УДК 004.236.321

Павлов І.М., Бірюков В.О. (ВІТІ НТУУ «КПІ»)

ФОРМАЛІЗАЦІЯ ПРОЕКТНИХ ПОКАЗНИКІВ ЯКОСТІ ЗАХИСТУ ІНФОРМАЦІЇ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

У статті, в формалізованому вигляді розглянуті та визначенні показники якості захисту інформації комплексною системою захисту інформації на етапі проектування.

Ключові слова: комплексна система захисту інформації, проектування, показники якості захисту інформації.

Вступ

Сучасні системи захисту інформації, які об'єднуються в єдину комплексну систему захисту інформації (КСЗІ), являють собою складні програмно-технічні системи, які будуються на комп'ютерних технологіях. Так, без впровадження сучасних комп'ютерних технологій неможливо підвищення ефективності захисту інформації, підтримання на сучасному стані якості захищеності інформаційних систем.

В той же час досвід експлуатації таких складних систем виявляє ряд проблем технічного та інформаційного характеру, до яких відноситься проблема підвищення ефективності обслуговування КСЗІ на різних рівнях розподіленої інформаційної системи.

Таким чином виникає протиріччя. З одного боку, для підвищення ефективності роботи необхідні сучасні комп'ютерні системи, які застосовуються для обробки, зберігання, аналізу та передачі конфіденційної інформації, з другого боку, застосування комп'ютерних технологій приводить до зниження захищеності інформації за рахунок несанкціонованого доступу та витоку інформації по технічним каналам, при цьому порушуються конфіденційність, цілісність, доступність та спостережність інформації.

Розширення цього протиріччя приводить до реалізації ризиків в результаті постійного впливу руйнівних загроз для КСЗІ.

Вирішення цього протиріччя виконується на етапі проектування КСЗІ [1] та на етапах реалізації та підтримання функціонування КСЗІ.

З теорії практичного застосування автоматизованих інформаційних систем відомо, що при правильному виборі і організації функціонування КСЗІ, в основному показники надійності її складових та живучості системи захисту в цілому, помилки при розробці програмного забезпечення − впливають на основні якісні властивості КСЗІ. Таким чином, підтримання на визначеному рівні показників якості захищеності КСЗІ є гарантією ефективного застосування систем захисту інформації.

Тому *метою цієї статті* є визначення показників якості захисту інформації комплексної системи захисту інформації під час її проектування та подання цих показників в формалізованому вигляді.

Постановка задачі

Аналіз [1-5] показав, що основними вимогами, які на етапі проектування пред'являються до показників, які характеризують захищеність інформації КСЗІ, є:

− відносна простота і чіткий фізичний смисл;

− забезпеченість вихідними даними і можливість їх обчислення;

− критичність до різних варіантів обслуговування елементів КСЗІ.

Для зручності проведення оцінки проектної ефективності застосування КСЗІ необхідно провести класифікацію показників якості захищеності інформації КСЗІ. Під якістю розуміється сукупність властивостей, які відповідають визначеним вимогам, відповідно до яких КСЗІ може застосовуватися за призначенням [4]. Однак, виходячи з задач, рішення яких покладається на КСЗІ, специфіки її застосування, можна визначити наступні групи показників якості захисту інформації (рис.1):

− групи показників необхідності використання КСЗІ;

− групи показників продуктивності КСЗІ;
− групи показників надійності елементів КСЗІ;
− групи показників живучості КСЗІ;
− групи показників ступені захищеності інформації;
− група показників технічного рівня;
− вартісні групи показників.

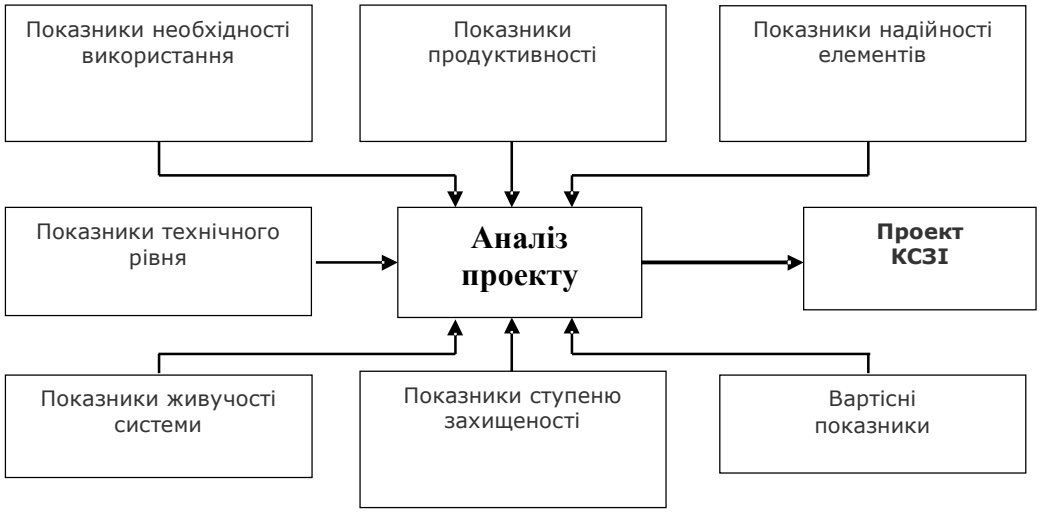


Рис. 1. Групи проектних показників якості захисту інформації

Розгляд основної частини

Розглянемо проектні показники якості захищеності інформації докладніше:

Показники необхідності використання КСЗІ характеризують властивість КСЗІ, яка визначає і обумовлює її корисність, специфіку, призначення і використання.

Ці показники можуть бути представлені в вигляді:

$$P_{\text{н}} = (\{N_m\}, \{G\}, \{f_m\}, \vartheta), \tag{1}$$

де $\{N_m\}$ – множина задач і функцій, які вирішуються в КСЗІ; $\{G\}$ – множина вимог та умов функціонування, які виконуються (у відповідності з замовленням або документацією); ϑ – кількість задач, які необхідно вирішити в КСЗІ, $m = 1, \vartheta$; $\{f_m\}$ − індикаторна функція впровадження задач спеціального програмного забезпечення КСЗІ, яка визначається виразом:

$$f_m = \begin{cases} 1, - & \text{задача вирішується} \\ 0, - & \text{задача не вирішується.} \end{cases} \tag{2}$$

Показники необхідності можуть визначатися різними відношеннями елементів множин. Найбільш представницьким (превалюючим) показником необхідності є показник впровадження функціональних задач, функцій, умов $K_{\text{вз}}$. В загальному випадку:

$$K_{\text{вз}} = \prod_{m=1}^{\vartheta} f_m, \tag{3}$$

де $K_{\text{вз}}$– визначає ступінь впровадженості задач в КСЗІ ($K_{\text{вз}} = 0$ або 1).

Коли хоча б одна із задач, які необхідно вирішувати в КСЗІ, не виконується (не реалізується), КСЗІ не може в повній ступені використовуватися по призначенню. В цьому випадку $K_{вз} = 0.$

Показники продуктивності відображають основні вірогіднісно-часові характеристики процесу виконання функцій (рішення задач) КСЗІ.

В якості показників продуктивності можуть використовуватися, наприклад, потенціальна продуктивність КСЗІ при рішенні комплексу функціональних задач, математичне очікування часу реакції на вплив загроз, середній час відбиття загроз тощо. Аналіз показує, що інтегральним, головним показником цієї групи є своєчасність (оперативність), яка визначається вірогідністю $P(T_{обр} \leq T_д)$ того, що час обробки і рішення комплексу функціональних задач виконується за час, який не перевищує директивний (визначений).

Показники надійності визначають властивості КСЗІ, які дозволяють зберігати працездатність під час відмов її елементів або груп елементів. Тобто надійність КСЗІ – це властивість системи зберігати свої функції згідно визначених розробником умов роботи її елементів [5] .

По числу можливих станів (працездатності) елементи КСЗІ можуть знаходитися у двох станах – працездатному або непрацездатному, а по режиму застосування (функціонування) КСЗІ відноситься до систем безперервного застосування. КСЗІ відноситься до систем, які в процесі експлуатації можуть відмовитися або перейти в критичний стан.

Критеріями відмови КСЗІ є:

− припинення виконання КСЗІ заданих функцій, зниження якості функціонування до критичного рівня;

− неправильне рішення задач захисту від відмов.

Критеріями критичних станів КСЗІ є:

− відмова однієї або декількох складових частин системи, відновлення або заміна, яких, повинна проводитися в ремонтних органах;

− зниження показників якості властивостей КСЗІ до критично допустимого рівня;

− зниження напрацювання на відмову нижче заданого рівня;

− перевищення встановленого рівня існуючих (сумарних) витрат на розробку, впровадження та експлуатацію КСЗІ, яке визначає економічну невигідність системи захисту по відношенню з важливістю інформації, яку необхідно захищати.

По наслідкам відмов або досягнень критичного стану при застосуванні комп'ютерна техніка відноситься до виробів, відмови яких або перехід в критичний стан яких не приводить до катастрофічних наслідків (загрози для людини), але загрози потенційного впливу на інформацію, яка циркулює в комп'ютерних мережах, можуть привести до катастрофічних наслідків як для людини, так і для суспільства (в залежності від самої інформації і задач інформаційної системи).

По впливу відмов на результат виконання задач КСЗІ можна класифікувати як систему, у якій вихідний ефект застосування пропорціональний сумарному часу безвідмовної роботи.

По можливості відновлення працездатності після відмов, в процесі експлуатації КСЗІ відноситься до систем, які відновлюються [6].

Враховуючи вищесказане, в якості основного інтегрального показника надійності КСЗІ вибирається $K_г$ − коефіцієнт готовності КСЗІ до роботи. Тому коефіцієнт готовності визначається, як вірогідність того, що КСЗІ буде працездатним в випадковий момент часу:

$$K_г = {T_{рп}}/{(T_{рп} + T_{чв})}, \quad (4)$$

де $T_{рп}$ – час роботи КСЗІ при використанні по призначенню; $T_{чв}$ – час на відновлення елементів КСЗІ.

Показники живучості КСЗІ визначають спроможність системи компенсувати (повністю або хоча-б частково) вплив небезпечних зовнішніх впливів (атак) на якість її цільового функціонування відповідним чином організованої реакцією своєї структури або алгоритму функціонування.

Тобто живучість КСЗІ це спроможність системи виконувати хоча-б мінімальний встановлений об'єм функцій при зовнішніх впливах, не передбачених умовами нормальної експлуатації.

Під час аналізу живучості КСЗІ оцінюється [7]:

1) ціль функціонування КСЗІ (де, в якій системі і для захисту якої інформації встановлюється);

2) множина задач, рішення яких забезпечує система захисту;

$$Z = \{z_1, z_2, ..., z_k\}. \tag{5}$$

3) множина бар'єрів, які є складовими частинами КСЗІ.

$$B = \{b_1, b_2, ..., b_g\}. \tag{6}$$

У КСЗІ, яка має властивості живучості, можна визначити три типу цілей функціонування:

1. В системі захисту повинно забезпечуватися рішення всієї множини задач Z з заданою ефективністю (наприклад, з дотриманням критеріїв конфіденційності, цілісності) в вільному стані $d \in D$, тобто повинна виконуватися умова:

$$Z = \prod_{i=1}^{k} x(Z_i) = 1, \text{ при } x(Z_i) = \begin{cases} 1, \text{коли задача } Z_i \text{ вирішується в КСЗІ} \\ 0, \text{в протилежному випадку.} \end{cases} \tag{7}$$

.

2. Система захисту в будь-яких можливих станах $d \in D$ повинна виконувати з заданою ефективністю деяку (пріоритетну) підмножину задач z^* з множини Z_i, які можуть виконуватися в системі у випадку звільнення необхідних ресурсів. Таким чином, множина задач, яка виконується КСЗІ, залежить від стану, в якому знаходиться система і не є постійною:

$$Z \subseteq \sum_{i=1}^{k} x(z_i^*). \tag{8}$$

3. Система повинна забезпечувати рішення хоча б однієї (можливо найбільш важливої) задачі $z^{\wedge}$ з підмножини z^* в своєму вільному стані $d \in D$, тобто:

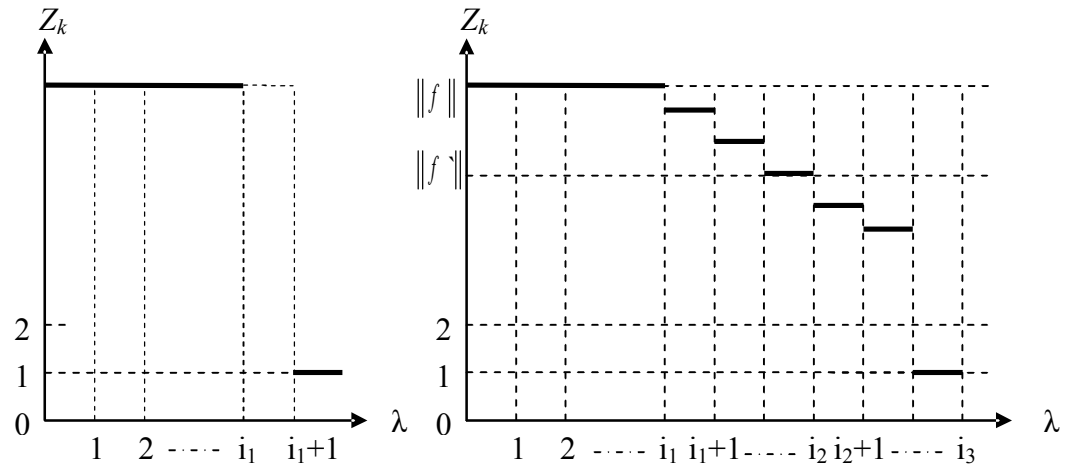
$$Z = \subseteq \sum_{i=1}^{k} x(z_i^{\wedge}). \tag{9}$$

Оцінка живучості КСЗІ повинна будуватися з врахуванням цілі функціонування.

Ціль функціонування – це поняття, яке вводиться для живучих та відмовостійких систем, однак зміни цілей можливі тільки для систем, які мають властивості живучості.

Якісна залежність цілі функціонування від кількості функціональних відмов, під час впливу загроз (атак), або технічних, програмних відмов для відмовостійких та живучих систем надана на рис. 2.

Як зрозуміло з рисунку деградація системи, яка має властивості живучості, їде "плавно" на відміну від відмовостійких систем. Це забезпечується засобами, які дозволяють перебудовуватися на виконання "нової" цілі функціонування, для якої в системі можна добитися необхідної якості виконання.



а) відмовостійкі системи б) живучі системи

Рис. 2. Якісна залежність цілі функціонування від кількості відмов в різних системах

Показники ступеню захищеності інформації характеризують рівень захищеності інформації, який забезпечує КСЗІ. В цій показник, як приклад, можуть входити оцінки захищеності, які забезпечуються на окремих елементах КСЗІ (бар'єрах механізмів захисту).

В загальному випадку, показник ступеню захищеності інформації в КСЗІ розглядається як:

$$P_{\text{в}} = \langle \{Y_i\}, \{q_i\}, n, \{P_{nj}\}, Z, \{P_{\text{дод}}\} \rangle, \tag{10}$$

де $\{Y_i\}$ – множина якісних вимог до КСЗІ по захисту інформації згідно [8], $i = \overline{1,n;}$ – кількість класів захисту, де n – кількість бар'єрів захисту; $\{q_i\}$ – ступінь реалізації вимог i-го класу захисту; $\{P_{nj}\}$ – множина показників блокування загроз бар'єрами механізмів захисту КСЗІ, $j = \overline{1,z;}$ – кількість зон, рівнів, засобів захисту; $\{P_{\text{дод}}\}$ – множина додаткових показників, які уточнюють, при необхідності, вибір $P_{\text{в}}$.

Частіше усі вимоги захищеності інформації неможливо розглянути на етапі проектування, тому цій показник відносять до розряду обмежень і рахують у вигляді мультиплікативного критерію:

$$P_{\text{в}} = \prod_{i=1}^{n} P_{\text{в}i}, \tag{11}$$

де $P_{\text{в}i}$ – індикаторна функція вигляду:

$$P_{si} = \begin{cases} 1, - & \text{вимоги виконуються} \\ 0, - & \text{вимоги не виконуються.} \end{cases} \quad (12)$$

Показники технічного рівня характеризують як критерії додержання відповідних концепцій на основі розробок, які існують, які мають якісні властивості по відношенню з кращими зразками (в цьому випадку засобами обчислювальної техніки, програмного забезпечення, комунікаційного обладнання тощо) та кращі показники фізичного та морального старіння.

Показник технічного рівня може бути представлений у наступному вигляді:

$$P_{\text{тр}} = \langle \{P_\theta\}, \{P_{\theta\delta}\} \rangle, \quad (13)$$

де $\{P_\theta\}$ – множина значень параметрів, які використовуються і оцінюються в КСЗІ; $\{P_{\theta\delta}\}$ – множина досяжних (кращих), технічно реалізованих значень параметрів окремих базових засобів в КСЗІ.

Вартісні показники характеризують матеріальні і часові витрати на КСЗІ на різних етапах життєвого циклу КСЗІ [9].

До складу цієї групи входять: $C_{\text{р}}$– витрати на етапі розробки, $C_{\text{ве}}$ – витрати на етапі вводу до експлуатації КСЗІ, $C_{\text{е}}$ – вартість експлуатації КСЗІ продовж визначеного строку і $C_{\text{КСЗІ}}$ – як комплексна основна вартісна складова.

Найбільш повно характеризує вартісну складову КСЗІ її загальна вартість з врахуванням витрат на основних етапах життєвого циклу. В загальному вигляді цій показник може бути представлений як:

$$C_{\text{КСЗІ}} = C_{\text{р}} + C_{\text{ве}} + C_{\text{е}}. \quad (14)$$

Приведена система показників якості захисту інформації в різній ступені характеризує КСЗІ. Обрані показники утворюють систему взаємопов'язаних (в загальному випадку) показників, які характеризують якісні властивості КСЗІ, з урахуванням складу, динаміки і процесів розвитку, витратних механізмів, які відрізняються повнотою і достатністю на етапі проектування.

Висновки. Ще до початку розробки КСЗІ розробнику необхідно визначитися, в яких рамках повинна бути стійка КСЗІ, і як вона повинна працювати в інформаційній системі, до якої приділяються вимоги конфіденційності, цілісності, доступності та спостережності інформації. Відомо, що рівень захисту інформаційних систем визначається системою кількісних та якісних показників, які представлені, як правило, в лінгвістичній, нечітко визначеною замовником формою, які інтерпретуються через еталони параметрів. Тому формалізація проектних показників якості захисту інформації в КСЗІ є необхідною умовою для діагностики проектних рішень по створенню систем захисту інформації.

Список літератури

1. Павлов И.Н. Проектирование систем защиты информации. Формальный подход [Текст] / И.Н. Павлов // Збірник "Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні". – К.: 2005. – Вып. 11. – С. 54 – 60.

2. Герасименко В.А. Защита информации в автоматизированных системах обработки данных / В.А. Герасименко // – М.: Наука и техника, 1994. – Кн. 1. – 399 с.

3. Горбач И. Защита информации от несанкционированного доступа в распределённых автоматизированных системах [Текст] / И. Горбач, М. Дума, В. Куценко // "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". – Київ, 2000. – Вып. 2. – С. 155 – 158.

4. Домарев В.В. Безопасность информационных технологий. Методо-логия создания систем защиты / В.В. Домарев // – К.: Свифт, 2001. – 680 с.

5. Малюк А.А. Информационная безопасность: Концептуальные и методологические основы защиты информации / А.А. Малюк // – М.: Высшая школа, 2004. – 280 с.

6. Павлов І.М. Методика аналізу надійності комплексних систем захисту інформації в автоматизованих системах [Текст] / І.М. Павлов // Збірник "Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні". – К.: 2005. – Вип. 10. – С. 59 – 65.

7. Павлов І.М. Методика оцінки живучості підсистеми захисту інформації в інтегрованих базах даних спеціальних автоматизованих систем [Текст] / І.М. Павлов // Збірник наукових праць НДІ ГУР. − К.: 2005. − Вип. 13. − С. 81 − 93.

8. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Текст] // НД ТЗІ 2.5 – 004 – 99. – Київ, 1999. – 51 с.

9. Щеглов А.Ю. Проблемы и принципы проектирования систем защиты информации от НСД [Текст] / А.Ю. Щеглов // Сборник "Экономика и производство". – М.: 2001. – № 3. – С. 34 – 46.

Надійшла: 13.05.2011 р.

Рецензент: д.т.н., проф. Конахович Г.Ф.