геш-код обчислюється як $h=H(M)$. Для попередження можливості попереднього обчислення колізій функції гешування потрібно здійснити заміщення виразу $h = H(M)$ виразом вигляду $h = H(M \| m')$, де m' – ціле число, яке обчислено на основі таємного ключа.

Отже розглянуті спроби зламу зводяться до вирішення задачі дискретного логарифмування в групі точок ЕК. На основі проведеного аналізу криптостійкості запропонованого методу ЦП можна зробити висновок, що метод є достатньо криптостійким.

VI Висновки

Запропоновано метод ЦП на основі математичного апарату ЕК, який дозволив прискорити процес перевірки цифрового підпису за рахунок перенесення операції скалярного добутку великого цілого числа на базову точку ЕК з процедури перевірки цифрового підпису в процедуру формування та введенням в ці процедури додаткових обчислень над великими цілими числами за модулем порядку базової точки.

Здійснено програмну реалізацію запропонованого методу, проведено порівняльний аналіз часу формування/перевірки підпису за даним та відомим методом ЦП. Запропонований метод ЦП має приблизно на 70% більш швидку процедуру перевірки підпису порівняно з відомими методами ЦП на основі ЕК. Це забезпечується за рахунок менш швидкої (на 60 %) процедури формування підпису.

Таким чином, запропонований метод дозволив підвищити швидкість перевірки цифрового підпису порівняно з відомими методами, що в свою чергу, дозволяє вирішувати проблему перевантаження процедури перевірки підпису в задачах, де ця проблема є критичною.

Дослідження криптостійкості запропонованого методу показало, що спроби його зламу зводяться до необхідності вирішення задачі дискретного логарифмування в групі точок ЕК.

Література: ***1.*** *Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. CRC Press, 1996.* ***2.*** *Miller V. S. Use of Elliptic Curves in Cryptography// Advances in Cryptology - Crypto'85. LNCS 218, - 1986, p. 417 - 426.* ***3.*** *Болотов А. А., Машков С. Б., Фролов А. Б., Часовских А. А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. - М.: КомКнига, 2006. - 328 с.* ***4.*** *Бессалов А. В., Телиженко А. Б. Криптосистемы на эллиптических кривых: Учеб. Пособие. – К.: ІОЦ «Видавництво «Політехніка», 2004. – 224 с.: іл.* ***5.*** *Adrian Antipa, Daniel R. L. Brown, Robert P. Gallant, Robert J. Lambert, Rene Struik, Scott Vanstone. "Accelerated Verification of ECDSA Signatures". Certicom Research, Canada, 2005: p. 307-318.* ***6.*** *Пат. EP1306750 JP, МКИ G09C1/00; G06F7/72; G09C1/00; G06F7/60; (IPC1-7): G06F7/72. "Multi-scalar multiplication computation in elliptic curve signature verification": Пат. EP1306750, МКИ G06F7/72F1. // Okeya Katsuyuki (JP) - № EP20020255073; Заявл. 19.07.2002; Опубл. 02. 05. 2003.* ***7.*** *Пат. US2007064932 CA, МКИ H04L9/30; H04L9/28. "Accelerated verification of digital signatures and public keys" // Struik Marinus; Brown Daniel; Vanstone Scott; Gallant Robert; Antipa Adrian; Lambert Robert - №US20060333296. Заявл. 18. 01. 2006; Опубл. 22. 03. 2007.* ***8.*** *ДСТУ 4145-2002. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. - К.: Держстандарт України, 2003. – 94 с.* ***9.*** *Anthony Mulcahy. BorZoi - An Elliptic Curve Cryptography Library // Available at http://dragongate-technologies.com/products.html.*

УДК 681.528.54

ВИКОРИСТАННЯ МАТЕМАТИЧНОГО АПАРАТУ НЕЧІТКИХ МНОЖИН ДЛЯ РОЗРОБКИ МЕТОДІВ, ТЕХНОЛОГІЙ, МОДЕЛЕЙ СИСТЕМ БЕЗПЕКИ ІНФОРМАЦІЇ

Валерій Домарєв
Апарат РНБО України

Анотація: **Викладено питання розроблення методів, технологій, моделей і систем безпеки інформації, які з використанням математичного апарату нечітких множин дозволяють ефективно впроваджувати захищені інформаційні технології.**
Summary: **The subjects of methods, technologies, models and information security systems development are presented, which with the use of mathematical fuzzy sets apparatus allow effective introduction of the protected information technologies.**
Ключові слова: **Методи, технології, моделі систем безпеки інформації.**

Ускладнення технологій обробки інформації (інформаційних технологій – ІТ) призвело до появи нових видів загроз для процесів функціонування комп'ютерних систем. Вкрай актуальною стає проблема пошуку ефективних шляхів адекватної протидії сучасним загрозам в інформаційній сфері.

На відміну від існуючого підходу створення комплексів засобів технічного захисту інформації на окремих об'єктах інформаційної діяльності, сучасні ІТ потребують захисту складних процесів обробки інформації в розподілених ІТ системах. Ця тенденція вимагає дослідження відповідних методів, моделей та систем безпеки інформаційних технологій.

Для захисту ІТ потрібне сумісне використання різних за функціями та складом компонентів безпеки інформації, таких як: заходи, методи, засоби, механізми, процедури захисту та ін. Ці компоненти потребують об'єднання в систему безпеки інформаційних технологій (СБІТ) та встановлення жорстких логічних та функціональних зв'язків між ними. Як показує практика, саме якість зазначених зв'язків визначає рівень ефективності систем безпеки інформації. Тому виникає проблема дослідження та впровадження сучасних підходів та методичного апарату для створення ***систем безпеки інформаційних технологій***.

На відміну від об'єктного підходу до захисту інформації, в розробці СБІТ основну частину складають задачі системного моделювання та аналізу. Це задачі декомпозиції проблеми, побудови системних моделей різного класу, комплексування проектних рішень, розробки вимог до елементів систем захисту, аналізу коректності та ефективності технологічних рішень щодо створення СБІТ [1]. В роботах зі створення СБІТ, як правило, беруть участь десятки фахівців різних напрямків захисту інформації. Це накладає специфічні вимоги стосовно координації, узгодження, взаємодії колективів при розробці та впровадженні захищених інформаційних технологій.

Сучасні стандарти та нормативно-методичні документи системи ТЗІ України не враховують швидких темпів розвитку ІТ та не містять конкретних рекомендацій з формування режиму безпеки ІТ. Водночас з практичної точки зору більш потрібні рекомендації, які дають не строго оптимальні, але досить ефективні рішення щодо захисту інформації.

Питання технічного захисту інформації на об'єктах інформаційної діяльності та в ІТС розглянуто в роботах В. Герасименка, В. Гайковича, В. Тарасенка, та ін. Але, незважаючи на існування великої кількості праць, в яких розглядаються конкретні рішення щодо технічного або криптографічного захисту інформації, практично не досліджені теоретичні підходи до вирішення проблем безпеки інформаційних технологій в розподілених ІТС різної структури, конфігурації та форм власності.

Створення СБІТ має свої характерні властивості, а саме:

- глобальну мету функціонування з багаторівневим, складним комплексом взаємозв'язаних цілей;
- велику кількість функціональних задач, різних за властивостями, що комплексно взаємодіють і складають велику багаторівневу систему;
- складну, багаторівневу організацію матеріальних та інформаційних потоків взаємодії елементів організаційної структури системи;
- алгоритми функціонування і управління системи з багаторівневим характером та складною динамікою.

Процеси створення та впровадження СБІТ характеризуються великим ступенем невизначеності, випадковості, нестабільності, а їх відображення здійснюється системою кількісних і якісних показників, які зазвичай подаються в лінгвістичній, нечітко заданій формі [2]. Тому методи теорії нечітких множин можуть стати найбільш ефективним інструментом для моделювання складних процесів захисту інформації. Можливості апарату нечіткої логіки як основи приблизних розрахунків та рішень визначено в роботах Болдуіна, Циммермана, Мукаидоно, Мідзумото, Бартолена та ін. Основу математичного апарату теорії нечіткості заклав Лотфі Заде, а далі її розвинули у теоретичному і прикладному аспекті О. Алєксєєв, А. Борисов, Д, Дюбуа, А. Кофман, В. Кузьмін, Ю. Мінаєв, С. Орловський, О. Орлов, Д. Поспєлов, А. Прал, О. Ротштейн, Р. Ягер та інші вчені.

Ця тенденція вплинула і на створення відповідних методів, моделей та систем у галузі безпеки інформаційних технологій. Значною мірою це пов'язано з тим, що процеси, які відбуваються в об'єктах дослідження, характеризуються великим ступенем невизначеності, випадковості, нестабільності, впливом різноманітних збурень у часі, а їх відображення здійснюється системою кількісних і якісних показників, які зазвичай подаються в лінгвістичній, нечітко заданій формі.

Обробку параметрів дослідження завдяки нечітким множинам (НМ) можна реалізовувати в числовій формі, а для розв'язання прикладних задач немає потреби детально вивчати моделі цифрових перетворень. Математична точність методів НМ значною мірою залежить від точності формування функцій належності та класифікації в нечітких категоріях. Ці питання теорії нечіткості викладені в роботах П. Норвича, С. Туркмена, В. Овчинникова, Я. Танки та ін.

Нечіткі методи характеризуються використанням лінгвістичних змінних замість числових (чи як доповнення до них), прості відносини описуються за допомогою нечітких висловлень, а більш складні - нечіткими алгоритмами. Відповідні правила дозволяють швидко обробляти складні сполучення, що є важливою перевагою розмитої логіки [3]. Тому моделі реальних систем, побудовані на основі нечіткої математики, характеризуються великою гнучкістю і адекватністю реальному світу, а також порівняно з традиційними моделями швидшим отриманням остаточного результату через специфічну побудову і простоту використовуваних нечітких операцій.

Для формалізації лінгвістичних даних, що характеризують стан безпеки інформації в системі, пропонується використати логіко-лінгвістичний підхід, що базується на поняттях нечіткої і лінгвістичної змінних, які містять параметри, подані не тільки в кількісному, але і в якісному вигляді. При цьому лінгвістичні змінні дозволяють поставити у відповідність якісним значенням певну кількісну інтерпретацію і таким чином формалізувати їх [4].

Запропоновано модель процесу захисту інформації, в якій розглядаються джерела загроз (ДЗ) що генерують сукупність загроз інформаційним технологіям в ІТС; нехай вона буде кінцевою і точною; $i = \overline{1, n}$. Кожна *i*-а загроза характеризується імовірністю появи $\mathrm{P}i_{угр}$ і збитком $\Delta q_i^{угр}$, нанесеним інформаційно-управляючій системі.

Засобами СБІТ виконується функціональна чи часткова компенсація загроз. Основною характеристикою засобів безпеки є імовірність усунення кожної і-ї загрози $\mathrm{P}i_{угр}^{устр}$.

За рахунок функціонування СБІТ забезпечується зменшення збитку *W*, що наноситься ІТС дією загроз. Позначимо загальний відвернений збиток ІТС через $\overline{W}$, а відвернений збиток за рахунок ліквідації впливу і-ї загрози через $\overline{\omega}_i$.

Після введених позначень сформулюємо в загальному виді задачу синтезу безпеки інформації в ІТС. Необхідно вибрати варіант реалізації СБІТ, що забезпечує максимум відверненого збитку від впливу загроз при припустимих витратах на СБІТ.

Формальна постановка задачі має вигляд:

знайти

$$\begin{aligned} \mathrm{T}^0 &= \omega q \max \overline{W}(\mathrm{T}) \\ \mathrm{T}^0 &\in \mathrm{T}^+ \end{aligned} \tag{1}$$

при обмеженні

$$C(\mathrm{T}^0) \le C\partial on, \tag{2}$$

де Т – деякий вектор, що характеризує варіант технічної реалізації СБІТ; T^+, T^0 – припустиме й оптимальне значення вектора Т; *Сдоп* – припустимі витрати на СБІТ.

Для рішення задачі необхідно насамперед сформувати показник якості функціонування СБІТ $\overline{W}$ (Т).

Очевидно, відвернений збиток у загальному вигляді визначається співвідношенням:

$$\overline{W} = F(Pi_{упр}; \Delta qi^{упр}; \mathrm{P}i_{угр}^{устр}; i = \overline{1, n}). \tag{3}$$

Відвернений збиток за рахунок ліквідації впливу її загрози

$$\overline{\omega}_i = \mathrm{P}i_{угр} \bullet \Delta qi^{угр} \bullet \mathrm{P}i_{угр}^{устр}; i = \overline{1, n}. \tag{4}$$

За умови незалежності загроз і адитивності їх наслідків одержуємо

$$\overline{W} = \sum_{i=1}^{n} \mathrm{P}i_{угр} \bullet \Delta qi^{угр} \bullet \mathrm{P}i_{угр}^{устр}. \tag{5}$$

Імовірність появи *i*-ї загрози $Pi_{угр}$ визначається статистично і відповідає відносній частоті її появи

$$\mathrm{P}i_{угр} = \frac{\lambda_i}{\sum_{i=1}^{\lambda} \lambda_i} = \overline{\lambda}_i, \tag{6}$$

де λ_i – частота появи *i*-ї загрози.

Збиток за рахунок реалізації *i*-ї загрози Δq_i може визначатися в абсолютних одиницях: економічних

втратах, тимчасових витратах, обсязі знищеної чи "зіпсованої" інформації і т. д.

Однак, практично це зробити дуже важко, особливо на ранніх етапах проектування СБІТ. Тому доцільно замість абсолютного збитку використовувати відносний збиток, що по суті являє собою ступінь небезпеки *i*-ї загрози для інформаційно-управляючої системи. Ступінь небезпеки може бути визначений експертним шляхом у припущенні, що всі загрози для ІТС складають повну групу повідомлень [3], тобто

$$0 \le \Delta qi \le 1; \sum_{i=1}^{n} \Delta qi = 1 .$$

Найбільш складним питанням є визначення імовірності усунення *i*-й загрози $\mathrm{P}i_{угр}^{устр}$ при проектуванні СБІТ. Зробимо природне допущення, що ця імовірність визначається тим, наскільки повно враховані якісні і кількісні вимоги до СБІТ при їх проектуванні, тобто

$$\mathrm{P}i_{угр}^{устр} = \gamma i(xi1,..,xi\gamma,..,xim), \qquad (7)$$

де $xi\gamma$ – ступінь виконання *i*-й вимоги до СБІТ для усунення її загрози, $i = 1,\overline{n}; \gamma = 1,\overline{m}$.

Таким чином, перевага НМ полягає в можливості описувати та обробляти множини зі змінним ступенем належності без урахування різноманітних комбінацій. З практичного погляду методи НМ допомагають експертам формалізувати свої знання зрозумілою для них мовою.

Отже, розроблення методів, технологій, моделей і систем безпеки інформації, які з використанням математичного апарату нечітких множин дозволяють ефективно впроваджувати захищені інформаційні технології, є актуальним науковим завданням. Дослідження цієї проблеми дозволить визначити методичні шляхи створення ефективних систем безпеки ІТ, які раціонально об'єднують різноманітні за властивостями засоби, заходи і методи захисту інформації.

Література: ***1.*** *Кофман А. Введение в теорию нечетких множеств М.: Радио и связь, 1982 - 432 с.* ***2.*** *Поспелова Д. А. Нечеткие множества в моделях управления и искусственного интелекта - М. :Наука, 1986 - 312 с.* ***3.*** *Борисов А. Н., Алексеев А. В., Меркурьев Г. В. и др. Обработка нечеткой информации в системах принятия решений-М: Радио и связь, 1989 - 304 с.* ***4.*** *Домарев В. В. Безопасность информационных технологий. Системный подход. – К.: ООО ТИД Диа Софт, 2004. – 992 с.*

УДК 681.3.06

БЕЗОПАСНОСТЬ ПАРОЛЬНОЙ ЗАЩИТЫ ПРИ РАЗЛИЧНЫХ МЕТОДАХ ВЗЛОМА

Сергей Емельянов

Международный гуманитарный университет, г. Одесса

Анотація: **Розглянуто основні фактори, що визначають безпеку парольного захисту. Наведено практичні рекомендації щодо посилення парольного захисту як від силового, так і від «інтелектуального» зламу.**

Summary: **Basic factors, which determine safety of password defense, are considered in this article. Practical recommendations are resulted in relation to strengthening of password defense both from power one and from a «intellectual» attack.**

Ключевые слова: **Парольная защита, безопасность пароля, силовой перебор паролей, «интеллектуальный» взлом.**

I Введение

Механизмы парольной защиты (ПЗ) широко используются в компьютерных технологиях в целях предотвращения несанкционированного доступа (НСД) при загрузке операционной системы, открытии различных приложений, доступе к информационным ресурсам, входе в компьютерные сети и др. Поэтому оценка надежности ПЗ и разработка практических рекомендаций по ее усилению являются актуальными задачами [1 – 4]. В немалой степени этому способствует и постоянное совершенствование аппаратно-программного обеспечения и технологий для взлома парольной защиты [5 – 7].

В общем случае вероятность *P* подбора пароля злоумышленником описывается функцией [2]:

$$P = F(m, n, P_1, s(t), T), \qquad (1)$$

где: *m* – размер алфавита, из символов которого может быть составлен пароль;