Ключові слова: інформаційне протистояння, вразливість, розподіл ресурсів, оптимізація.

Рассмотрена роль двух основных факторов, которые влияют на эффективность разведки: уязвимости объектов и количества ресурсов. В системах с различными значениями уязвимости определи граничные значения ресурсов, при которых целесообразно проводить разведку, оптимальное соотношения между количеством ресурсов, выделяемых на разведку и на утечку информации, и оптимальное распределение ресурсов между отдельными объектами.

Ключевые слова: информационное противостояние, уязвимость, распределение, оптимизация.

The role of two basic factors that influence on reconnaissance efficiency – objects vulnerability and resources number – is considered. In systems with various vulnerabilities the resources extreme number at which the reconnaissance is expedient, optimal correlation between resources number that direct at reconnaissance and at extraction and optimal resources distribution among objects are determined.

Keywords: Information Confrontation, Vulnerability, Resources Distribution, Optimization.

Рецензент:д.т.н., проф Хорошко В.О..
Надійшла:11.01.2011

УДК 004.681.5

Пискун І.В., Скоробогатько О.А., Хорошко В.О.

ОЦІНКА ХАРАКТЕРИСТИК ЗАХИЩЕНОСТІ СИСТЕМ ЗВ'ЯЗКУ

Вступ

Сучасне суспільство не може існувати без інформації. А наявність інформації потребує її захисту. Тому основними задачами забезпечення інформаційної безпеки є:

- виявлення, оцінка та прогнозування джерел загроз інформаційній безпеці;
- розробка державної політики забезпечення інформаційної безпеки та комплексу заходів і механізмів її реалізації;
- створення нормативно-правових засад забезпечення інформаційної безпеки;
- розвиток системи забезпечення інформаційної безпеки, вдосконалення її організації, форм, методів і засобів запобігання загрозам інформаційній безпеці та ліквідації наслідків її порушення.

Основна частина

При розробці систем зв'язку, які забезпечують інформацією різні системи, слід визначити функціональні вимоги до захисту інформації в ній, вимоги щодо гарантування безпеки інформації. При вирішені цих задач дуже важливою є розробка методології оцінки рівня захищеності системи зв'язку з використанням існуючих вимог стандартизації.

Створення та використання за призначенням систем зв'язку(СЗ) передбачає реалізацію ряду організаційних, математичних та інженерних методів забезпечення необхідною рівня безпеки інформації.[1].

СЗ може мати **m** вразливостей, кожна з яких характеризується певною ймовірністю існування $P_{враз/i}$, **i** $\in$ **m**. Реалізація заходів захисту інформації(ЗІ) дозволяє зменшити цю ймовірність до значення:

$$P_{враз\ i}^{(1)}:P_{враз\ i}^{(1)}=P_{враз\ i}(1-P_{зах\ i}), \quad (1)$$

де $P_{зах\ i}$ – імовірність реалізації заходу щодо ЗІ щодо імовірнісної вразливості.

Ризик отримати певні наслідки від впливу імовірнісної загрози на частково захищену систему становить (рис. 1)

Рис.1 Наслідки впливу загроз на СЗ, яка частково захищена

При одночасному впливі **m** загроз ризик отримати наслідки при роботі частково захищеної СЗ становить:

$$P^{(1)}_{риз} = \sum_{i=1}^{m} P_{ризі} = \sum_{i=1}^{m} P_{загі} * P_{вразі}(1 - P_{захі}) \qquad (2)$$

Якщо система по кожній і-тій загрозі не захищена ($P_{зах\ i}=0$), то цей вираз матиме вигляд:

$$P_{риз} = \sum_{i=1}^{m} P_{загрі} * P_{вразі} \qquad (3)$$

Тоді ефективність інформації може бути визначена за допомогою коефіцієнта, який показує, у скільки разів система захисту дозволяє зменшити ймовірність виникнення ризику [2]:

$$K_{зм.риз} = \frac{P_{риз}}{P^{(1)}_{риз}} = \left[\sum_{S=1}^{m} P_{загрі} * P_{вразі} \right] * \left[\sum_{i=1}^{m} P_{загрі} * P_{вразі}(1 - P_{захі}) \right]^{-1} \qquad (4)$$

Ризик отримання економічного збитку від впливу загроз функціонуванню СЗ становить:

$$P^{(1)}_{ек.риз.} = \sum_{i=1}^{m} P_{загрі} * P_{вразі}(1 - P_{зах}) * W_i \ , \qquad (5)$$

де W_i – економічні збитки внаслідок впливу і-ї загрози.

Якщо СЗ може одночасно перебувати під впливом декількох n загроз, то нерідко різні з них можуть призводити майже до однакових наслідків, наприклад, до втрати інформації, яка передається. Імовірність втрати інформації за одночасного впливу n загроз становить:

$$P_{втр} = 1 - A = 1 - \prod_{i=1}^{n} (1 - P_i) \qquad (6)$$

де p_i – імовірність реалізації інформаційної загрози (I Є 1; n); A= імовірність існування(доступність) інформації за одночасного впливу n загроз.

При однакових значеннях ймовірностей реалізації і-тих загроз (p_i=p) вираз (6) матиме вигляд:

$$P_{втр}= 1-(1-P)^n = \sum_{i=1}^{n} C^i{}_n * P^i (-1)^{i-1} \qquad (7)$$

Доступність (наявність) інформації можна розглядати як добуток ймовірностей відсутності і-тих загроз ($P_{ВЗі}$)

$$A= \prod_{i=1}^{n}(1-P_i) = \prod_{i=1}^{n} P_{\hat{A}\hat{C}} \qquad (8)$$

При показникових законах розподілення інтервалів часу між появою загроз, ймовірність появи і-загрози в момент часу t дорівнює:

$$P_{ВЗі}(t) = \exp(-\lambda_i * t), \qquad (9)$$

де λ – інтенсивність появи і-ї загрози.

З урахуванням вимог нормативних документів спостереження ймовірність появи одночасно n загроз в момент t не повинна перевищувати рівень:

$$A(t) = \prod_{i=1}^{n} \exp(-\lambda_i t) = \exp(-\sum_{i=1}^{n} \lambda_i) \geq 0{,}999 \qquad (10)$$

Показник недоступності інформації при одночасному впливі n загроз дорівнює:

$$N(t) = 1-\exp(-\sum_{i=1}^{n} \lambda_i) \qquad (11)$$

За наявності відомих і-тих загроз та ймовірностей їхнього впливу P_i внаслідок існуючих вразливостей СЗ можливе виникнення двох варіантів появи, коли наслідки впливу загроз мають:

- адитивний, взаємно незалежний характер;
- неадитивний характер, при якому наслідки одночасного впливу не є сумою наслідків впливу кожної з загроз у сукупності в усіх станах СЗ.

При можливості появи, наприклад, двох загроз система може перебувати у наступних станах: 0 – загрози відсутні; 1 – існує тільки одна загроза; 2 – існує тільки друга загроза; 3 – існують одночасно обидві загрози.

Реалізація загроз можлива у станах 1, 2 і 3; здійснюється з ймовірностями для цих станів відповідно P_1, P_2 і P_1P_2.

Для першого варіанту за наявності двох загроз за вибраним критерієм вимірювання наслідків для СЗ (W) останні (можливість реалізації загроз) визначаються так:

$$W = W_1P_1 + W_2P_2 + (W_1+W_2)P_1P_2 \qquad (12)$$

Для другого варіанту:

$$W = W_1P_1 + W_2P_2 + W_3P_1P_2, \qquad (13)$$

де $W_3<W_1+W_2$ – ефективність реалізації двох загроз при їх одночасному впливі на роботу вразливої системи.

Зрозуміло, що неадитивна щодо наслідків загроз СЗ більш стійка порівняно з системою адитивною щодо наслідків [3].

Але однаковий рівень ймовірностей $P_i=P$ на практиці зустрічається часто. Тоді при $P_i\neq P$ при наявності, наприклад, двох загроз отримаємо:

$$P_{втр.інф.} = P_1+P_2 - P_1P_2, \tag{14}$$

при наявності трьох загроз:

$$P_{втр.інф.} = P_1+P_2+P_3 - P_1P_2 - P_1P_3 - P_2P_3 + P_1P_2P_3, \tag{15}$$

а при чотирьох загрозах:

$$P_{втр.інф.} = P_1+P_2+P_3+P_4 - P_1P_2 - P_1P_3 - P_1P_4 - P_2P_3 - P_2P_4 - P_3P_4 + P_1P_2P_3 + P_1P_3P_4 + P_2P_3P_4 + P_1P_2P_4 - P_1P_2P_3P_4. \tag{16}$$

При наявності п'яти загроз:

$$P_{втр.інф.} = P_1+P_2+P_3+P_4+P_5 - P_1P_2 - P_1P_3 - P_1P_4 - P_1P_5 - P_2P_3 - P_2P_4 - P_2P_5 - P_3P_4 - P_3P_5 - P_4P_5 + P_1P_2P_3 + P_1P_2P_4 + P_1P_2P_5 + P_1P_3P_4 + P_1P_3P_5 + P_1P_4P_5 + P_2P_3P_4 + P_2P_3P_5 + P_2P_4P_5 + P_3P_4P_5 - P_1P_2P_3P_4 - P_1P_2P_3P_5 - P_2P_3P_4P_5 + P_1P_2P_3P_4 + P_5. \tag{17}$$

При $P_i = P$ ці вирази зводяться до виразу (7).

Вплив дестабілізуючих факторів та загроз не завжди призводить до втрат інформації. Нерідко це призводить до зменшення її цінності.

Якщо, наприклад, без наявності загроз цінність інформації становить величину C_1, то у випадку реалізації двох загроз цінність інформації зменшується до величини:

$$C_{зіб} = \tilde{N}_1(Đ_1\alpha_1 + Đ_2\alpha_2 - Đ_1Đ_2\alpha_{1,2}), \tag{18}$$

де $\alpha_1,\alpha_2,\alpha_{12}$ - коефіцієнт знецінення інформації внаслідок впливу реалізованої першої, другої та обох одночасно загроз відповідно.

Втрачена внаслідок дії двох загроз цінність інформації становить:

$$\Delta C = C_{інф} - C_1 = C_1(1 - P_1\alpha_1 - P_2\alpha_2 + P_1P_2\alpha_{1,2}) \tag{19}$$

При наявності трьох можливих загроз матимемо:

$$C_{інф} = C_1\left|P_1\alpha_1 + P_2\alpha_2 + P_3\alpha_3 - P_1P_2\alpha_{1,2} - P_1P_3\alpha_{1,3} - P_2P_3\alpha_{2,3} + P_1P_2P_3\alpha_{1,2,3}\right|$$

$$\Delta C_1 = C_1(1 - P_1\alpha_1 - P_2\alpha_2 - P_3\alpha_3 + P_1P_2P_{1,2} + P_1P_2P_3\alpha_{1,3} + P_2P_3\alpha_{2,3} - P_1P_2P_3\alpha_{1,2,3}).$$

При наявності n загроз:

$$C_{інф}^{(n)} = C_1\left[1 - \prod_{i=1}^{n}(1 - \alpha_i P_i)\right] \tag{20}$$

Економічна ефективність існуючої системи захисту інформації при цьому може бути визначена так:

$$K_{ефзах} = \frac{C_{інф}}{C_1} = \left[1 - \prod_{i=1}^{n}(1-\alpha_i P)\right] \le 1 \qquad (21)$$

Наявність вразливостей і відповідних загроз може викликати шкоду в роботі СЗ тільки тоді, коли існує потреба в інформації є саме в момент існування загрози. В СЗ іноді існують моменти, коли інформація відсутня. В такому разі поява загрози і втрати чи перекручення інформації не викликає шкоди. У цьому випадку ймовірність втрати інформації повинна визначатися з урахуванням трьох ймовірностей:

$$P_{втрінф} = P_{враз} * P_{загр} * P_{необінф}, \qquad (22)$$

де $P_{необінф}$ - ймовірність того, що загроза з'явиться в момент, коли інформація конче необхідна саме в даний момент.

Розглянемо СЗ, яка може випадково підпадати під вплив загроз і в якій випадково можуть з'явитися вразливості, що сприяють реалізації цих загроз. Будемо вважати надалі що:

- вразливості в СЗ виникають випадково у відповідності з показниковим законом розподілення з параметром λ;
- вразливості які виникають, миттєво починають усуватись обслуговуючим персоналом; час їх усунення випадковий, показниково розподілений з параметром μ;
- система функціонує в умовах загроз, які надходять випадково, і час їх надходження розподілений показниково з параметром q;
- час існування загрози випадковий, розподілений показниково з параметром φ;
- процеси появи вразливостей системи та загроз її функціонуванню взаємно незалежні; усунення вразливостей може здійснюватись незалежно від існування загроз.

Система зв'язку може перебувати у таких станах:

0 – коли загрози не можуть бути реалізовані в наслідок відсутності відповідних вразливостей;

1 – коли загрози можуть бути реалізованими внаслідок існування відповідних вразливостей.

Позначимо $P_0(t), P_1(t)$ відповідно ймовірність перебування системи в момент часу t у стані 0 або 1. Цим станам відповідає система диференціальних рівнянь:

$$P_0'(t) = -qP_{вр}P_0(t) + \varphi P_1(t);$$
$$P_1'(t) = qP_{вр}P_0(t) - \varphi P_1(t)$$

Нормуюча умова має певний вигляд: $P_0(t) + P_1(t) = 1$

Вирішення цих рівнянь у перехідному режимі дає:

$$P_0(t) = \frac{\varphi}{qP_{вр}+\varphi} + \frac{qP_{вр}}{qP_{вр}+\varphi} * e^{-(qP_{вр}+\varphi)};$$

$$P_1(t) = \frac{qP_{вр}}{qP_{вр}+\varphi} - \frac{qP_{вр}}{qP_{вр}+\varphi} * e^{-(qP_{вр}+\varphi)}.$$

У сталому режимі, коли $t \to \infty$, маємо:

$$P_0(t) = \frac{\varphi}{qP_{вр} + \varphi};$$

$$P_1(t) = \frac{qP_{вр}}{qP_{вр} + \varphi.}$$

Якщо в системі вразливостей немає, то $P_{âä} = 0$ і $Ð_0(t) = 1; Ð_1(t) = 0$, а якщо в системі існують вразливості, через які діє кожна з існуючих загроз, то

$$P_{вр} = 1 \text{ і } \quad P_0(t) = \frac{\varphi}{q+\varphi}; P_1(t) = \frac{q}{q+\varphi}.$$

У розглянутому випадку вважаємо, що вразливості системи існують з незмінною у часі ймовірністю. На практиці нерідко виникають ситуації, коли ймовірність існування вразливостей змінюється у часі(найчастіше з часом зростає). Надалі вважаємо, що ця залежність має вигляд:

$$P_{вр}(t) = 1 - e^{-bt},$$

де b – коефіцієнт, який характеризує швидкість зростання ймовірності $P_{âä}(t)$ з часом.

У цьому випадку система рівнянь матиме такий вигляд:

$$P_0'(t) = -q\left(1 - e^{-bt}\right)P_0(t) + \varphi P_1(t)$$
$$P_1'(t) = q\left(1 - e^{-bt}\right)P_0(t) - \varphi P_1(t)$$

Якщо, ймовірність появи вразливості лінійно залежить від часу, тобто при $P_{bp}(t) = a + bt \le 1$, то поведінка СЗ описується такою системою диференціальних рівнянь:

$$P_0'(t) = -q(a + bt)P_0(t) + \varphi P_1(t)$$
$$P_0'(t) = q(a + bt)P_0(t) - \varphi P_1(t)$$

де a,b – коефіцієнти, що характеризують відповідно незалежну та залежну від часу складову ймовірності $Pâð(t)$.

Система може перебувати у таких станах: 0- у системі нема вразливостей, загроз її функціонуванню теж нема;

1- у системі нема вразливостей, але існує загроз, яка в середньому триває час $t_{çàãä} = \frac{1}{\varphi}$;

2 – у системі існує вразливість, яка усувається, але загроз нема;

3 – у системі існує вразливість, яка учувається, існує також загроза її функціонуванню.

На рис. 2 наведено граф переходів СЗ з одного стану в інший, якому відповідає наступна система диференційних рівнянь:

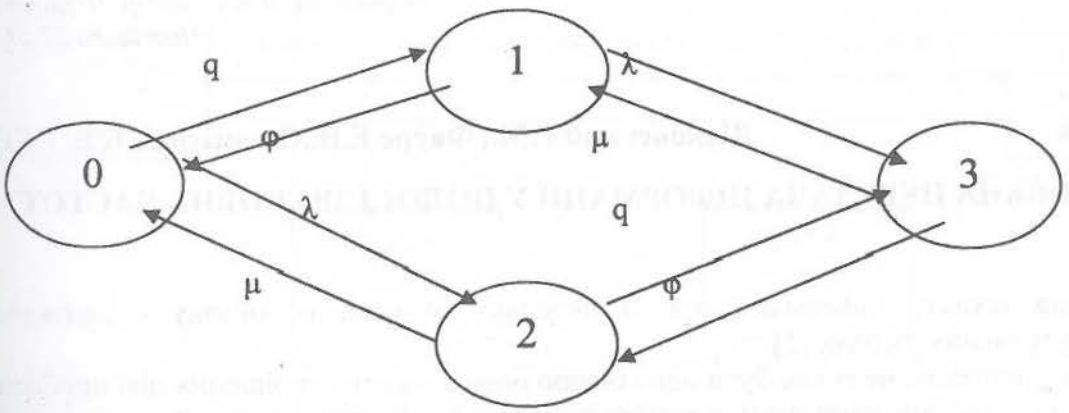
$$\begin{aligned} P_0'(t) &= -(\lambda+q)P_0(t)+\varphi P_1(t)+\mu P_2(t) \\ P_1'(t) &= qP_0(t)-(\lambda+\varphi)P_1(t)+\mu P_3(t) \\ P_2'(t) &= \lambda P_0(t)-(q+\mu)P_2(t)+\varphi P_3(t) \\ P_3'(t) &= \lambda P_1(t)+qP_2(t)-(\mu+\varphi)P_3(t) \end{aligned}, \qquad (23)$$

де $P_i(t)$ - ймовірність перебування інформаційної системи в і-тому стані на момент часу t.

Нормуюча умова має вигляд: $\sum_{i=1}^{3} P_i(t) = 1$ (24)

Вирішення системи рівнянь (23) разом з (24) у сталому режимі (при $t \to \infty$) дозволяє отримати ймовірності перебування системи у станах P_i:

$$P_0 = \frac{\mu\varphi}{(\lambda+\mu)(q+\varphi)}; P_1 = \frac{\mu q}{(\lambda+\mu)(q+\varphi)}; P_2 = \frac{\lambda\varphi}{(\lambda+\mu)(q+\varphi)}; P_3 = \frac{\lambda q}{(\lambda+\mu)(q+\varphi)} \qquad (25)$$



Звідси отримаємо:

- ймовірність того, що СЗ нормально функціонує навіть при наявності загроз:

$$P_{і.д.} = \sum_{i=0}^{2} P_i = \frac{\lambda\varphi+\mu(q+\varphi)}{(\lambda+\mu)(q+\varphi)}; \qquad (26)$$

- ймовірність реалізації загрози:

$$P_{втр.інф} = P_3 = \frac{\lambda q}{(\lambda+\mu)(q+\varphi)}.$$

Цей вираз ілюструє ймовірність реалізації загрози у вигляді втрати інформації в ряді появи цієї загрози в момент існування відповідної вразливості системи.

Висновки

Несанкціоноване втручення в роботу системи зв'язку може здійснюватись з метою порушень процесу її функціонування. Розглянуті в роботі питання направлені не тільки на вирішення проблеми інформації залежності системи зв'язку, але і на те, щоб звернути увагу на актуальність і важливість, залучити для її вирішування якомога більшу кількість фахівців та визначити основні напрямки робіт в цьому напрямку.

Література

1. Биковцев І.С. – Захист інформації в системі організації повітряного руху/ Биковцев І.С., Дем'янчук В.С., Клименко В.О., Дорошко В.О. та інші. – К.:ДП ОПР України, 2008. – 236 с.
2. Невойт Л.В. – Практичні аспекти забезпечення інформаційної безпеки/ Невойт Л.В., Дорошко В.О., Чередниченко В.С.// Сучасний захист інформації, №2, 2010. – с. 4-9.
3. Петров А.А. – Оценка эффективности комплексной системы защиты информации в сетях общею пользования/ Петров А.А., Хорошко В.А.// Збір.наук.праць ВІКНУ ім. Т. Шевченка, Вип. № 21, 2009. – с. 128-131.

В даній статі розглянуті питання направлені на вирішення проблеми інформації залежності системи зв'язку, та зроблена спроба оцінки характеристик захищеності системи зв'язку.

В данной статье рассмотренные вопросы направленные на решение проблемы информации зависимости системы связи, и сделанная попытка оценки характеристик защищенности системы связи.

In this article the considered questions the problems of information of dependence of communication network, and done attempt of estimation of descriptions of protected of communication network, directed on a decision.

Рецензент: д.т.н., проф. Шелест М.Є.
Надійшла 27.01.2011

УДК 621.396

Дідковський Р.М., Фауре Е.В.,Олексієнко В.В. (ЧДТУ)

ПРИХОВАНА ПЕРЕДАЧА ІНФОРМАЦІЇ У ПОЛОСІ ЗВУКОВИХ ЧАСТОТ

Вступ

Проблема захисту інформації при її передачі по каналах зв'язку є надзвичайно актуальною в сучасних умовах [1].

Не існує і, напевне, не може бути однозначно оптимального вирішення цієї проблеми. Її різноманітними засобами намагаються вирішувати фахівці багатьох галузей науки і техніки: криптографії [2], стеганографії [3], зв'язку та телекомунікацій [4].

Криптографічні методи не передбачають приховування факту передачі інформації. Їх, як правило використовують у комбінації з іншими методами.

Якщо розглядати методи, що безпосередньо спрямовані на приховування або маскування передачі, то увага багатьох фахівців прикута до двох напрямків: цифрова стеганографія [5] та маскування мовних сигналів [6-7]. В останньому випадку аналоговий мовний сигнал маскується спеціально сформованим (в деяких випадках цифровими методами) псевдошумовим сигналом.

У системі зв'язку, яка запропонована в даній роботі, мовний (або в більш загальному звуковий) та псевдошумовий сигнали міняються ролями. Звуковий сигнал маскує передачу цифрової інформації за допомогою псевдошумового сигналу малої потужності.

До такого рішення підштовхують активні дослідження останніх десятиліть у галузі передачі інформації за допомогою шумоподібних [4], хаотичних [8-9] та істино шумових сигналів [10, 11]. Перевагою таких систем є їх здатність працювати «під шумом». Однак, на шляху використання методів передачі даних, розроблених для систем такого типу, виникає ряд проблем.

Звуковий частотний діапазон, обраний для побудови системи, дозволяє легко здійснювати фіксацію і цифровий аналіз сигналів загальнодоступними мультимедійними засобами. Тому специфічна форма осцилограми і спектру сигналу з стрибкоподібною зміною