0}} P_j c_j,$$

$$c_i = c_i^1 + c_i^2 + c_i^3 + c_i^4 + c_i^5,$$

де c_i^1, c_i^2, c_i^3 – обсяг збитків від порушення конфіденційності інформації, цілісності, доступності інформації БпІКС; c_i^4 – обсяг збитків від невиконання завдань; c_i^5 – ціна відновлення БпІКС при реалізації порушником i-ї атаки для реалізації власної цілі.

2. Вірогідність реалізації порушником всіх цілей:

$$P^{\text{р}} = \sum_{j=1}^{n} P_j p_{jn}.$$

3. Вірогідність успішної протидії СЗІ діям порушника:

$$P^{\text{з}} = 1 - \sum_{i=1}^{n} P_j p_{jn}.$$

Перший показник дає можливість оцінити ризик нанесення збитку системі. Параметри обсягу втрат визначають збиток, що отримує власник інформації при реалізації інформаційних атак. Другий і третій показники оцінюють порушника і захищеність системи відповідно. Вони взаємопов'язані, що видно з формули (9). Для відображення повної картини функціонування системи захисту БпІКС необхідно розглядати перший та третій показники ефективності системи захисту.

Висновки

Останнім часом велика увага приділяється захисту інформаційно-комунікаційних систем. Але механізми захисту, що впроваджуються, здебільшого орієнтовані на захист інформації на вищих рівнях OSI. В той час, як безпроводові інформаційно-комунікаційні системи стрімко розвиваються, розвиток механізмів захисту цих систем аналогічної тенденції не витримує. Найуразливішими є фізичний та канальний рівні безпроводових інформаційно-комунікаційних систем.

Під час ведення інформаційної боротьби «арсенал» атак порушника збільшується, та постійно модернізується. Відповідно і захищеність безпроводових інформаційно-комунікаційних систем в даних умовах необхідно підвищувати на порядок, особливо тих, що використовуються відомчими структурами.

Новизною представленої моделі загроз інформації безпроводових інформаційно-комунікаційних систем є поєднання найвірогідніших загроз, які можуть виникнути при реалізації порушником атак на перші два рівні безпроводових інформаційно-комунікаційних систем відповідно до концепцій інформаційної боротьби. Кожній атаці відповідає певний механізм захисту, що відображає множина псевдовершин. Це дозволяє більш наглядно відобразити процес «атака-захист». Враховуються і показники можливості реалізації атак порушником, і подолання системи захисту. Модель загроз є уніфікованою і може бути використана для опису конкретної технології БпІКС або системи зв'язку, що включає радіозасоби.

Модель загроз для безпроводових інформаційно-комунікаційних систем дозволяє виділити та оцінити атаки порушників, що створюють ці загрози, дозволить в подальшому оцінки ризики нанесення збитків активам, захищеність безпроводових інформаційно-комунікаційних систем та застосувати ефективні механізми захисту відомчих безпроводові інформаційно-комунікаційні системи , що діють в умовах інформаційної боротьби.

Подальшим завданням є розробка методів оцінки ризиків, створення адекватної системи захисту інформації, яка б перекривала всі вразливості без зменшення продуктивності безпроводові інформаційно-комунікаційні системи .

Список літератури

1. *Данільян О.Г.* Національна безпека України. Сутність, структура та напрямки реалізації / Данільян О.Г., Дзьобань О.П., Панов М.І. – Х.: Фоліо, 2002. – 150 с.
2. *Толубко В.Б.* Інформаційна безпека держави у контексті протидії інформаційним війнам / Навчальний посібник. – Київ.: НАОУ. – 2003. – 332 с.
3. *Міночкін А.І.* Інформаційна боротьба: сучасний стан та досвід підготовки фахівців. – Оборонний вісник, № 2. – 2011. – С. 12 – 14.
4. *Расторгуев С.П.* Информационная война. – М: Радио и связь, 1999. – 416 с.
5. Joint information operations planning handbook. – Virginia, Joint forces staff college national defense university Norfolk, 2003. – 206 p.
6. Information operations primer. – Philadelphia, U.S. Army War College, 2006. – 168 p.
7. *Матов О.Я.* Модель загроз в розподілених мережах / Матов О.Я., Василенко В.С. // Реєстрація, зберігання і оброб. даних. – 2008. – Т. 10, № 1. – С. 91 – 102.
8. *Акиншин Р.Н.* Математические модели, методы и алгоритмы анализа современных телекоммуникационных систем с целью обеспечения защищённости информации: дис. на соискание учёной степени канд. техн. наук: 05.13.19 / Акиншин Русла Николаевич. – Тула, 2005. – 162 с.
9. *Сердюков П.Н.* Защищенные радиосистемы цифровой передачи информации / Сердюков П.Н., Бельчиков А.В., Дронов А.Е. и др. – М.: АСТ, 2006. – 403 с.
10. Защита информации в сетях сотовой подвижной связи / [Максименко В.Н., Афанасьев В.В., Волков Н.В.]; под ред. Макаревича О.Б. – М.: Горячая линия – Телеком, 2007. – 360 с., ил.
11. *Сёмкин С.Н.* Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие / [Сёмкин С.Н., Беляков Е.В., Гребенев С.В., Козачок В.И.]. – М.: Гелио АРВ, 2005. – 192 с.
12. *Коханов Р.П.* Защита информации в системах пакетной радиосвязи на основе управления длительностью сигналов: дис. на соискание учёной степени канд. техн. наук: 05.12.04 / Коханов Роман Павлович. – Воронеж, 2004. – 138 с.
13. *Кокотов О.В.* Загрози інформаційній безпеці систем безпроводового зв'язку в умовах інформаційної боротьби відповідно до критеріїв захищеності інформації / Кокотов О.В., Шевченко А.С. // Збірник наукових праць ВІТІ НТУУ „КПІ". – 2010. – № 1. – С. 35 – 40.
14. *Кокотов О.В.* Модель загроз інформації в системах безпроводового зв'язку в умовах ведення інформаційної війни / Кокотов О.В., Шевченко А.С. // V науково-практичний семінар „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення". – К.: ВІТІ НТУУ„КПІ". – 2009. – С. 140.
15. *Самарский А.А.* Математическое моделирование: Идеи. Методы. Примеры. / Самарский А.А., Михайлов А.П. – [изд. 2-е, исправленное] – М.: ФИЗМАТЛИТ, 2005. – 320 с.
16. Information technology. Security techniques. Information security management systems. Requirements: ISO/ IEC 27001: 2005.
17. *Астахов А.М.* Искусство управления информационными рисками. – М.: ДМК Пресс, 2010. – 312 с., ил.

18. *Борисов В.И.* Помехозащищённость систем радиосвязи. Вероятностно-временной подход / Борисов В.И., Зинчук В.М. – [изд. 2-е, исправленное] – М.: Радио Софт, 2008. – 260 с.

19. *Кристофидес Н.* Теория графов. Алгоритмический подход. – М. Мир, 1978. – 432 с.

Рецензент: Єрохін В.Ф.
Надійшла 24.01.2011

УДК 004.681

Левченко Є. Г., Рабчун А. О. (нац. авіац. унів.)

НЕПЕРЕРВНІ МАРКОВСЬКІ ЛАНЦЮГИ В ЗОБРАЖЕННІ СТАНІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Ми розглянули спроби вилучення інформації як кроки марковського ланцюга з дискретними станами і дискретним часом. В реальних ситуаціях ці спроби можуть здійснюватись не в певні дискретні, а й у будь-які моменти, тобто являють собою марковські випадкові процеси з дискретними станами і неперервним часом, або неперервні марковські ланцюги [2,3]. В цьому випадку стан інформаційної безпеки оцінюється не кількістю кроків, а при заданій інтенсивності потоку подій – часовою залежністю імовірностей переходу системи зі стану в стан. Імовірність $p_i(t)$ знаходження системи в i-му стані в момент t визначається системою диференціальних рівнянь Колмогорова:

$$\frac{dp_i(t)}{dt} = -\sum_{i=1}^{n} \lambda_{ij} p_i(t) + \sum_{j=1}^{n} \lambda_{ij} p_j(t), \quad i = \overline{1,n}, \quad t \geq 0,$$

де i та j - номери станів;

$\lambda_{ij} = \lambda_{ij}(t) = \lim\limits_{\Delta t \to 0} \frac{p_{ij}(t, \Delta t)}{\Delta t}$ - щільність імовірності переходу системи зі стану S_i в стан S_j;

$p_{ij}(t, \Delta t)$ - імовірність переходу системи зі стану S_i в стан S_j.

Розглянемо інформаційну систему, яка складається з трьох однакових об'єктів, захищених чотирма перешкодами, розташованими за послідовно-паралельною схемою (рис.1).

Одна з перешкод є загальною (це може бути периметр території, що охороняється), інші – індивідуальні (окремі приміщення). Кожен з об'єктів містить об'єм інформації g. Через X і Y позначено загальна кількість ресурсів нападу і, відповідно, захисту.

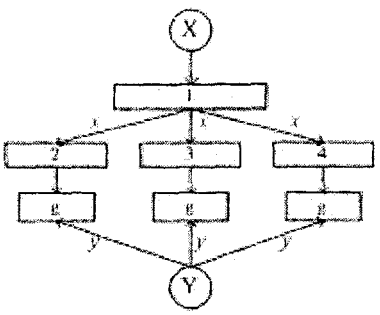

рис. 1

На подолання кожної з перешкод напад виділяє кількість ресурсів x ($X=4x$), на захист кожного з об'єктів – кількість ресурсів y ($Y=3y$).

Вважатимемо, що напади здійснюються послідовно, утворюючи ординарний пуассонівський випадковий потік, який формує неперервний марковський ланцюг. Протистояння відбувається за такою схемою. Напад спрямовується спочатку на першу перешкоду, а після її подолання напади розподіляються рівномірно на подолання всіх інших перешкод. Стани інформаційної системи визначимо наступним чином:

S_1 – вся система непорушна;