УДК 37.035—053.81+316.752

Антонюк А. О.

ПРО ДЕЯКІ ПОНЯТТЯ ЗАХИЩЕНОЇ ІНФОРМАЦІЇ

Розглянуто такі важливі поняття Національного стандарту із захисту інформації, як властивості захищеної інформації, критерії захищеності інформації, функціональний профіль захищеності, політика безпеки. Сформульована задача оцінки рівня захищеності системи захисту інформації, а також задача вибору придатного профілю захищеності.

При побудові автоматизованих систем (АС), в яких обробляється інформація обмеженого доступу, важливе місце посідає поняття функціонального профілю захищеності інформації або просто профілю. Воно належним чином визначено в Національному стандарті із захисту інформації [1—4]. Проте його визначення базується на інших важливих поняттях захисту інформації, які слід розглянути перед тим, як почати обговорювати самі профілі.

/. *Основні поняття*

У процесі розробки будь-яких засобів захисту інформації, при побудові систем захисту інформації (СЗІ), а також при проведенні оцінок рівня захищеності СЗІ завжди постає питання поєднання інтересів виробника, споживача і експерта, до того ж інтереси кожного досить суттєво відрізняються один від одного [5]. Саме для вирішення таких питань потрібна система нормативних документів із захисту інформації в АС або, простіше кажучи, стандарти із захисту інформації. Відомо, що перша така система документів була розроблена у США Міністерством оборони і вперше видана у 1983 році. Вона мала назву "Оранжева книга" за кольором обкладинки. Значення "Оранжевої книги" важко переоцінити, оскільки в ній вперше було чітко сформульовано всі основні проблеми безпеки інформації. У нас конфіденційна інформація оброблялася специфічним чином, отже, потреби в таких документах не було. Але з того часу багато що змінилося. Були розроблені і канадські критерії, і європейські, і російські, і знову федеральні США, а зараз є єдині критерії. Отже, цілком зрозуміло, що й незалежній державі, якою тепер є Україна, для організації захисту своєї інформації теж конче потрібні подібні документи. Перша версія Українського стандарту із захисту інформації була видана у 1998 році [1—4] і регламентує наступні питання:

- визначення вимог щодо захисту комп'ютерних мереж від несанкціонованого доступу (НСД);
- створення захищених АС і засобів їх захисту від НСД;
- оцінки захищеності АС і їх здатності для розв'язку задач споживача.

Українська система основних нормативних документів із захисту інформації або стандарт із захисту, або (дуже поширений термін) "Критерії", складається з чотирьох документів. Серед найбільш важливих понять в стандарті подані основні властивості інформації, що визначають її цінність, і називаються фундаментальними властивостями захищеної інформації (ФВЗІ). Такими властивостями є конфіденційність, цілісність, доступність і спостережність. Точні їх визначення подаються в стандарті, а тут зазначимо, що завжди існують можливості їх порушення або невиконання, тобто можливості загроз. Загрози інформації розглядаються з точки зору їх будь-якого небажаного впливу на будь-яку з цих властивостей і можливого їх порушення, тобто загроза — це потенційно можлива несприятлива дія на інформацію. З такої точки зору та згідно зі стандартом за результатами впливу на інформацію та систему її обробки в АС розрізняються наступні класи загроз інформації:

- порушення конфіденційності;
- порушення цілісності (логічної і фізичної);
- порушення доступності або відмова в обслуговуванні;
- порушення спостережності або керованості;
- несанкціоноване використання інформаційних ресурсів.

Детальний опис загроз для конкретної АС є змістом моделі загроз, яка згідно з визначенням стандарту, є абстрактним формалізованим або неформалізованим описом методів та засобів реалізації загроз.

Фундаментальні властивості захищеної інформації — конфіденційність, цілісність, доступність і спостережність — характеризуються важливими особливостями: незалежністю одна від одної, конструктивністю, можливістю повторного їх дублювання при використанні різних механізмів і засобів захисту, можливістю враховування конкретних загроз інформації, можливістю визначення послуг забезпечення кожної з властивостей залежно від

рівня важливості інформації, очікуваних загроз інформації, цілей і завдань захисту.

Саме для підтримки кожної з чотирьох ФВЗІ в стандарті визначено чотири групи критеріїв, кожна з яких є переліком певних послуг протистоянню певним загрозам і до того ж кожна послуга має чіткий змістовний сенс. Всього визначено 22 послуги. Наприклад, для забезпечення конфіденційності їх є 5: 1) довірча конфіденційність, тобто коли обробка інформації довіряється користувачу; 2) адміністративна конфіденційність, коли обробкою інформації керує адміністратор системи; 3) повторне використання об'єктів, коли при їх повторному використанні в них може залишатися закрита інформація; 4) аналіз прихованих каналів, тобто каналів витоку інформації, не зафіксованих при побудові системи; 5) конфіденційність при обміні, тобто при передачі інформації від одного об'єкта до другого. В свою чергу, кожна з послуг ранжується за рівнями зростаючої важливості. Кожний наступний рівень включає всі попередні. Наприклад, для довірчої конфіденційності це такі рівні: мінімальна довірча конфіденційність, базова довірча конфіденційність, повна довірча конфіденційність та абсолютна довірча конфіденційність. Але головне полягає в тому, що в стандарті подається чітко визначений перелік необхідних умов для практичного забезпечення кожного з рівней для кожної з послуг. Наприклад, для забезпечення абсолютної довірчої конфіденційності потрібно виконання таких умов: наявність відповідної політики безпеки, визначення певних правил розмежування доступу, певних послуг щодо спостережності тощо. Практична реалізація необхідних умов може бути досягнута різними механізмами і засобами захисту.

2. Профілі захищеності інформації

На основі наведених вище ФВЗІ в стандарті визначається фундаментальне поняття функціонального профілю захищеності інформації. Функціональний профіль захищеності — це мінімально необхідний перелік послуг СЗІ, що забезпечують певний рівень захищеності інформації. В стандарті подається опис і семантика профілів. Визначено 90 стандартних профілів захисту і перелічені всі вимоги до механізмів та засобів захисту, які мають бути у наявності при реалізації профілів.

Формальний опис профілю можна здійснити так. Згідно зі стандартом, профіль повинен включати ідентифікатор і для кожної з ФВЗІ перелік певних послуг певних рівнів. Тоді вираз для позначення профілю буде набором множин, відповідно до кожної з ФВЗІ, і матиме вигляд

$$CIA = \{\{C_{ij}\}, \{I_{ij}\}, \{A_{ij}\}, \{S_{ij}\}\}, \qquad (1)$$

де *CIA* — ідентифікатор профілю, C — конфіденційність, I — цілісність, *A* — доступність, *S* — спостережність, *i,j* — індекси послуг і рівней відповідно конфіденційності, цілісності, доступності та спостережності. У кожному випадку множини індексів визначаються відповідно до стандарту.

Можливі також і інші ідентифікатори функціональних профілів захищеності, наприклад, *CI, IA* та ін., тобто в лівій частині можуть бути не всі ФВЗІ. Наприклад, можливий такий функціональний профіль захищеності

$$I = \{\{C_{ij}\}, \{I_{ij}\}, \{A_{ij}\}, \{S_{ij}\}\},$$

що означає: даний функціональний профіль має бути реалізований у системі, де основна вимога щодо захисту інформації є забезпечення її цілісності. Отже ясно, що не всюди і не завжди необхідно підтримувати одразу всі ФВЗІ — іноді достатньо лише деяких. Все залежить від конкретної цілі і завдань захисту, а також від очікуваних загроз інформації. Наприклад, у деяких випадках достатньо підтримувати лише конфіденційність, яку можна реалізувати таким механізмом, як криптографія. Іноді, особливо в мережевих конфігураціях, винятково важливою є підтримка доступності.

Слід звернути увагу на те, що в правій частині виразу (1) відповідно до стандарту завжди присутня спостережність. Тобто на кожному рівні спостережність повинна бути присутня в усіх профілях без винятку, що змістовно означає потребу практичного спостереження (аудиту або протоколювання) в АС подій, які стосуються безпеки інформації. Звичайно, обсяг інформації, що контролюється, залежить від рівня захищеності, який підтримується в АС.

3. Оцінка ймовірності зламу захисту

Наведені ФВЗІ, а також поняття профілю дозволяють застосувати наступний підхід до його моделювання. Саме завдяки незалежності ФВЗІ їх можна вважати певними підсистемами (або частинами всієї системи), що складають СЗІ, кожна з яких виконує свою функцію і кожну з яких потрібно підтримувати у працездатному стані. Невиконання хоча б однієї ФВЗІ (тобто однієї з частин або підсистем) означає порушення захисту або, як кажуть на практиці, злам захисту.

Кожній з чотирьох наведених ФВЗІ поставимо у відповідність деяку ймовірність p_i, i = 1, 2, 3, 4 порушення кожної з них. Тоді, в силу незалежності ФВЗІ, ймовірність ρ порушення (зламу) всієї СЗІ визначиться за формулою

$$p = 1 - \prod_{i=1}^{4} (1 - p_i). \qquad (2)$$

Для визначення ймовірностей порушення ФВЗІ p_i необхідно скористатися поняттям послуг та їх рівнів, що входять до профілю. Як було зазначено раніше, у визначення профілю входять чотири множини, в кожну з яких входят певні послуги певного рівня. Нехай p_{ij} — ймовірність порушення i-ї послуги j-го рівня, $j = 1, ..., N_i$, де N_i — кількість рівней, необхідних для підтримки i-ї властивості. Тоді ймовірність порушення i-ї властивості визначиться із співвідношення

$$p_i = 1 - \prod_{j=1}^{N_i} (1 - p_{ij}). \qquad (3)$$

Об'єднуючи формули (1) і (2), отримуємо

$$p = 1 - \prod_{i=1}^{4} (1 - \prod_{j=1}^{N_i} (1 - p_{ij})). \qquad (4)$$

Отже, знаючи розподіли ймовірностей порушення (або невиконання) деяких послуг деяких рівнів можна отримати оцінку ймовірності порушення (або зламу) всієї СЗІ. У свою чергу ці ймовірності можна виразити через ймовірності невиконання необхідних умов для реалізації послуг. Нехай p_{ijk} — ймовірність невиконання k-ї умови i-ї послуги j-го рівня, $k = 1, ..., N_{ij}$. Тоді

$$p_{ij} = 1 - \prod_{k=1}^{N_{ij}} (1 - p_{ijk}) \qquad (5)$$

і в результаті

$$p = 1 - \prod_{i=1}^{4} (1 - \prod_{j=1}^{N_i} (1 - \prod_{k=1}^{N_{ij}} (1 - p_{ijk}))). \qquad (6)$$

Таким чином, справа звелася до ймовірностей невиконання необхідних умов. Але невиконання умов — це реалізація загроз. Отже, проблема полягає в тому, як отримати розподіли загроз інформації. Для деяких класів загроз (наприклад, стихійні лиха) можна отримати оцінки необхідних розподілів ймовірностей з практики, але для більшості загроз, що, як правило, пов'язані з діяльністю порушника — людини, найбільш придатним методом оцінки ймовірностей їх реалізації слід вважати експертний метод. Тут мають враховуватися цінність інформації для її власника, її цінність для зовнішніх зацікавлених об'єктів, можливостей СЗІ та ін.

Співвідношення (6) дає оцінку ймовірності зламу СЗІ. Однак можна сформулювати деякі задачі поновлення СЗІ після зламу. Аналогічно можуть бути сформульовані задачі миттєвого або повільного поновлення СЗІ. Змістовно, наприклад, задача миттєвого поновлення СЗІ може відповідати ситуації, коли злам захисту реалізується в системі з високими вимогами до інформації, тобто вона настільки важлива, що поновлення СЗІ має бути зроблено в найкоротші терміни.

4. Задача вибору профілю захищеності

Розглянемо ще одну задачу моделювання профілю захищеності. Вивчення наведених в [4] профілів показує, що кожний з них вирізняється своїм унікальним набором послуг та їх кількістю. При цьому найскладнішим є профіль *CIA*, в якому містяться 22 послуги. Зауважимо, що це взагалі максимально можлива для профілів кількість послуг. Це дозволяє для всіх профілів ввести єдине позначення, інтерпретуючи формулу (1) як вектор p, що має 22 компоненти, тобто $p = (p_1, ..., p_{22})$. Числове ж значення кожної компоненти дорівнюватиме номеру рівня послуги, оскільки кожна послуга ранжується за рівнями. Якщо деяка послуга взагалі відсутня, то вважається, що відповідна компонента вектора p дорівнює нулю.

Наявність такої кількості різних профілів визначає існування суттєвої різниці між АС. Для полегшення процесу встановлення відповідності вимог до СЗІ з характеристиками АС в стандарті введена класифікація АС. Хоча вона суттєво полегшує процес вибору придатного профілю, все ж цей процес поки залишається дуже складним. Однак цілком зрозуміло, що має існувати деяка формальна (можливо, не взаємооднозначна) відповідність між характеристиками АС і відповідним їй профілем.

Кожному профілю з деякої множини профілів P поставимо у відповідність вектор $p = (p_1, ..., p_n)$ евклідового простору E^n, тобто $p \in E^n$. Аналогічно введемо вектор характеристик АС $d = (d_1, ..., d_m)$, $d \in E^m$, який відповідає деякому набору з множини D характеристик АС. Будемо вважати, що між кожною парою векторів p і d існує формальна відповідність (відображення), яку позначимо

$$F(d) = p, \quad d \in E^m, \quad F, p \in E^n, \qquad (7)$$

де F — деяка функція (оператор), що відображає множину D на множину P. Коли б вигляд оператора (7) був відомий, то для споживача задача вибору придатного профілю звелася б до визначення вектора d (набір характеристик АС) і застосування (7), тобто безпосереднього визначення профілю p. Оскільки $F(d)$ невідоме, то виникає задача його ідентифікації або, що теж саме, ідентифікації моделі (7). Як відомо, для розв'язку задачі ідентифікації моделі потрібні додаткові (експериментальні) дані про об'єкт моделювання, на основі яких можна було б встановити конкретний вигляд (7). Однак в такому загальному вигляді цю задачу розв'язати дуже важко, оскільки:

- невідомо, які дані про об'єкт моделювання необхідні і як їх отримати;
- невідомо, як сформувати якусь гіпотезу про конкретний вигляд (7);
- дуже важко сформувати набір конкретних характерних ознак АС.

Остання обставина є особливо важливою тому, що при вивченні списку профілів виявляється певна неоднозначність у виборі профілю. Справді, відповідно до [4] тільки для одного класу АС пропонується цілий список профілів. Однак така неоднозначність лише уявна і виникає внаслідок того, що поки не існує детальної і однозначної класифікації АС. Очевидно, що коли набір характеристик АС буде достатньо повним і детальним, неоднозначність автоматично зникне — кожній АС буде відповідати єдиний профіль. Однак той факт, що в [4] все ж є деякий список найбільш розповсюджених профілів, означає, що складна частина цієї задачі хоча і неформально (експертним шляхом), але розв'язана, а саме: встановлена деяка множина наборів характеристик АС D_e, $D_e \subset D$ і множина відповідних їм профілів P_e, $P_e \subset P$ (множина P_e є набором профілів). У даному випадку в якості множини наборів характеристик АС D_e можна взяти їх класифікацію з [4], а множину профілів P_e можна сформувати, взявши для кожного класу АС лише один профіль з запропонованого списку (наприклад, перший). Це дає можливість скористатися списком [4] для формулювання наступного варіанта задачі (7).

Розглянемо в якості (7) найбільш просте лінійне відображення, тобто

$$Ad + b = p, \quad d \in E^m, \quad b, p \in E^n, \tag{8}$$

де A — матриця розмірності $m \times n$.

У (8) в якості задачі ідентифікації моделі виникає також складна задача визначення матриці A і вектора b. Як відзначалося раніше, фактично у вказаному списку профілів дається відповідність: тип АС — профіль. Тобто кожному k-му вектору характеристик АС $d_k = (d_{1k}, ..., d_{mk})$, $d_k \in D_e$, відповідає певний профіль — вектор $p_k = (p_{1k}, ..., p_{nk})$, $p_k \in P_e$, $k = 1, ..., K$, K — кількість профілів у P_e і наборів характеристик АС в D_e. Така відповідність множин дозволяє сформулювати і розв'язати задачу ідентифікації матриці A і вектора b. Аналогічно (8) випишемо наступну систему лінійних векторних рівнянь відносно елементів матриці A і компонент вектора b

$$Ad_k + b = p_k, \quad k = 1, ..., K. \tag{9}$$

Із загальних міркувань випливає, що вектор b має дорівнювати нулю — немає характеристик, немає і профілю. Задача ідентифікації матриці A тепер може бути сформульована наступним чином. Визначимо функцію $f(A)$ від елементів матриці A (всього nm змінних) так

$$f(A,b) = \sum_{k=1}^{K} \left\| Ad_k - p_k \right\|^2, \tag{10}$$

де через $\|\cdot\|$ позначена звичайна евклідова норма вектора. Тепер задача ідентифікації зводиться до задачі безумовної мінімізації функції (нев'язки) (10) по елементах матриці A. Зазначимо, що для забезпечення єдності мінімуму функції (10), тобто єдності матриці A, необхідно, щоб вектори d і p були лінійно незалежними. Із властивостей функції (10) відзначимо, що вона неперервна і диференційована на елементах матриці A, тому для її мінімізації можна застосувати будь-який з відомих методів безумовної мінімізації неперервних функцій. Матриця A, що забезпечує мінімум функції (10), може в подальшому використовуватися для вибору профілю.

Замість (8) можна розглядати більш складне відображення (наприклад, квадратичне). При цьому вся схема задач ідентифікації зберігається, зміниться лише кількість та вигляд змінних, а також вигляд функцій (9) і (10).

5. Про політику безпеки інформації

Звідки виникає так звана політика безпеки (ПБ) і навіщо вона взагалі потрібна? Як відомо, при побудові СЗІ і організації захисту в АС завжди виникають питання: хто, що і як конкретно має робити у процесі експлуатації АС. Саме ці питання вирішуються побудовою відповідної ПБ [6, 7]. Під поняттям ПБ інформації розуміється організована сукупність документованих керівних рішень, спрямованих на захист інформації і асоційованих із нею ресурсів системи. Політика включає систему поглядів, основних принципів, практичних рекомендацій і вимог, що закладаються в основу реалізованої в системі комплексної СЗІ.

Будь-який захист починається з визначення того, що потрібно захищати, від яких загроз і якими засобами. Визначання інформації, яка має захищатися, зводиться до того, що вона повинна мати ФВЗІ. Ці властивості іноді є взаємовиключаючими, що ускладнює забезпечення їх одночасної підтримки. Тому захист інформації починається з встановлення співвідносин між цими властивостями для конкретної предметної сфери. Саме ці співвідносини, що містять правила розподілу, збереження і обробки інформації, і є змістом ПБ інформації.

Дотримання ПБ повинно забезпечити виконання того компромісу між альтернативами, який вибрали володарі цінної інформації для її захисту. Річ у тому, що для організації захисту навіть у конкретній системі немає єдиного шляху. Отже, завжди будуть компроміси і тому ПБ ніколи не задовольнить усі сторони, які беруть участь у взаємодії з інформацією, що захищається. Водночас вибір ПБ — це врешті-решт вирішення проблеми: що — добре і що — погано при спілкуванні з цінною інформацією. Після прийняття такого рішення можна будувати захист, тобто систему підтримки

виконання правил ПБ. Таким чином, побудована СЗІ є якісною, коли вона надійно підтримує виконання правил ПБ. Навпаки, СЗІ — погана, якщо вона ненадійно підтримує ПБ.

Таке вирішення проблеми захищеності інформації та проблеми побудови СЗІ дозволяє залучити точні математичні методи, тобто довести, що дана система у заданих умовах підтримує ПБ. Саме у цьому полягає суть доказового підходу до захисту інформації, який дозволяє говорити про "гарантовано захищену систему". Суть "гарантованого захисту" у тому, що при дотриманні початкових умов свідомо виконуються всі правила ПБ.

Основними етапами формального підходу до аналізу СЗІ є:

1) визначення об'єктів і цілей захисту;

2) розробка політики;

3) доведення того, що при її додержанні інформація не компрометується відповідно до п. 1;

4) визначення набору функцій для підтримки політики;

5) доведення того, що набір функцій забезпечує додержання політики;

6) вибір апаратного і програмного забезпечення для реалізації функцій ЗІ.

Для формальних доведень в пунктах 3 і 5 можуть використовуватися математичні методи, якщо сама ПБ була визначена достатньо строго.

Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.— НД ТЗІ 1.1-002-99, ДСТСЗІ СБ України, Київ, 1999.

Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.— НД ТЗІ 1.1 -003-99, ДСТСЗІ СБ України, Київ, 1999.

Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу— НД ТЗІ 2.5-004-99, ДСТСЗІ СБ України, Київ, 1999.

Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.— НД ТЗІ 2.5.-005-99, ДСТСЗІ СБ України, Київ, 1999.

5. *Зегжда Д. П., Ивашко А. М.* Как построить защищенную информационную систему.— НПО: "Мир и семья-95".— СПб., 1997.
6. *Грушо А. А., Тимонина Е. Е.* Теоретические основы защиты информации.— М.: Яхтсмен, 1996.
7. *Антонюк А. А., Заславская Е. А., Лащевский В. И.* Некоторые вопросы разработки политики безопасности информации // Сб. науч. трудов "Защита информации".— Киев: КМУЦА, 1999.—4 с.

Antoniuk A. O.

ABOUT THE SOME **NOTATIONS OF** SECURITY **INFORMATION**

The such important notions of National information security standard as properties of security information, security evaluation criteria, functionality profile of security, information security policy are considered. The problem of information security evaluation and the problem of suitable functionality profile choice are formulated.