УДК 681.3, 004.3

В. Глухов
Національний університет “Львівська політехніка”,
кафедра електронних обчислювальних машин

ОЦІНЮВАННЯ ГАРАНТОЗДАТНОСТІ КРИПТОГРАФІЧНИХ КОМП’ЮТЕРНИХ СИСТЕМ

Досліджується питання оцінювання гарантоздатності криптографічних комп’ютерних систем.

The paper describes computer systems dependability measure method.

Вступ

Від комп’ютерних засобів інтегрованих систем керування завжди, крім розв’язання основної задачі керування, вимагалося виконання додаткової вимоги, а саме забезпечення надійності.

Поняття гарантоздатності виросло з поняття надійності і містить як характеристики традиційно надійних систем (власне показники надійності, показники готовності до роботи, характеристики безперервність роботи та інші), так і нові вимоги, які раніше до поняття надійності не входили, зокрема – конфіденційність та цілісність, недоторканність. Для побудови гарантоздатних систем необхідно вміти оцінювати гарантоздатність. Відомі джерела дають визначення гарантоздатності, але не містять методів визначення її величини.

У статті пропонується метод оцінювання гарантоздатності криптографічних комп’ютерних систем, виходячи із визначення гарантоздатності.

Аналіз публікацій і окреслення проблеми

Від комп’ютерних засобів інтегрованих систем керування завжди, крім розв’язання основної задачі керування, вимагалося виконання додаткової вимоги, а саме забезпечення надійності. Вирішенню цього питання присвячена велика кількість робіт, серед них роботи [1–7]. Терміни, якими оперують під час оцінювання надійності, визначені низкою вітчизняних стандартів [8–10].

Термін «надійність» в його сучасному розумінні набуває відтінку «довірчості», тобто мова у цьому випадку йде про «довірчу надійність», що передбачає аспекти безпеки, класичної надійності (reliability), продуктивності і живучості в широкому діапазоні потенційних ризиків і погроз [11].

Концепція довірчої надійності практично збігається з тим, що у багатьох англомовних джерелах, особливо які мають відношення до американського Інституту інженерів з електротехніки й електроніки (IEEE), прийнято називати dependability («функціональна надійність» або «гарантоздатність», що забезпечує отримання достовірних результатів за наявності несправностей).

Основною теоретичною роботою у галузі гарантоздатних систем є [12], де був сформульований принцип “Dependable computing” (гарантоздатних обчислень) як обчислень, стійких до відмов апаратних засобів і програмних засобів, тобто до відмов, обумовленим проявом їх дефектів, внесених при розробленні і не виявлених тестуванням. Тепер визначення гарантоздатності міститься у міжнародних стандартах [13, 14]. Сьогодні теорію гарантоздатних систем, сервісів і технологій розвиває науково-технічний центр DeSSerT (Dependable Systems, Services & Technologies) [15]. Відомі роботи, в яких існуюча концепція гарантоздатності доповнюється положеннями, які ґрунтуються на кібернетичному підході і сінергетиці [16].

Вужче визначають поняття гарантоздатності військові документи [17, 18].

Одним з методів забезпечення конфіденційності гарантоздатних систем є використання електронного цифрового підпису на основі еліптичних кривих. Стійкість нових стандартів електронного цифрового підпису [19, 20] заснована на складності розв’язання задачі дискретного логарифмування в групі точок еліптичної кривої. У ряді робіт [21, 22, 23] наводиться оцінка цієї складності.

Водночас разом з розумінням, якою повинна бути гарантоздатна комп'ютерна система, відсутній як метод оцінювання гарантоздатності загалом, так і метод оцінювання складових частин гарантоздатності, зокрема і конфіденційності, що не дає змоги порівнювати різні варіанти гарантоздатних систем.

Мета роботи

Метою роботи є розроблення методу оцінювання гарантоздатності криптографічних комп'ютерних систем, зокрема систем цифрового підпису, враховуючи відомі і погоджені визначення гарантоздатності і результати обчислення складності зламу алгоритмів цифрового підпису.

Визначення гарантоздатності

Згідно з [17] гарантоздатність визначає рівень сумарного впливу на об'єкт усіх факторів, від яких залежить надійність, ремонтопридатність та зручність обслуговування об'єкта, при якому об'єкт ще працездатний і може виконувати покладені на нього функції у будь-який час після початку виконання цих функцій (під час виконання покладеної на нього місії) за умови, що на початку виконання місії об'єкт був придатний до виконання цих функцій (available). Поняття «під час місії» не містить час поза межами місії, тобто до початку місії і після її закінчення. Таке визначення гарантоздатності істотно відрізняється від визначення, яке наведене у [13, 14].

Згідно з [13] гарантоздатність – це загальний термін, що використовується для опису забезпечення операційної готовності і факторів, які на неї впливають: показників надійності, ремонтопридатності та технічного обслуговування (рис. 1, табл. 1). Тобто, визначення розширюється до загального опису без використання кількісних характеристик. Таке визначення не дає змоги порівнювати різні комп'ютерні системи за параметром гарантоздатності.

Рис. 1. Гарантоздатність сервісу

Придатність [17] визначає рівень сумарного впливу на об'єкт усіх факторів, від яких залежить надійність, ремонтопридатність та зручність обслуговування об'єкта, при якому об'єкт на момент початку місії ще працездатний і може виконувати покладені на нього функції незалежно від часу початку місії.

Доступний час (uptime) [17] – час, протягом якого об'єкт може виконувати покладені на нього функції.

Час простою (downtime) [17] – час, коли об'єкт працює, але не може виконувати покладені на нього функції.

Частка доступного часу [17] – загальна міра придатності і гарантоздатності об'єкта, яка залежить від сумарних наслідків проектування, встановлення, якості, роботи, технічного обслуговування, ремонту і логістичного супроводження об'єкта, а також дії навколишнього середовища.

Ефективність системи [17] – міра можливості системи досягти поставлених перед місією специфічних вимог. Ефективність залежить від готовності системи (або придатності) і успіху місії (або гарантоздатності).

Гарантоздатність пов'язана з надійністю, але гарантоздатність є ширшим поняттям, ніж надійність.

Таблиця 1

Ефективність системи

Складові частини	Придатність	Гарантоздатність	Продуктивність (результативність)
Визначає	Стан об'єкта перед початком місії	Стан об'єкта на протязі місії	Результати місії
Впливають	Надійність,	Ремонтопридатність,	Діапазон,
	ремонтопридатність,	безпечність,	точність,
	зручність обслуговування,	виживаність,	потужність,
	людський фактор,	уразливість	смертність,
	логістика		інше

Як показано у табл. 1, основні характеристики ефективності системи відповідають на запитання «Як часто?» (придатність), «Як довго?» (гарантоздатність) і «Наскільки добре?» (результативність).

Система гарантоздатна, якщо вона (рис. 2, [24]):

доступна (available) – готова для використання, коли це потрібно;

надійна (reliable) – здатна забезпечити безперервність обслуговування під час використання;

безпечна (safe) – не має катастрофічного впливу на оточення;

захищена (secure) – здатна зберегти конфіденційність (confidentity), забезпечувати недоторканність (integrity);

ремонтопридатна (mintainability).

Вужче визначення терміна «Гарантоздатність» [17] визначає часовий інтервал, у середині якого гарантоздатність є критичним фактором, але враховує тільки показники надійності і ремонтопридатності, що не дає можливість врахувати сучасні вимоги до гарантоздатних систем, такі як конфіденційність.

Оцінювання ефективності гарантоздатних систем

Згідно з [18] ефективність системи (*SE*) оцінюється як

$$SE = ADC,$$

де $A = (a_1, a_2, a_3, \ldots, a_i, \ldots a_n)$ – придатність, векторний масив імовірностей знаходження системи у різноманітних станах на початку місії, $\sum_{i=1}^{n} a_i = 1$;

D – гарантоздатність, матриця умовних імовірностей для заданого часового інтервалу, залежних від стану виконання місії за попередній часовий інтервал,

$$D = \begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1n} \\ d_{21} & d_{22} & \cdots & d_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ d_{n1} & d_{n2} & \cdots & d_{nn} \end{bmatrix}$$, d_{ij} – визначається як імовірність того, що система, яка почала місію із стану *i*, закінчить її у стані *j*.

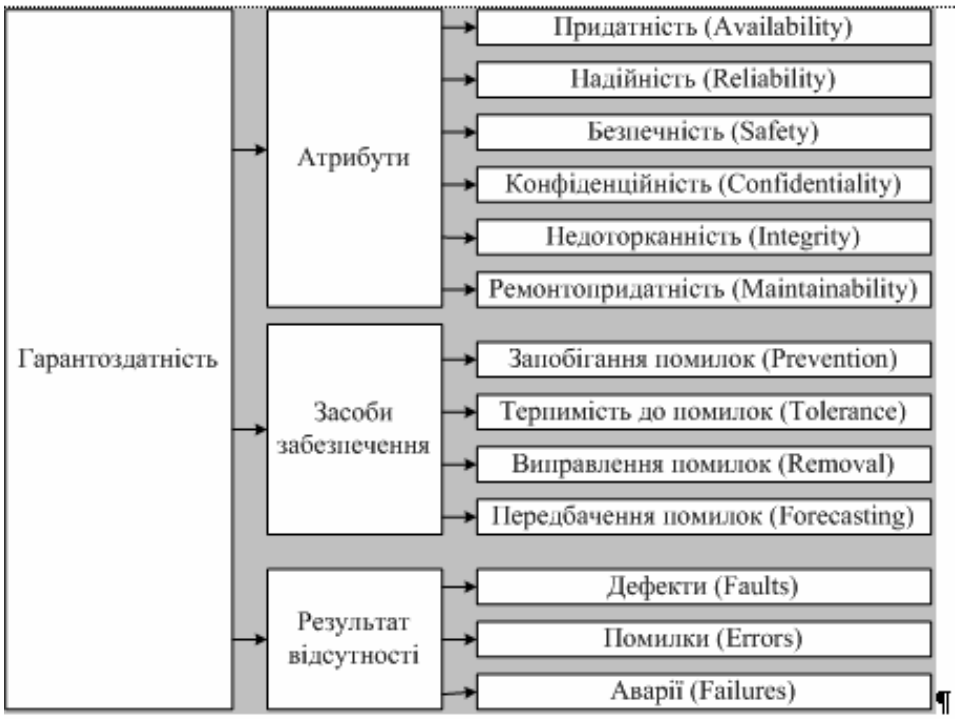

Рис. 2. Гарантоздатність

Коли ремонт під час виконання місії не передбачається, то система, у кращому випадку, залишиться у стані, з якого вона почала місію. У гіршому випадку стан системи погіршуватимуться до повного виходу з ладу. При цьому деякі елементи матриці *D* дорівнюватимуть 0. Якщо прийняти, що стан 1 – найкращий стан (усе працює), а стан *n* – найгірший (повне руйнування), то матриця *D* стане трикутною і матиме вигляд

$$D = \begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1n} \\ 0 & d_{22} & \cdots & d_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_{nn} \end{bmatrix}.$$

Якщо матриця *D* побудована правильно, то сума ймовірностей у кожному її рядку буде однакова. Для першого рядка буде справедливо $d_{11}+d_{12}+\ldots+d_{1n} = 1$.

Таке ж співвідношення буде справедливим і для інших рядків матриці *D*.

C – результативність, нелінійна матриця ймовірностей, що представляє спектр результатів залежно від заданої місії і стану системи, тобто, очікувані кількісні характеристики переваг системи. Коли вимірюється тільки один результат виконання місії, то матриця *C* має вигляд

$$C = \begin{bmatrix} c_1 \\ c_2 \\ \dots \\ c_n \end{bmatrix}. \text{ Тоді CE} = [a_1\, a_2 \dots a_n] \cdot \begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1n} \\ 0 & d_{22} & \cdots & d_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_{nn} \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ \dots \\ c_n \end{bmatrix} = \sum_{i=1}^{n} \sum_{j=1}^{n} a_i d_{ij} c_j \ .$$

Отже, елементи матриці D характеризують вплив кожного зі складників гарантоздатності на її загальну величину. Для спрощення задачі оцінювання гарантоздатності і порівняння різних гарантоздатних систем можна порівнювати їх за кожним елементом матриці D окремо. При цьому для спрощення можна вважати, що система може перебувати лише в двох станах (1 та 2) – справному і несправному.

Оцінювання конфіденційної складової гарантоздатності

Описаний підхід до оцінювання ефективності систем дає можливість оцінити вплив на гарантоздатність складових частин гарантоздатності, зокрема, криптографічних засобів, що забезпечують конфіденційність. Нижче пропонується метод оцінювання гарантоздатності систем електронного цифрового підпису.

Гарантоздатність криптографічних засобів можна оцінити величиною ймовірності d_{11} того, що під час виконання місії стан системи не погіршиться (для спрощення можна вважати, що $d_{11} + d_{12} = 1$). Стосовно цифрового підпису стан системи не погіршиться, якщо за час виконання місії підпис не буде підроблений, якщо спроби його підробити починаються тільки після початку місії.

Стійкість нових стандартів електронного цифрового підпису [19, 20] ґрунтується на складності розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої. Ця задача формулюється так:

задано еліптичну криву E над полем $GF(p)$ або $GF(2^p)$, де p – просте число;

обрано точку P, що має порядок n у групі точок кривої E;

знаючи точку dP, необхідно відновити натуральне число d.

Найшвидшими алгоритмами розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої при правильному виборі параметрів вважаються ρ-метод і λ-метод Полларда [21]. Так, для поліпшеного ρ-методу Полларда обчислювальна складність оцінюється для Кобліцевих кривих над полями $GF(2^p)$ як $I_p = \sqrt{\pi n / 4p}$ і для усіх інших кривих над полями $GF(2^p)$ і $GF(p)$ як $I_p = \sqrt{\pi n / 4}$ [23]. У всіх випадках обчислювальна складність визначає кількість операцій додавання точок еліптичної кривої. У [23] продуктивність V засобів, що виконують пошук дискретного логарифму, прийнято V=16000 таких операцій на секунду.

Тобто, ймовірність погіршення стану системи d_{12} за час місії t_m дорівнює ймовірності вирішення проблеми дискретного логарифмування за час місії $d_{12} = t_m / t_{DL} = t_m / I_p \cdot t_{add} = t_m / I_p \cdot V = C / I_p$,

де t_{DL} – очікуваний час дискретного логарифмування, $t_{DL} \geq t_m$;

t_{add} – час виконання операції додавання точок еліптичної кривої;

V – продуктивність системи, яка проводить дискретне логарифмування.

При порівнянні різних гарантоздатних систем можна приймати V – const. t_m – const, тоді $t_m V = C$ – *const*. Кращою вважатиметься гарантоздатна система з меншим d_{12} і, відповідно, з більшим I_p.

За цим підходом за межами розгляду залишається питання ціни забезпечення гарантоздатності.

У табл. 2 [23] наведено орієнтовну кількість операцій додавання, необхідних для обчислення одного дискретного логарифму для різних значень p.

Таблиця 2

Складність дискретного логарифмування

Розмір поля p (біт)	Значення для поля $GF(2^p)$ $\sqrt{\frac{\pi n}{4}} = I_p$	Значення для поля $GF(p)$ $\sqrt{\frac{\pi n}{4}} = I_p$
79	4.9×10^{11}	6.1×10^{11}
89	1.8×10^{13}	2.4×10^{13}
97	2.5×10^{14}	3.0×10^{14}
109	1.6×10^{16}	2.1×10^{16}
131	3.3×10^{19}	3.5×10^{19}
163	1.7×10^{23}	2.4×10^{24}
191	3.5×10^{28}	4.9×10^{28}
		8.2×10^{35}
353	1.1×10^{53}	
359		9.6×10^{53}

Для підкреслення переваг використання еліптичних кривих у табл. 3 [22] наведено оцінку обчислювальної складності вирішення задач дискретного логарифмування в групі точок еліптичної кривої I_p (кількість операцій додавання точок еліптичної кривої) і у простому полі I_{pp} (кількість операцій множення елементів у полі $GF(p)$). Хоча самі операції додавання точок еліптичної кривої і множення елементів у полі $GF(p)$ мають різну складність, це неістотно впливає на результат порівняння. Як видно, нові алгоритми цифрового підпису, що ґрунтуються на еліптичних кривих, забезпечують більшу гарантоздатність криптографічної комп'ютерної системи.

Таблиця 3

Обчислювальна складність злому стандартів ЕЦП

Порядок поля p і порядок q базової точки P (біт)	I_p	I_{pp}
128	$1{,}63 \times 10^{19}$	$1{,}35 \times 10^{10}$
256	$3{,}02 \times 10^{38}$	$1{,}12 \times 10^{14}$
512	$1{,}03 \times 10^{77}$	$1{,}76 \times 10^{19}$
1024	$1{,}19 \times 10^{154}$	$1{,}32 \times 10^{26}$
1536	$1{,}38 \times 10^{231}$	$1{,}31 \times 10^{31}$
2048	$1{,}59 \times 10^{308}$	$1{,}53 \times 10^{35}$

Висновки

Запропоновано метод оцінювання гарантоздатності криптографічних комп'ютерних систем цифрового підпису, що ґрунтуються на використанні еліптичних кривих. Пропонується визначати гарантоздатність таких систем як імовірність того, що підпис не буде зламаний під час виконання місії. В основу метода покладене визначення складності дискретного логарифмування в групі точок

обраної еліптичної кривої. Показано, що алгоритми, які ґрунтуються на використанні еліптичних кривих, забезпечують більшу гарантоздатність порівняно з алгоритмами, що не використовують еліптичні криві.

1. Шишонок Н.А., Репкин В.Ф., Барвинский Л.Л. Основы теории надежности и эксплуатации радиоэлектронной техники / Под ред. Н.А. Шишонка. – М.: Советское радио, 1964. 2. Сотков Б.С. Основы теории и расчета надежности элементов и устройств автоматики и вычислительной техники. Изд. 1-е: Учеб. пособие для вузов по спец. «Автоматика и телемеханика» и «Математические и счетно-решающие приборы и устройства». – М.: Высшая школа, 1970. 3. Журавлев Ю.П. и др. Надежность и контроль ЭВМ / Ю.П. Журавлев, Л.А. Котелюк, И. Циклинский. – М.: Сов.радио, 1978. – 416 с., ил. 4. Надежность технических систем: Справочник / Ю.К.Беляев, В.А.Богатырев, В.В.Болотин и др.; Под ред. И.А.Ушакова. – М.: Радио и связь, 1985. – 608 с., ил. 5. Иыуду К.А. Надежность, контроль и диагностика вычислительных машин и систем: Учеб. пособие для вузов по спец. «Вычислительные машины, комплексы, системы и сети». – М.: Высш. шк., 1989. – 216 с.: ил. 6. Пацюра И.В., Корнейчук В.И., Довбыш Л.В. Надежность электронных систем. – К.: Світ, 1997. 7. Локазюк В.М., Савченко Ю.Г. Надійність, контроль, діагностика і модернізація ПК. Посібник. За редакцією д.т.н., проф. В.М. Локазюка. – К.: Видавничий центр «Академія», 2004. 8. ГОСТ 27.002-83. Надежность в технике. Термины и определения. 9. ДСТУ 2668-94 Безвідмовність обслуговування та готовність. Терміни та визначення. 10. ДСТУ 2860-94 Надійність техніки. Терміни та визначення. 11. Лашкарев Ю., Павлов Л., Лаврешин Г. Как обеспечить надежность банковских ИТС http://www.bdm.ru/arhiv/2003/12/56-59.htm. 12. Avizienis A., Laprie J.-C., Randell B. and Landwehr C. "Basic Concepts and Taxonomy of Dependable and Secure Computing," IEEE Transactions on Dependable and Secure Computing, vol. 1, pp. 11-33, 2004. 13. IEC 50(191):1990 International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service. 135 p. 14. IEC 60050-191-am2 (2002) Ed. 1.0 International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service. 15. "DeSSerT" http://stc-dessert.com 16. Теслер Г.С. Концепція побудови гарантоздатних обчислювальних систем // Математичні машини і системи. – 2006. – № 1. – С. 134 – 145. 17. Military handbook MIL-HDBK-338b. Electronic reliability design handbook. Department of defense of USA. 1 october 1998. 18. AFSC-TR-65-6, Chairman's Final Report. Weapon System Effectiveness Industry Advisory Committee (WSEIAC), Air Force Systems Command, January 1965, (AD-467816). 19. IEEE Std 1363-2000 IEEE Standard Specifications for Public-Key Cryptography Sponsor Microprocessor and Microcomputer Standards Committee of the IEEE Computer Society. Approved 30 January 2000. 20. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – К.: Державний комітет України з питань технічного регулювання та споживчої політики. 2003. 21. Бондаренко М.Ф., Горбенко И.Д., Качко Е.Г., Свинарев А.В., Григоренко Т.А. Сущность и результаты исследований свойств перспективных стандартов цифровой подписи X9.62-1998 и распределения ключей X9.63-199X на эллиптических кривых. 22. Игоничкина Е.В. Анализ алгоритмов электронной цифровой подписи // Материалы III Международного конкурса по информационной безопасности "Securitatea informationala – 2006" (14–15 апреля 2006 года). http://www.security.ase.md/publ/ru/pubru86. 23. Certicom ECC Challenge. http://www.certicom.com/ download/aid-111/cert_ecc_challenge.pdf. Copyright 2008 Certicom Corp. 24. set01.pdf//lion.ee.ntu.edu.