другому випадку, розглянемо наступну послідовність. Нехай $d_{i-1} \cup Q$ заперечна система. Це означає, що d_{i-1} і q_{i-1} не задовільняють умові взаємозалежності, тобто $\neg(q_{i-1} \leftrightarrow d_{i-1})$. Це в свою чергу означає, що q_{i-1} приводить до протиріччя в $c' = q_{i-1} \cup D$. Проводячи аналогічні міркування по відношенню до d_{i-k} і q_{i-k}, в силу скінченості реалізації p_i інтерфейса J, можна прийти до формули $\varphi(Q)$, яка є цільовою функцією реалізації інтерфейсу J. Але якщо $\varphi(C)$, де $C = (Q \cup D)$ призводить до протиріччя в C, то $\varphi(C)$ вибрана не коректно, що не допустимо при формуванні $\varphi(C)$. Таким чином другий випадок також не може мати місце. Отже формування і реалізація довільного $p_i(d_{i-1}, q_i)$ або $p_j(q_{i-1}, d_i)$ може бути здійснена за рахунок розширень Q і D.

Висновок

Для реалізації інтерфейсу J використовувались Q і D для реалізації P, то реалізація інтерфейсу J також допустима, якщо функція $\varphi(C)$ незаперечна з C.

Література

1. Information Technology Security Evaluation Criteria. Harmonized Criteria of France-Germany-Netherlands-United Kingdom. Department of Trade and Industry. – London. -2001.
2. Кейсрер Г. – Теория моделей / Кейсрер Г., Чэн Ч.Ч. –М.: Мир, 1977. -607 с.

В роботі розглядається моделювання протоколів взаємодії в системах захисту інформації. Визначені параметри адаптації, основними з яких є характеристики і критерії, що задають рівень безпеки об'єкта захисту. Надані підходи щодо побудови універсального інтерфейсу, який задовольняє всім вимогам, що висуваються прикладними системами.

Рецензент:д.т.н., проф. Лєнков С.В.
Надійшла 16.11.2010

УДК 004.056, 004.075 **Дудикевич В.Б., Гарасим Ю.Р.** (НУ «Львівська політехніка»)

МАТЕМАТИЧНА МОДЕЛЬ ОЦІНКИ ЖИВУЧОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ЗА СТАНОМ СИСТЕМИ

Вступ

В сучасних умовах широкої інформатизації суспільства, масового поширення засобів комп'ютерної техніки (які, в свою чергу, з'єднують в локальні, районні, корпоративні, глобальні мережі зв'язку), зростанню злочинних посягань та несанкціонованих дій над інформацією, необхідністю захисту як державної, військової інформації, так і промислової, комерційної, фінансової таємниць проблема захисту інформації стає все більш актуальною.

Системи захисту інформації (СЗІ), які є основним механізмом забезпечення безпеки корпоративних мереж зв'язку (КМЗ) повинні мати властивість живучості [1] для того, щоб функціонувати в «агресивному» середовищі при дії зовнішніх та внутрішніх дестабілізуючих факторів (ДФ). Ця необхідність зумовлена тим, що припинення функціонування СЗІ КМЗ внаслідок дії ДФ призводить до великих економічних, фізичних, інформаційних втрат або катастрофічних наслідків внаслідок реалізації загроз конфіденційності, доступності та цілісності інформації, яка в них функціонує.

Разом із проблемою захисту інформації в КМЗ, які все частіше характеризують гетерогенністю структури, постає ще не до кінця досліджена проблема проектування та експлуатації СЗІ із заданими показниками живучості (survivability), для чого необхідно проводити її оцінку [2, 3]. На цей час завдання оцінки живучості СЗІ КМЗ залишається невирішеним. Вирішення цього завдання дасть змогу проектувати СЗІ КМЗ із заданими показниками живучості, експлуатувати їх в умовах впливу ДФ із гіршими показниками якості функціонування, а також відновлювати їх роботу.

Постановка проблеми

Модель оцінки живучості СЗІ КМЗ за станом системи, яку відносять до класу логіко-ймовірнісних моделей є простим видом моделей живучості. У ній передбачають використання двозначної логіки поведінки елементів і системи захисту в цілому, тобто елементи і система мають лише дві множини станів: працездатні і непрацездатні. Наступним суттєвим припущенням моделі є незалежність подій в системі, що сталися в різні моменти часу. Це дозволяє використовувати опис системи за допомогою статичної моделі, яка не містить час в кількості незалежних змінних. Функціональні ж залежності між змінними можуть бути повністю відображені за допомогою функцій алгебри логіки. Елементи системи є точковими об'єктами, які з'єднані між собою невразливими лініями зв'язку. Вторинні наслідки ДФ відсутні, тому стійкий стан системи відомий безпосередньо після ДФ. Засоби забезпечення живучості контролюють необхідні від'єднання і перемикання в технічній і функціонально-алгоритмічній структурі з тією метою, щоб забезпечити працездатність системи за допомогою працездатних елементів, що залишилися, з врахуванням їх взаємозамінюваності. Інші припущення моделі уточнюватимуться далі.

При описі елементів вважатимемо, що кожен функціональний елемент СЗІ КМЗ може знаходитися в одному з трьох станів: елемент працездатний і включений в роботу; елемент працездатний і від'єднаний від системи захисту через різні причини; елемент непрацездатний. Методика оцінки живучості за станом системи складається із семи етапів: опис станів функціональних елементів (ФЕ); встановлення логічних залежностей між ФЕ СЗІ КМЗ; вирішення систем логічних рівнянь; ймовірнісний опис ФЕ та дестабілізуючих факторів; перетворення функції працездатності до форми переходу до заміщення; запис змішаної форми; визначення показників живучості.

Постановка завдання

Підсумовуючи усе вищесказане в статті пропонується математична модель оцінки живучості системи захисту інформації корпоративної мережі зв'язку за станом системи, що, на відміну від інших [4], дає можливість оцінити виживаність системи захисту при n-кратному впливі дестабілізуючих факторів та використовувати точкову, статичну модель системи без врахування стійкості елементів і вторинних наслідків після впливу дестабілізуючих факторів

Основний матеріал

Нехай існує двополюсна система захисту із N точкових елементів з довільними з'єднаннями між ними і функцією працездатності

$$F = f(X), X = \{x_1, x_2, ..., x_N\}.$$

Система піддається впливу потоку незалежних точкових ДФ з рівноймовірним ураженням кожного функціонального елементу СЗІ КМЗ при появі ДФ, тобто $\varphi_{kj} = 1/N, j = 1, ..., N$. Вважатимемо також, що стійкість елементів дорівнює 0, а інтенсивність ДФ достатня для того, щоб гарантувати перехід в непрацездатний стан елементу, який попав в область дії ДФ. Оцінку живучості проведемо за показниками, що наведено нижче.

Виживаність системи при n-кратному ДФ

$$R_n = 1 - Q(n) = P(F = 1/A_n). \tag{1}$$

Запас живучості (d-живучість)

$$d = C - 1 \tag{2}$$

є критичною кількістю дефектів, зменшене на одиницю. Дефект – це одиниця вимірювання збитку, який наносять системі дестабілізуючі фактори. Це може бути один елемент, який видалений із системи в результаті ДФ, визначена номінальна захищеність чи конфіденційність в системі захисту, яка втрачається для абонентів внаслідок впливу ДФ тощо. Критичною називають мінімальну кількість дефектів, поява яких призводить до втрати працездатності.

Запас живучості (m-живучість)

$$m = \max(i)m_i \tag{3}$$

є максимальною кількістю дефектів, яку ще може витримати система без втрати працездатності.

Середня кількість ДФ, що призводить до втрати працездатності

$$\bar{\omega} = \sum_{n=0} R(n) \tag{4}$$

є математичним сподіванням кількості ДФ, яке задається розподілом

$$Q(n) = P(F = 0/A_n). \tag{5}$$

Середній запас живучості

$$\bar{d} = \bar{\omega} - 1. \tag{6}$$

Ця величина невід'ємна, оскільки $\bar{\omega} \geq 1$. Це випливає із (4), оскільки $R(0) = 1$. Показники (1), (4), (5) та (6) є ймовірнісними, (2) і (3) – детерміновані.

Виживаність системи при n-кратному ДФ можна представити у вигляді

$$R(n) = \sum_{X \in X_1} P(X/A_n) = P(F = 1/A_n), \tag{7}$$

де X_1 – підмножина векторів X, що відповідають працездатним станам системи. Ймовірність $P(X/A_n)$ знаходимо за формулою:

$$P(X/A_n) = \sum_{\bar{n} \in M_n} P(\bar{n})P(X/\bar{n}), \tag{8}$$

де $\bar{n} = (n_1, n_2, ..., n_k)$ – вектор кількості ДФ, що належать k підсистемам, M_n – множина векторів, що задовольняють умові $n_1 + n_2 + ... + n_k = n$. Ймовірність

$$P(\bar{n}) = \frac{n!}{n_1! n_2! ... n_k!} \gamma_1^{n_1} \gamma_1^{n_2} ... \gamma_1^{n_k}, \tag{9}$$

де γ_i – ймовірність того, що i-та підсистема входить в область дії ДФ. В окремих випадках тут може бути $k = N$.

При рівноймовірному ураженні елементів формули (7)–(9) можна уточнити, представивши функцію працездатності у вигляді ортогональної диз'юнктивної нормальної (ОДНФ) форми

$$F = \bigcup_{i=1} Q_i.$$

Запишемо (7) у вигляді

$$R(n) = \sum_{i=1}^{m} P(Q_i = 1/A_n). \quad (10)$$

Для імплікант, які містять $l_i = 0,1,2$ заперечення, можна записати формули в (10) у явному вигляді:

$$P(Q_1 = 1/A_n) = (1 - s_1/N)^n, l_1 = 0, n \geq 1,$$

$$P(Q_i = 1/A_n) = \sum_{j=1}^{n} C_n^{\ j} (1 - s_i/N)^{n-j} / N^j, l_1 = 1, n \geq 1,$$

$$P(Q_i = 1/A_n) = \sum_{k=2}^{n} \sum_{j=1}^{k-1} C_n^{\ j} (1 - s_i/N)^{n-k} / N^{-n}, l_1 = 2, n \geq 2,$$

де s_i – кількість букв в імпліканті Q_i.

Ці формули є окремим випадком (9) при $k = 2$ та різних значеннях n_1 і n_2.

Для випадку рівноймовірного попадання елементів в область впливу ДФ можливим є й інший спосіб обчислення виживаності системи при n-кратному впливі. За базовою структурою S_0 визначають всі можливі працездатні структури $S_i, i = 1,..., N_p$. Тоді:

$$R(n) = \sum_{j=1}^{N_p} r_j(n) / N^n = r_n / N^n,$$

де $r_j(n)$ – кількість випадків, в яких виникає структура S_i при n-кратному ДФ. Цю кількість визначають за формулою

$$r_j(n) = \sum_{(k)} L_{nk} B_{kj},$$

де L_{nk} – кількість перестановок із n елементів k типів, B_{kj} – кількість різних векторів X з k нулями, які приводять до структури S_i. Оскільки параметри d та m із формул (2) і (3) зазвичай невеликі, не виникає жодних ускладнень знайти B_{kj} простим перебором векторів. Максимальна кількість векторів для дослідження дорівнює mN, а практично вона значно менша.

Числа L_{nk} – так звані числа Моргана. Вони пов'язані з числами Стірлінга другого роду співвідношенням

$$L_{nk} = k! S_{nk},$$

де S_{nk} знаходять за допомогою рекурентного відношення

$$S_{nk} = S_{n-1,k-1} + kS_{n-1,k}; S_{nk} = S_{nk} = 0 \text{ при } n < k; S_{nr} = 1.$$

Висновки

Розроблено математичну модель оцінки живучості СЗІ КМЗ за станом системи, що дає можливість оцінити виживаність системи при n-кратному впливі ДФ та дає змогу проектувальникам СЗІ КМЗ використовувати точкову, статичну модель системи захисту без врахування стійкості елементів і вторинних наслідків після впливу ДФ.

Список літератури

1. Гарасим Ю. Р. Поняття живучості системи захисту інформації захищених корпоративних мереж зв'язку / Ю. Р. Гарасим, В. Б. Дудикевич // Тези доповідей III міжнародної науково-практичної конференції «Інформаційна та економічна безпека (INFECO-2010)». – Харків, 2010. – Випуск 3 (84). – С. 107-109.
2. Dudykevych V. Survivable security Systems Analysis / V. Dudykevych, I. Garasym // Computer science and information technologies: Materials of the VIth International scientific and technical conference CSIT 2010. – Lviv : Publishing House Vezha&Co, 2010. – pp. 108-110.
3. Гарасим Ю. Розробка моделі оцінки живучості для систем захисту інформації / Ю. Гарасим // Комп'ютерні науки та інженерія: Матеріали IV Міжнародної конференції молодих вчених CSE-2010. – Львів : Видавництво Львівської політехніки, 2010. – С. 320-321.
4. Дудикевич В. Б. Моделі оцінки живучості систем захисту інформації / В. Б. Дудикевич, Ю. Р. Гарасим // «Обчислювальні методи і системи перетворення інформації»: зб. праць наук. техн. конф., Львів, 7-8 жовтня 2010 р. – Львів : ФМІ НАНУ, 2010. – С. 104-107.

В статті розроблено математичну модель оцінки живучості системи захисту інформації корпоративної мережі зв'язку за станом системи, що, на відміну від інших, дає можливість оцінити виживаність системи захисту при n-кратному впливі дестабілізуючих факторів та використовувати точкову, статичну модель системи без врахування стійкості елементів і вторинних наслідків після впливу дестабілізуючих факторів.

Ключові слова: оцінка живучості, живучість систем захисту інформації, корпоративні мережі зв'язку.

Рецензент:д.т.н., проф. Рибальський О.В.
Надійшла 16.11.2010

УДК 004.621.519 **Браиловский Н.Н., Орленко В.С., Хорошко В.А.** (ГУИКТ)

ФОРМИРОВАНИЕ КОМПЛЕКСНЫХ ПРОГРАММ ПО ЗАЩИТЕ ОБЪЕКТОВ ПРИ НАЛИЧИИ УГРОЗ И РИСКОВ

Введение

При разработке требований и системе защиты информации (СЗИ) следует учитывать возникновения угроз и рисков, анализировать их влияние и на этой основе предусматривать меры по их отражению.

При формировании требований с учетом угроз и рисков возникают следующие задачи:

– Определение количественных характеристик влияния угроз и рисков на эффективность СЗИ;

– Определение количественных показателей относительной эффективности СЗИ при наличии угроз и рисков;

– Распределения ресурсов между отражению угроз и рисков и системой, имеющими созидательную направленность.

Известные методы решения первой задачи предусматривает идентификацию рисков (количественный анализ) [1], а также оценивание вероятностей и размеров возможного ущерба (количественный анализ) [2]. Однако при этом задача оценки эффективности защиты с учетом рисков не решается и остается уделом лица, принимающего решения (ЛПР). Более того, определения ущерба в абсолютном измерении (в денежном выражении) часто невозможно для сложенных СЗИ.

Метод решения задачи относительной эффективности защиты при наличии угроз и рисков естественно разрабатывает на основе методов решения данной задачи без учета этих факторов. Наиболее распространение в настоящие время получили мультикритериальные