УДК 004.056.53

В.Л. Шевченко, Д.С. Берестов

МЕТОД ПОШУКУ ПРОЕКТНИХ АЛЬТЕРНАТИВ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Розглянуто проблемні питання побудови системи захисту інформації від несанкціонованого доступу та формальна постановка завдання вибору оптимального профілю захищеності, запропоновано метод пошуку проектних альтернатив системи захисту інформації з урахуванням ресурсних обмежень на її реалізацію, визначено можливі практичні шляхи подальшої реалізації розробленого методу.

Ключові слова: система захисту інформації, проектні альтернативи, оптимізація.

Постановка проблеми

При створенні та розвитку автоматизованих систем (АС) потрібне гнучке формування і застосування сукупностей базових стандартів і нормативних документів різного рівня. У зв'язку із цією потребою сформувалося поняття “профілів”, як основного інструмента функціональної стандартизації, що являє собою сукупність декількох базових стандартів із підмножинами обов'язкових можливостей. Однак незважаючи на те, що дотепер уже частково розроблені і продовжують розроблятися міжнародні стандарти, спрямовані на забезпечення захисту інформації, а в Україні прийняті та діють нормативні документи [1, 2], що регламентують порядок організації робіт в області захисту комп'ютерної інформації, проблема захисту інформації, досить далека від остаточного рішення. Це пояснюється тим, що в даних стандартах і документах викладені тільки вимоги до функціональних послуг безпеки [3, 4], тобто, до функцій, які повинні бути реалізовані в системі захисту інформації (СЗІ) для забезпечення захисту інформації від несанкціонованого доступу. Ніяких методик побудови систем захисту інформації для АС (вибору необхідного набору механізмів захисту, що реалізують послуги безпеки), у даних документах не приводиться. Важливість постановки та вирішення зазначеної проблеми обумовлюється необхідністю уточнення та обґрунтування достатності застосовуваних заходів захисту інформації, оптимізації систем захисту, підвищення ефективності управління та контролю безпеки інформації.

При проведенні аналізу сучасного стану питання визначено, що підходи, які використовуються на практиці до захисту інформації, яка обробляється в АС визначаються наступними характеристиками:

- формалізованими вимогами до набору та параметрів механізмів захисту, що регламентують сучасні вимоги до забезпечення захисту;
- реальними механізмами захисту, які в більшості представлені вбудованими механізмами захисту операційних систем;
- існуючою статистикою загроз інформації.

Викладення основного матеріалу

Для розробки моделі функціонального профілю захищеності (ФПЗ) в [5] проведено аналіз складу та властивостей ФПЗ, в ході проведення якого виявилося, що для різних класів АС визначені семантично ідентичні ФПЗ, які, однак, на практиці принципово не можуть бути ідентичними внаслідок суттєвої різниці як за механізмами, так і можливостями реалізації, а також крім якісного їх порівняння, необхідно мати можливість їх кількісного порівняння, яке було б дуже корисним для полегшення вибору переліку функцій для захищених АС, мінімізації витрат на початкових етапах створення АС, при визначенні рівня захищеності АС.

Для аналізу складу та властивостей ФПЗ розглянуті його основні складові – послуги. Спроможність АС забезпечувати певний рівень захисту оброблюваної інформації визначається функціональними критеріями, які розбиті на чотири групи: конфіденційності, цілісності, доступності і спостереженості. Кожна з груп критеріїв описує послуги, що забезпечують захист відповідно від загроз одного з чотирьох основних типів: конфіденційності, цілісності, доступності і спостереженості. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз.

Семантичний опис ФПЗ складається з буквеного ідентифікатора, знака рівності і переліку послуг певних рівнів, взятого у фігурні дужки. Ідентифікатор включає: буквену

частину, що характеризує види загроз, від яких забезпечується захист (К, і/або Ц, і/або Д). Таким чином, виділяється 7 груп профілів, що забезпечують: К – конфіденційність, Ц – цілісність, Д – доступність, КЦ – конфіденційність і цілісність, КД – конфіденційність і доступність, ЦД – цілісність і доступність, КЦД – конфіденційність, цілісність і доступність.

Формальне представлення ФПЗ надамо у вигляді

$$КЦД = \{\{К_{ij}\},\{Ц_{ij}\},\{Д_{ij}\},\{Н_{ij}\}\}, \quad (1)$$

де *КДЦ* - ідентифікатор профілю, *К* - позначає конфіденційність, *Ц* - цілісність, *Д* - доступність, *Н* - спостережність, *i,j* - індекси послуг і рівнів відповідно до конфіденційності, цілісності, доступності та спостережності, причому для кожної із властивостей інформації, що захищається, визначені свої множини індексів.

Проведений аналіз показує, що найбільш складним є ФПЗ *КЦД,* це дозволяє для всіх профілів ввести єдине позначення, інтерпретуючи формулу (1) як вектор p, що має m компонент, тобто $p = (p_1,..., p_m)$. Числові ж значення компонентів можна дорівняти номеру рівня послуги. Якщо деяка послуга взагалі відсутня, то відповідний компонент вектору p дорівнює нулю. Таким чином ФПЗ можна звести в таблицю, в якій стовпці являють собою профілі, а рядки - відповідні послуги.

Рішення задачі вибору оптимального ФПЗ включає формування множини припустимих варіантів ФПЗ, визначення сукупності показників якості, завдання критерію оптимальності, а також вибір варіантів, оптимальних за заданим критерієм оптимальності.

Враховуючі наведений семантичний опис ФПЗ розглянемо його математичну модель. Нехай $\overline{P}$ – множина усіх можливих ФПЗ. Під $P \in \overline{P}$ будемо розуміти вектор розмірності m. Така розмірність введена для зручності та уніфікації опису, оскільки до складу багатьох профілів входять не всі послуги. У випадку відсутності якої-небудь послуги відповідний компонент дорівнює нулю.

За рахунок реалізації певного ФПЗ забезпечується виконання політики безпеки і зменшення збитку, що завдається впливом загроз. Позначимо загальний відвернений збиток через $S(P)$.

Формальна постановка задачі має вигляд [6]: знайти

$$P_o = \arg\max S(P)$$

$$P_o \in \overline{P}$$

при обмеженні (2)

$$C(P_o) \le C_{доп},$$

де P – деякий вектор, що характеризує ФПЗ, $\overline{P}$ – множина припустимих ФПЗ, P_0 – оптимальне значення вектора P, $C_{доп}$ – припустимі витрати на профіль.

Враховуючі, що кожна загроза інформації є наслідком реалізації деякої множини факторів, в разі реалізації яких може виникнути множина загроз $T = \{t_i\}$, $i = 1...n$. Кожну *i*-у загрозу будемо характеризувати ймовірністю її появи $P(t_i)$ та збитком, завдаваємим АС s_i.

Загрози повинні нейтралізуватися відповідними засобами та механізмами СЗІ, які забезпечуються реалізацією функціональних послуг. Оскільки функціональні послуги складають профіль, то імовірність усунення *i*-ой загрози повинна залежати від всього вектора p. Їх величини визначаються експертним шляхом. При цьому основною характеристикою СЗІ буде коефіцієнт її ефективності, наприклад відвернені збитки.

За рахунок реалізації необхідного ФПЗ забезпечується зменшення збитку *S*, завдаваємого впливом загроз.

Відвернений збиток в загальному вигляді виражається співвідношенням:

$$R = \sum_{j=1}^{n} P(t_j) P_{нейтр}(t_j) s_j \qquad (3)$$

Відвернений збиток за рахунок ліквідації впливу *i*-ой загрози:

$$\overline{R}_i = P(t_i) P_{нейтр}(t_i) s_i \qquad (4)$$

Збиток, s_i завдаваємий *i*-ою загрозою може визначатися в абсолютних одиницях: економічних втратах, тимчасових витратах, зниженні рівня захищеності, обсязі знищеної або зіпсованої інформації і т.д., які інтерпретуються бальними оцінками.

Виходячи з того, що ФПЗ являє собою ієрархічну систему критеріїв, для рішення поставленого завдання покладено метод вкладених скалярних згорток [7], при якому кожна з альтернатив (об'єктів) розглядається як сукупність елементів з різними властивостями, відмінними від властивостей усієї системи в цілому, що повністю відображає сутність ФПЗ (рис. 1), де *ФУ* – функційна послуга безпеки віднесена до одної їз груп: *К* – конфіденційності, *Ц* – цілісності, *Д* – доступності, *Н* – спостережності, де взважені компоненти векторних критеріїв нижчого рівня служать компонентами критеріїв вищого рівня (5), в свою чергу відображають цілі захищеності, які повинна досягнути СЗІ.

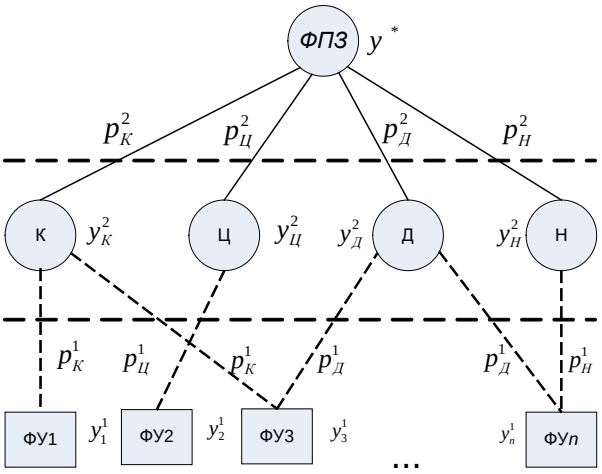

Рис.1. Структурна схема системи критеріїв якості альтернативи ФПЗ

$$y^* = ФПЗ^* = 1 - \frac{1}{\sum_{i=1}^{n^{(2)}} p^{(2)}_{n(2)} (1 - y^{(2)}_n)^{-1}} \qquad (5)$$

Визначення коефіцієнтів p на кожному рівні ієрархії виконано методом експертних оцінок по шкалі балів, де необхідно оцінити відносний вплив кожного часткового критерію нижчого рівня ієрархії на загальну оцінку n-ої властивості альтернативи на наступному рівні. Якісну оцінку альтернативи отримуємо шляхом співвідношення аналітичної оцінки зі зверненою нормованою фундаментальною шкалою Харрінгтона [8] представленою таблицею 1, в якій показаний зв'язок між якісними градаціями властивостей об'єктів і відповідними нормованими кількісними оцінками.

Табл. 1
Звернена нормована шкала Харінгтона

Категорія якості	Інтервали зверненої нормованої фундаментальної шкали оцінок
Висока	0,20-0,00
Добра	0,37-0,20
Задовільна	0,63 - 0,37
Низька	0,80-0,63
Недопустима	1,00 -0,80

Враховуючи розглянуті показники якості було проведене моделювання (численне дослідження) можливих варіантів залежностей R і $C(P)$ всіх підмножин m-елементного вектору p. Результатом якого є множина можливих рішень ФПЗ (X), яка надається у вигляді дискретного графіка (рис. 1), де кожне його значення відповідає реалізації певного ФПЗ.

Вибір рішень з множини X представляє задачу для розв'язання необхідно в математичних термінах виразити у вигляді максимізації (або мінімізації) деяку числову функцію f задану на множині X. У нашому випадку необхідно максимізувати відвернений збиток за рахунок реалізації ФПЗ із множини X (рис. 2), тобто побудувати множину парето-оптимальних рішень [9] $P_f(X)$, для якого діє наступне включення $P_f(X) \subset X$. Перехід від множини можливих рішень X до аналізу лише множини $P_f(X)$, дозволяє наочно представити парето-оптимальні ФПЗ [10] (рис. 3). У такий же спосіб для різних умов функціонування АС (різних множин можливих рішень X) може бути сформоване ціле сімейство парето-оптимальних ФПЗ (рис. 4), серед яких у подальшому буде обрана як конкретна крива, так і конкретне парето-оптимальне рішення.

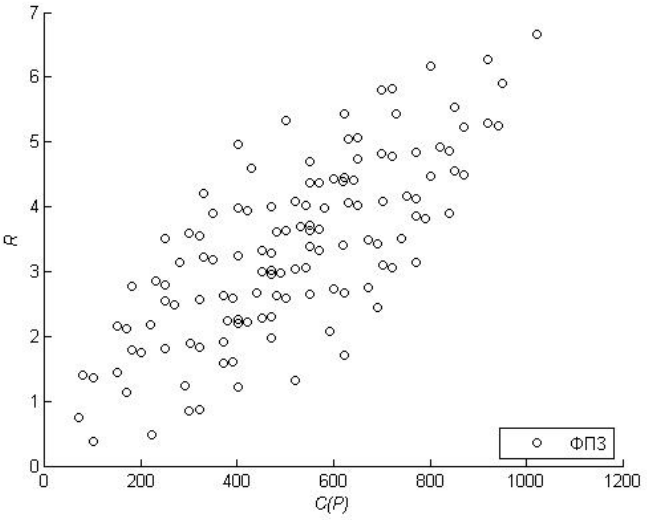

Рис. 2. Множина можливих ФПЗ

Для подальшого врахування забезпечення виконання політики безпеки АС, як набору норм і правил, та опираючись на визначення ФПЗ, була сформована вихідна припустима множина варіантів рішень виходячи з вимог політики безпеки, що висуваються до АС, тобто для підкласів ФПЗ (сценаріїв) із присутністю умовно-необхідних послуг, головною вимогою до яких є забезпечення К (конфіденційності), Ц (цілісності), Д (доступності), КЦ, КД, ЦД, КЦД. На рис. 4 представлені сімейства парето-оптимальних ФПЗ, які знайдені на множинах припустимих рішень побудованих для 5 груп ФПЗ із присутністю умовно-необхідних функціональних послуг безпеки по забезпеченню К, Ц, Д, КЦ, КД.

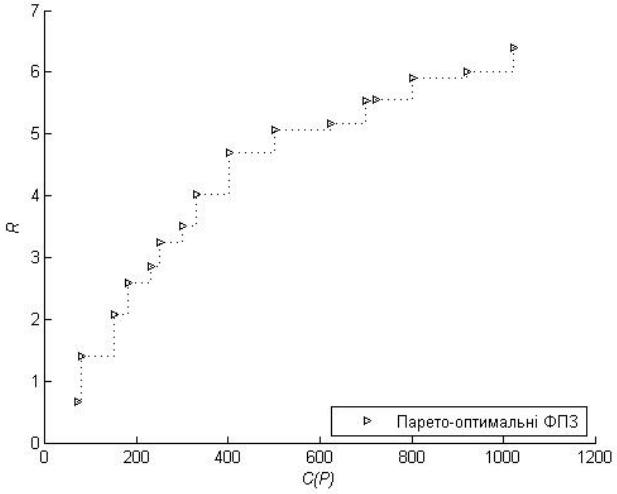

Рис. 3. Множина Парето-оптимальних ФПЗ

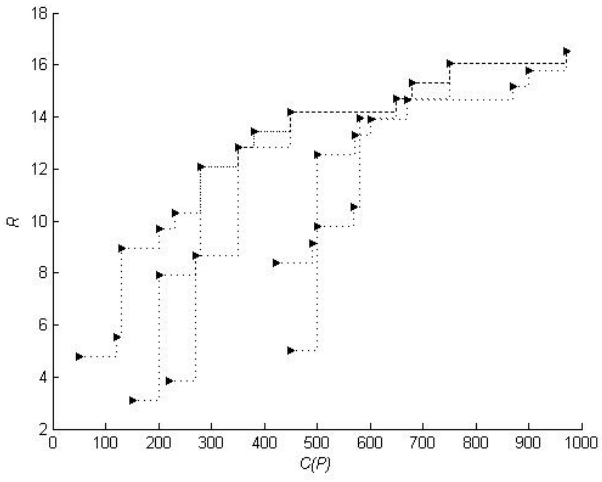

Рис. 4. Сімейство Парето-оптимальних ФПЗ

Враховуючі властивості ФПЗ та вимоги [1] розглянемо наступні можливі варіанти захисту інформації:

- досягнення необхідного рівня захисту інформації за мінімальних затрат і допустимого рівня обмежень видів діяльності;

- досягнення необхідного рівня захисту інформації за допустимих затрат і заданого рівня обмежень видів діяльності;
- досягнення максимального рівня захисту інформації за необхідних затрат і мінімального рівня обмежень видів діяльності.

Захист інформації, яка не є державною таємницею, забезпечується, як правило, застосуванням першого чи другого варіанту. Захист інформації, яка становить державну таємницю, забезпечується, як правило, застосуванням третього варіанту.

Виходячи з описаних варіантів захисту розглянуті такі варіанти введення формалізованих обмежень [11]. У першому випадку задача вибору являє собою максимізацію відверненого збитку R при ресурсних обмеженнях на C:

$$R \to \max \text{ за умови } C(p) \le C_{доп}, \tag{6}$$

де $C_{доп}$ - допустимі ресурсні обмеження на реалізацію ФПЗ.

У другому випадку мінімізація витрат на реалізацію ФПЗ (вектору p) при умові дотримання необхідного рівня захищеності АС:

$$C(p) \to \min \text{ за умови } R \ge R_{необ}, \tag{7}$$

де $R_{необ}$ - необхідний рівень захищеності АС за рахунок реалізації ФПЗ.

Численне дослідження показало, що при введенні певних обмежень на мінімально припустимий ефект, можлива ситуація коли оптимізаційне рішення відсутнє, для виходу з ситуації пропонується введення послуг (рис. 5, 6), які будуть виконуватись частково від заданого (нормативного) обсягу, що дозволяє зекономити ресурси, за рахунок яких можливо перерозподілити на користь інших послуг, які можуть надати більш високий приріст ефекту на одиницю витрат ресурсів.

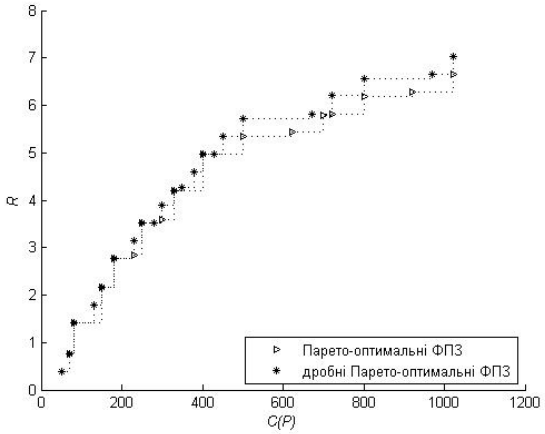

Рис. 5. Варіант *а* введення дрібних послуг

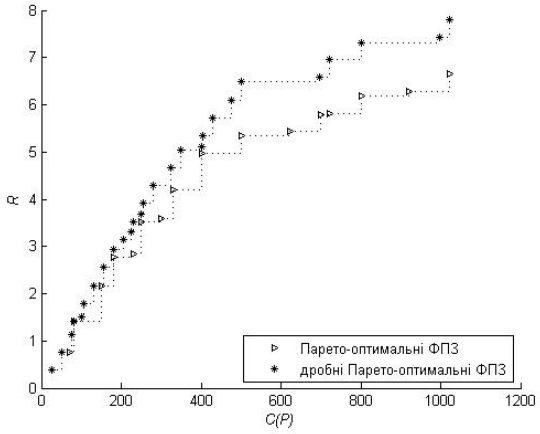

Рис. 6. Варіант *б* введення дрібних послуг

Залежності (рис. 5, 6) відповідають фізичному змісту ФПЗ, але не є зручними у використанні, оскільки ускладнено візуальне розрізнення сусідніх Парето-множин. Враховуючі результати проведеного моделювання введемо поняття критерію подібності рішень $\Delta_{доп}$. Якщо суміжні ділянки двох Парето-множин (d_1, d_2), які порівнюються, розрізнюються більше ніж на $\Delta_{доп}$ ($|d_1 - d_2| > \Delta_{доп}$), то ці ділянки вважаються різними. Якщо менше ($|d_1 - d_2| < \Delta_{доп}$), то вважаються однаковими. Виходячи з цього, зоною індиферентності рішень щодо рівня захищеності будемо вважати такі діапазони вартості

послуг, в яких виконується умова $|d_1 - d_2| < \Delta_{доп}$. Рішення, які ми порівнюємо, відповідають різним сценаріям побудови СЗІ. Отже зону індиферентності рішень будемо також називати зоною індиферентності сценаріїв. Якщо зона індиферентності визначена при порівнянні двох Парето-множин, то будемо називати її зоною другого порядку. Якщо при порівнянні n Парето-множин, то зоною індиферентності сценаріїв n-го порядку.

В зоні індиферентності сценарії вважаються рівноефективними. Отже в зоні індиферентності перевагу слід віддавати сценаріям більш простим в реалізації або таким, що задовольняють іншим додатковим вимогам, які можуть бути сформовані за допомогою введення обмежень на сукупності показників якості.

Висновки

Запропоновано метод вибору проектних альтернатив системи захисту інформації від несанкціонованого доступу, якій дозволяє визначити обрис системи захисту інформації від несанкціонованого доступу. Практична значимістьдослідження полягає в тому, що отримані результати дозволяють обґрунтувати вимоги до системи захисту інформації від несанкціонованого доступу шляхом чисельної та аналітичної оцінки проектних альтернатив, надають можливість формування обрису системи захисту інформації від несанкціонованого доступу та виявлення зон індиферентності можливих рішень.

Література

1. Захист інформації. Технічний захист інформації. Порядок проведення робіт: ДСТУ 3396.1-96 Державний стандарт України. — [Чинний від 1997-07-01]. — К. : Держспоживстандарт України, 1997. — IV, 5 с. — (Національний стандарт України)

2. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній систем: НД ТЗІ 3.7–003–05 — Офіц. вид. — К. : ДСТСЗІ СБ України, 2005. – 22 с

3. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.2–005–99 — Офіц. вид. — К. : ДСТСЗІ СБ України, 1999. – 23 с.

4. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5–004–99 — Офіц. вид. — К. : ДСТСЗІ СБ України, 1999. – 61 с.

5. Антонюк А. Аналіз складу профілів захищеності інформації / Анатолій Антонюк, Денис Берестов, Сергій Пустовіт // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : наук.-техн. збірник. – 10 вип., 2005. – С. 46 – 51.

6. Антонюк А. Постановка задачи оптимального выбора функционального профиля защищенности / Анатолий Антонюк, Денис Берестов, Владимир Шилин // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : наук.-техн. збірник. – 11 вип., 2005. – С. 47 – 50.

7. Воронин А. Н. Многокритериальные решения: модели и методы : монография / А. Н. Воронин, Ю. К. Зиатдинов, М. В. Куклинский. – К. : НАУ, 2011. – 348 с.

8. Адлер Ю. П. Планирование эксперимента при поиске оптимальных условий / Ю. П. Адлер, Е. В. Маркова, Ю. В. Грановский. – М.: Наука, 1977. - 280 с.

9. Подиновский В. В. Парето-оптимальные решения многокритериальных задач / Подиновский В. В., Ногин В. Д. – М.: Наука, Главная редакция физико-математической литературы, 1982. – 256 с.

10. Берестов Д. С. Побудова парето-оптимальних функціональних профілів захищеності / Д. С. Берестов, М. О. Гульков, В. А. Козачок // Збірник наукових праць. Вип. 1(39) / Редкол. Шевченко В. Л. (голова) та ін. – Київ. : ЦВСД НУОУ, 2009. – С. 89 – 94.

11. Шевченко В. Л. Звуження множини парето-оптимальних функціональних профілів захищеності з використанням експертних / В. Л. Шевченко, Д. С. Берестов, В. А. Козачок // Збірник наукових праць. Вип. 2(40) / Редкол. Шевченко В. Л. (голова) та ін. – Київ. : ЦВСД НУОУ, 2009. – С. 23 – 27.

Надійшла 11.08.2015 р. Рецензент: д.т.н., проф. Єрохін В.Ф.