УДК 004.681.5

В.О. Хорошко, Ю.Є. Хохлачова, М.П. Тимченко

Національний авіаційний університет, Київ

ОЦІНКА ЗАХИЩЕНОСТІ СИСТЕМ ЗВ'ЯЗКУ

Анотація: Несанкціоноване втручання в роботу системи зв'язку може здійснюватись з метою порушень процесу її функціонування. В роботі розглянуті питання щодо оцінки захищеності систем зв'язку, які направлені не тільки на вирішення проблеми інформаційної 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 цій сфері.

Ключові слова: *системи зв'язку, захищеність систем, оцінка захищеності.*

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 (СЗ), які забезпечують інформацією різні системи, слід визначити функціональні вимоги до захисту інформації (ЗІ) 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 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 $P_{вразі}$, $i \in m$. Реалізація заходів захисту інформації дозволяє зменшити цю ймовірність до значення:

$$P_{вразі}^{(1)} : P_{вразі}^{(1)} = P_{вразі}(1 - P_{захі}), \qquad (1)$$

де $P_{захі}$ – 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-й загрозі не захищена $(P_{захі} = 0)$, 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]:

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

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 $(I \in 1; n)$; A – імовірність існування(доступність) інформації за одночасного впливу n загроз.

При однакових значеннях ймовірностей реалізації і-х 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-х загроз $(P_{взі})$.

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

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-х 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:

$$W = W_1W_2 + W_2P_2 + (W_1 + W_2)P_1P_2. \qquad (12)$$

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:

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

при наявності трьох загроз:

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

а при чотирьох загрозах:

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

При наявності п’яти загроз:

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

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:

$$C_{інф} = C_1(P_1\alpha_1 + P_2\alpha_2 - P_1P_2\alpha_{1,2}), \qquad (18)$$

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:

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

При наявності трьох можливих загроз матимемо:

$$C_{інф} = C_1\left[\begin{array}{l} P_1\alpha_1 + P_2\alpha_2 + P_3\alpha_3 - P_1P_2\alpha_{1,2} - \\ -P_1P_3\alpha_{1,3} - P_2P_3\alpha_{2,3} + P_1P_2P_3\alpha_{1,2,3} \end{array}\right].$$

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

При наявності n загроз:

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

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

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

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:

$$P_{втр.інф} = P_{враз} * P_{загр} * P_{необ.інф}, \qquad (22)$$

де $P_{необ.інф}$ – 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 нема, то $P_{вр} = 0$ і $P_0(t) = 1; P_1(t) = 0$, а якщо в системі існують вразливості, через які діє кожна з існуючих загроз, то

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

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 $P_{вр}(t)$ 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 $P_{вр}(t)$.

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 $t_{загр} = \frac{1}{\varphi}$;

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

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

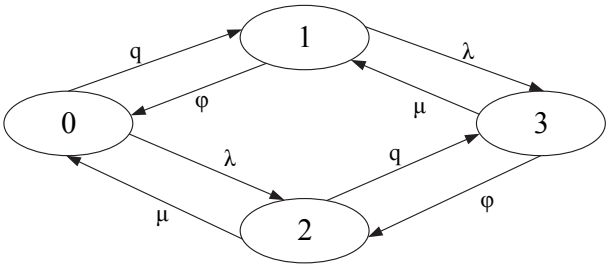

Рис. 2. Граф переходів СЗ з одного стану в інший

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

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

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

Нормуюча умова має вигляд:

$$\sum_{i=1}^{3} P_i(t) = 1. \quad (24)$$

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

$$\begin{aligned} P_0 &= \frac{\mu\varphi}{(\lambda + \mu)(q + \varphi)}; P_1 = \frac{\mu q}{(\lambda + \mu)(q + \varphi)}; \\ P_2 &= \frac{\lambda\varphi}{(\lambda + \mu)(q + \varphi)}; P_3 = \frac{\lambda q}{(\lambda + \mu)(q + \varphi)}. \end{aligned} \quad (25)$$

Звідси отримаємо:

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

$$P_{н.ф.} = \sum_{i=0}^{2} P_i = \frac{\lambda\varphi + \mu(q + \varphi)}{(\lambda + \mu)(q + \varphi)}; \quad (26)$$

– 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 втручання в роботу системи зв'язку може здійснюватись з метою порушень процесу її функціонування. Розглянуті в роботі питання направлені не тільки на вирішення проблеми інформаційної 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 цій сфері.

Список літератури

1. Биковцев І.С. Захист інформації в системі організації повітряного руху / І.С. Биковцев, В.С. Дем'янчук, В.О. Клименко, В.О. Хорошко та інші. – К.: ДП ОПР України, 2008. – 236 с.

2. Невойт Л.В. Практичні аспекти забезпечення інформаційної безпеки / Л.В. Невойт, В.О. Хорошко, В.С. Чередниченко // Сучасний захист інформації. – 2010. – №2. – С. 4-9.

3. Петров А.А. Оценка эффективности комплексной системы защиты информации в сетях общею пользования / А.А. Петров, В.А. Хорошко // Збір.наук.праць ВІКНУ ім. Т. Шевченка. – 2009. – Вип. №21. – С. 128-131.

Надійшла до редколегії 3.03.2017

Рецензент: д-р техн. наук, проф. Г.А. Кучук, НТУ "ХПІ", Харків.

ОЦЕНКА ЗАЩИЩЕННОСТИ СИСТЕМ СВЯЗИ

В.А. Хорошко, Ю.Е. Хохлачева, Н.П. Тимченко

Несанкционированное вмешательство в работу системы связи может осуществляться с целью нарушения процесса ее функционирования. В работе рассмотрены вопросы оценки защищенности систем связи, направленные не только на решение проблемы информационной зависимости системы связи, но и на то, чтобы обратить внимание на актуальность и важность, привлечь для ее решения как можно большее количество специалистов и определить основные направления работ в этой области.

Ключевые слова: *системы связи, защищенность систем, оценка защищенности.*

ESTIMATION OF SECURITY OF COMMUNICATION SYSTEMS

V. Khoroshko, Y. Khokhlacheva, N. Timchenko

Unauthorized intervention in the operation of the communication system can be implemented to disrupt its operation process. The paper deals with evaluation of security communication systems, aimed not only at solving the problem of information depending on the communication system, but also on what to pay attention to the relevance and importance to attract to address it as a lot of experts to determine the main directions of work in this area.

Keywords: *communication systems, security systems, security assessment.*