УДК 004.056.5(045)

Б. Є. Журиленко, канд. фіз.-мат. наук

ОЦІНЮВАННЯ ДЕГРАДАЦІЇ СТІЙКОСТІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ЧАСІ

НАУ, кафедра засобів захисту інформації, e–mail: KZZI @ nau.edu.ua

Отримано вираз і методику розрахунку для визначення імовірності комплексної системи захисту інформації в часі. Вираз враховує розвиток потужностей проникнення та систем знімання інформації, деградацію стійкості елементів комплексної системи захисту інформації.

Expression and method of calculation are got for determination of complex information defense system time probability. Penetration powers development, information reading systems development, complex information defense system elements firmness degradation are taken info account in expression.

Вступ

Для визначення ступеня і рівня захищеності інформації потрібна побудова моделей або образів, адекватних комплексній системі захисту інформації (КСЗІ) [1; 2]. Визначувані в процесі моделювання значення характеристик захисту мають відповідати значенням, які будуть або можуть бути в процесі функціонування реальної системи захисту.

Теоретично розроблено і практично апробовано вельми представницький арсенал методів моделювання, що дозволяє ефективно вирішувати завдання аналізу і синтезу систем захисту інформації різної природи і архітектури, а також управління процесами їх функціонування.

Аналіз досліджень і публікацій

Проте немає моделей, за допомогою яких можна було б оцінити деградацію стійкості комплексної системи захисту в часі.

Постановка завдання

У процесі створення КСЗІ до її використання системи захисту морально застарівають, і навіть тільки що створені окремі системи захисту в процесі створення КСЗІ і введення її в експлуатацію дещо втрачають свої захисні функції. Крім того, у КСЗІ як складові елементи можуть вмикатися окремі системи захисту, які вже існують деякий час і застосовуються в інших комплексних системах захисту. За цей час вони також теоретично втрачають свої захисні функції, причому тим більше, чим більший термін їх існування і функціонування. Це зв'язано з тим, що за цей час можлива організація великої кількості спроб проникнення через існуючу окрему систему захисту і, як наслідок, менший рівень надійності такої системи. Проте будь-яку з окремих систем захисту в КСЗІ через деякий час можна бути замінити на досконалішу, або в процесі експлуатації в КСЗІ додавати нові додаткові окремі системи захисту. У всіх цих випадках бажано знати, який рівень захисту забезпечує вживана КСЗІ тепер і який буде вона забезпечувати в майбутньому після закінчення деякого часу. Знання рівня захисту в майбутньому дозволить вчасно внести зміни в КСЗІ, щоб забезпечити необхідний наперед визначений рівень захисту і запобігати втратам інформації.

Мета цієї роботи – побудова моделі та методики оцінювання деградації стійкості КСЗІ в часі, яка мала б об'єктивний характер, тобто спиралася б при розрахунках на об'єктивні дані, визначувані з експериментальних досліджень і затверджених відповідною експертною або атестаційною комісією. У моделі має бути враховано розвиток і вдосконалення ресурсів проникнення через складові елементи системи захисту КСЗІ, виникнення нових методів проникнення, а також враховано заміну одних складових елементів захисту на інші, додавання нових окремих складових елементів захисту і визначення рівня КСЗІ на поточний момент і в майбутньому.

Основна частина

Позначимо через "α" феноменологічний параметр, визначуваний з експериментальних досліджень або сертифікаційних висновків експертної комісії під час атестації окремого складового елемента КСЗІ. Феноменологічний параметр "α" визначає час імовірності або термін, протягом якого зловмисник може проникнути через певний елемент системи захисту інформації.

Припустімо, що зловмисник пробує проникнути через елемент системи захисту інформації з деякого моменту часу – $t = 0$, коли ця система захисту починає функціонувати. Позначимо через $p(t)$ імовірність того, що за час t буде проникнення через систему захисту. Імовірність проникнення через елемент захисту з першого кроку буде $p(t+1)$. Аналогічно імовірність того, що з першого кроку проникнення не відбудеться,

$p(t–1)$, тобто буде збережений час і проникнення необхідно починати спочатку.

Позначимо через B_1 подію, яка полягає в тому, що через елемент системи захисту буде проникнення на першому ж кроці. Імовірність цієї події буде становити $P(B_1)$. Через B_2 позначимо подію, яка полягає в тому, що на першому ж кроці не буде проникнення через елемент захисту. Імовірність цієї події – $P(B_2)$. Умовна імовірність події A проникнення через елемент системи захисту в прийнятих позначеннях матиме вигляд:

$$P(A|\ B_1) = p(t+1);$$
$$P(A|\ B_2) = p(t-1).$$

Події B_1 і B_2 утворюють повну систему, оскільки на першому кроці або станеться проникнення через систему захисту, або його не буде.

Очевидно

$$P(B_1) = {}^1/_2,\ P(B_2) = {}^1/_2;$$
$$P(A) = P(A|B_1)\ P(B_1) + P(A|B_2)\ P(B_2) =$$
$$= {}^1/_2\ [\ p(t+1) + p(t-1)\ ].$$

Із формула повної умовної імовірності випливає таке рівняння для імовірності $p(t)$:

$$p(t) = {}^1/_2\ [\ p(t+1) + p(t-1)\ ],$$

за умови, що $1 \le t \le \alpha–1$, а граничні умови $p(0) = 0$, $p(\alpha) = 1$.

Розв'язанням цього рівняння є лінійна функція

$$p(t) = C_1 + C_2\ t,$$

коефіцієнти C_1 і C_2 якої можна визначити з граничних умов. Маємо:

$$p(0) = C_1 + C_2\ 0 = 0;\quad C_1 = 0;$$
$$p(\alpha) = C_2 \bullet \alpha = 1;\quad C_2 = 1/\alpha.$$

Звідси одержуємо остаточний вираз для шуканої імовірності проникнення $p(t)$ через елемент системи захисту інформації:

$$p(t) = t\ /\alpha,\quad \text{якщо } 0 \le t \le \alpha.$$

Розраховуючи захисні властивості елемента системи захисту, необхідно враховувати час з моменту атестації цієї системи до моменту її використання у вибраній КСЗІ. За цей час відбувається деградація стійкості захисних властивостей елемента системи, оскільки цей час може бути використаний для проникнення через цю систему захисту, і, отже, рівень захисних властивостей системи знижується.

Позначимо час від моменту атестації системи до моменту її застосування через t_0.

Якщо не враховувати розвиток методів і потужностей проникнення через систему захисту, то ймовірність проникнення з урахуванням тимчасової деградації захисних властивостей можна записати у вигляді:

$$p(t) = (t_0 + t)/\alpha.$$

У випадку, якщо необхідно враховувати розвиток потужностей засобів проникнення (РПЗП), то їх потрібно враховувати з моменту атестації системи. На підставі статистичних даних можна побудувати залежність РПЗП для цієї системи захисту в часі аж до наступного моменту.

Нехай крива розвитку потужностей засобів проникнення описується функцією $f(t)$. Розкладемо цю функцію в ряд Тейлора в точці t_0 [3] – точці введення системи захисту в експлуатацію. Оскільки імовірність проникнення через систему захисту залежатиме від величини наростання потужностей проникнення $f(t)$ у часі, то, розділивши всі члени ряду Тейлора на перший член розкладання $f(t_0)$, отримаємо вираз для РПЗП:

$$f_{\text{нм}}(t) = 1 + [f'(t_0)/f(t_0)]t + [f''(t_0)/(2!f(t_0))]t^2 + \dots,$$

де $f'(t_0)$, $f''(t_0)$ – перша і друга похідні в точці t_0; $f(t_0)$ – значення функції в точці t_0; t – поточний час після введення системи захисту в експлуатацію.

Таким чином, отримаємо імовірність проникнення через систему захисту інформації з урахуванням розвитку потужностей засобів проникнення через систему захисту:

$$p(t) = [f_{\text{нм}}(t)\ (t_0+t)]/\alpha\ .$$

Очевидно, що точність розрахунку імовірності проникнення з урахуванням зростання потужностей засобів проникнення через систему захисту залежить від кількості членів розкладання в ряд Тейлора, що використовуються для обчислень.

Провівши аналогічні міркування, можна отримати імовірність проникнення через систему захисту інформації з урахуванням модернізації і розвитку засобів і методів проникнення через цю систему захисту

$$p(t) = [f_{\text{рв}}(t)\ f_{\text{нм}}(t)\ (t_0+t)]/\alpha, \qquad (1)$$

де $f_{\text{рв}}(t)$ – функція аналогічна $f_{\text{нм}}(t)$, яка враховує зростання розвитку і модернізації методів несанкціонованого проникнення.

Щоб врахувати імовірність проникнення в майбутньому через систему захисту інформації, необхідно використовувати один з видів апроксимації функцій $f_{\text{рв}}(t)$, $f_{\text{нм}}(t)$ [3; 4] дотепер – t, а потім екстраполювати функції на майбутнє – Δt. У цьому випадку у виразі (1) необхідно t замінити на $t + \Delta t$.

На практиці для підвищення рівня стійкості та надійності системи захисту інформації або об'єкта зазвичай використовують декілька елементарних систем захисту, тобто застосовують комплексну систему захисту інформації. Розглянемо імовірність проникнення через декілька елементарних систем захисту, тобто через КСЗІ.

Припустімо, що в КСЗІ використовують декілька елементарних систем захисту, які було розглянуто вище. Будемо вважати, що проникнення

через КСЗІ походить з події O (повної захищеності) до події A (відсутність всякого захисту) через проміжні події B_1, B_2, B_3, … B_k – проникнення через елементарні системи захисту, де k – кількість вживаних елементарних систем захисту. Позначимо через B_n подію, яка полягає в тому, що зловмисник потрапляє в неї після проникнення через (n–1) елементарний захист. Щоб забезпечити проникнення через КСЗІ, необхідно пройти абсолютно довільним шляхом із стану O в стан A. Події B_1, B_2, B_3, … B_k утворюють повну систему. Очевидно, що ці події рівноймовірні, оскільки зловмисник вибирає проникнення через КСЗІ довільним чином. Звідси:

$$P(B_n) = {}^1/k ,$$

де k – кількість одиночних захистів у КСЗІ.

У цьому випадку умовну імовірність записуємо у вигляді

$$P(A|B_n)\, P(B_n) = p_n(t),$$

де $p_n(t)$ – імовірність проникнення через окрему n систему захисту КСЗІ.

Таким чином, можемо записати імовірність проникнення через КСЗІ у такому вигляді:

$$P_{\text{ВЗ}_{\text{КСЗИ}}}(A) = P(A|B_1)P(B_1) + P(A|B_2)P(B_2) + \ldots + P(A|B_k)\, P(B_k).$$

Або, підставивши відповідні значення, отримаємо

$$P_{\text{ВЗ}_{\text{КСЗИ}}}(t) = [({}^1/k)p_1(t)] + [({}^1/k)p_2(t)] + \ldots + [({}^1/k) \times p_k(t)] = \left(\frac{1}{k}\right) \sum_{n=1}^{k} [f_{\text{рв}_n}(t)\, f_{\text{нм}_n}(t) \frac{(t_{0n} + t)}{\alpha_n}]. \quad (2)$$

Ураховуючи вищевикладене, записуємо вираз, за допомогою якого можна обчислити імовірність стійкості комплексної системи захисту інформації в часі:

$$p_{\text{КСЗИ}}(t) = 1 - P_{\text{ВЗ}_{\text{КСЗИ}}}(t) = 1 - \left(\frac{1}{k}\right) \sum_{n=1}^{k} [f_{\text{рв}_n}(t)\, f_{\text{нм}_n}(t) \frac{(t_{0n} + t)}{\alpha_n}]. \quad (3)$$

З отриманих виразів (2), (3) видно, що якщо відбулося проникнення через якийсь елемент КСЗІ, то його ймовірність $p_n(t) = 1$ і рівень КСЗІ зменшиться на (^{1}/k). У разі проникнення через всі елементи захисту імовірність проникнення буде дорівнювати одиниці, а рівень стійкості КСЗІ – нулю, тобто в цьому випадку за даних елементів захисту в КСЗІ ніякого захисту інформації не буде. У процесі експлуатації можлива заміна однієї складової КСЗІ на іншу, то для обчислення рівня стійкості необхідно у виразі (3) замінити параметри замінюваної системи захисту на параметри вживаної, а при додаванні системи захисту додати параметри нової системи і водночас простежити за відповідністю параметра k, який відповідає за кількість елементарних захистів у КСЗІ. Щоб розрахувати рівень КСЗІ на майбутнє, достатньо у виразі (3) використати один з видів апроксимації функцій $f_{\text{рв}}(t)$, $f_{\text{нм}}(t)$ [3; 4] до теперішнього часу t, а потім екстраполювати функції в майбутній час Δt, і замінити t на $t + \Delta t$.

У процесі експлуатації КСЗІ можлива ситуація, коли зловмисник для зламування n складової системи захисту застосовуватиме m_n систем зламування або методів. Оскільки ці події незалежні, то можна переписати вираз для розрахунку рівня КСЗІ в часі у вигляді:

$$p_{\text{ксзи}}(t) = 1 - \left(\frac{1}{k}\right) \sum_{n=1}^{k} m_n [f_{\text{рв}_n}(t) f_{\text{нм}_n}(t) \frac{(t_{0n} + t)}{\alpha_n}],$$

де m_n – кількість вживаних систем або методів проникнення через n складову системи захисту, що становить КСЗІ.

Висновок

У результаті виконаної роботи можна зробити такі висновки.

Отримано вираз і методику розрахунку для визначення імовірності комплексної системи захисту інформації в часі. Вираз враховує розвиток потужностей проникнення через конкретні системи захисту, розвиток і вдосконалення методів проникнення, деградацію стійкості елементів КСЗІ в часі від моменту їх атестації до моменту застосування. Дає змогу визначити імовірність стійкості КСЗІ тепер, а також розрахувати час, протягом якого забезпечується належний рівень захисту інформації надалі. В отриманому виразі використовуються реальні експериментальні параметри атестації складових систем КСЗІ у часі в явному або неявному вигляді.

Література

1. *Герасименко В. А.* Защита информации в автоматизированных системах обработки данных: В 2 кн. – М.: Энергоатомиздат, 1994. – 576 с.
2. *Домарев В. В.* Безопасность информационных технологий. Системный подход. – К.: ООО ТИД "ДС", 2004. – 992 с.
3. *Курант Р.* Курс дифференциального и интегрального исчисления: В 2 т.: Пер. с нем. и англ. З. Г. Либина, Ю. Л. Рабиновича. – 4-е изд. перераб. и доп. – М.: Изд-во «Наука», Гл. ред. физ.-мат. лит. 1967. – 704 с.

Стаття надійшла до редакції 28.02.07.