УДК 004.056.5:34.03

ОБҐРУНТУВАННЯ РОЗУМНОЇ ДОСТАТНОСТІ СТРУКТУРИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВА

***Ю.І. Грицюк*[1], *О.О. Сівець*[2]**

Розглядаються особливості обґрунтування розумної достатності структури системи захисту інформаційних ресурсів (ІР) підприємства, яка б забезпечила безперервність бізнес-процесів підприємства, стійкість його функціонування та запобігання потенційним збиткам підприємства від реалізації інформаційних атак. Виявлено, що для ефективного використання інформації в той чи інший період її життєвого циклу, протягом якого вона є актуальною для потенційних конкурентів, необхідно вибрати такий режим доступу до неї, при якому ефект від її використання досягав би максимальної величини.

Ключові слова: інформаційна безпека (ІБ), комплексна система захисту інформації (КСЗІ), інформаційні ресурси (ІР), організаційна та математична модель ІБ підприємства.

Вступ. Стрімкий розвиток ІТ призвів до різкого нагромадження інформаційних ресурсів (ІР) підприємства [1]. Ці ресурси постійно піддаються різним інформаційним атакам з боку конкурентів, зловмисників чи просто хакерів [10, 15]. Наслідками таких атак може стати розголошення конфіденційної або спотворення цілісної інформації, нав'язування керівництву підприємства помилкової інформації, порушення доступу користувачів до достовірної інформації, а також відмови і збої роботи програмно-технічних систем [2].

Глобальні дослідження інформаційної безпеки [7] свідчать про те, що кількість дій зловмисників стосовно певних ІР підприємства не тільки постійно зростають, але й мають з плином часу набагато згубніші наслідки для нього [14]. Розуміючи це, керівники підприємств вимушені запроваджувати різні організаційні та програмно-технічні заходи щодо захисту важливих ІР [6, 9, 11].

Для вирішення поточних завдань захисту ІР підприємства впроваджується комплексна система захисту інформації (КСЗІ) [8]. Основна мета роботи КСЗІ направлена на недопущення: 1) несанкціонованого використання фінансових і матеріально-технічних цінностей підприємства; 2) спотворення цілісної інформації та перешкоджання електронному документообігу; 3) розголошення конфіденційної та витоку службової інформації, а також несанкціонованого доступу до неї; 4) порушення роботи програмно-технічних засобів забезпечення бізнес-діяльності підприємства.

Відповідно до *принципу розумної достатності* [3], КСЗІ має проектуватися так, щоб здійснювалася протидія тільки тим загрозам, що мають істотний вплив на *цілісність* та *конфіденційність ІР підприємства*. Система захисту ІР також маэ нейтралізувати чи послабити інформаційні атаки зловмисників або зменшити наслідки їх прояву. При цьому потенційні втрати підприємства від можливих реалізацій загроз не мають перевищувати гранично допустимих значень. Для виконання цих суперечливих завдань на стадії технічного проектування розробляється *модель системи захисту ІР підприємства* та визначається сукупність компонент функціональної структури КСЗІ, реалізація яких дасть змогу на належному рівні захистити ІР.

Однак, у доступній науковій літературі [1, 6, 9, 12, 14] немає адекватного теоретичного обґрунтування процесу побудови системи захист ІР підприємства, а також не наведено досконалі математичні моделі вибору раціонального варіанту КСЗІ. Тому обґрунтування достатньої структури системи захисту ІР підприємства залежно від їх вартості та конфіденційності є актуальним науково-практичним завданням, що сприяло виконанню цієї роботи та вимагає реалізації подальших досліджень.

Об'єкт дослідження – ефективність роботи КСЗІ на підприємстві.

Предмет дослідження – методи і засоби встановлення достатньої структури КСЗІ, впровадження якої забезпечить компроміс між конфіденційністю, доступністю та упущеною вигодою від використання ІР підприємства.

Мета роботи полягає в обґрунтуванні розумної достатності структури системи захисту ІР підприємства, яка дасть змогу визначити потенційні його збитки від витоку інформації, упущену вигоду від обмеженого її використання та необхідних витрат на надійний її захист.

Для реалізації зазначеної мети потрібно виконати такі основні завдання:

1) проаналізувати особливості визначення витрат на захист інформаційних ресурсів, виявити її недоліки та переваги з огляду на сучасні умови інформаційноъ безпеки;
2) проаналізувати наявні математичні моделі пошуку раціональної структури КСЗІ для впровадження на підприємстві, вибрати серед них найбільш придатні для прогнозування стану захищеності ІР;
3) зробити відповідні висновки та надати рекомендації щодо використання.

1. Особливості визначення витрат на захист інформаційних ресурсів

Для розуміння наведеного нижче, спробуємо згадати деякі основні поняття, які використовуються в системі захисту інформації.

Згідно з [6], *інформаційні ресурси* – документи і масиви даних у інформаційних системах (бібліотеках, архівах, фондах, банках даних, депозитаріях, музейних сховищах і т.і.). Розрізняють інформаційні ресурси *державні* та *недержавні*. До ІР підприємства [8] належать:

- комп'ютерні апаратні засоби та ПЗ;
- персональні дані працівників (аналітиків, системних програмістів, адміністраторів баз даних, фахівців зі створення комп'ютерних мереж);
- засоби підтримки, бази даних та бази знань;
- засоби комунікації та підтримки мереж;
- засоби та моделі підтримки прийняття рішень.

Інформація в FTP[1]-архівах розділена на три категорії:

- *захищена інформація*, режим доступу до якої визначається її власниками і дозволяється за спеціальною угодою із споживачем;
- *інформаційні ресурси обмеженого використання*, до яких належать, наприклад, програми класу shareware (Trumpet Winsock, Atis Mail, Netscape, і т.п.);

[1] проф. Ю.І. Грицюк, д-р техн. наук, НУ "Львівська політехніка", E-mail: yurii.i.hrytsiuk@lpnu.ua
[2] магістрант О.О. Сівець, НУ "Львівська політехніка", E-mail: olha.o.sivec@lpnu.ua

[1] FTP (англ. File Transfer Protocol) – протокол передачі файлів.

- *вільно розповсюджувані інформаційні ресурси* або freeware, якщо мова йде про ПЗ. До цих ресурсів належить все, що можна вільно отримати мережею без спеціальної реєстрації.

Конфіденційна інформація – інформація про фізичну особу (персональні дані) або юридичну особу, доступ та поширення якої можливі тільки за згодою її власників (тобто тих, кого ця інформація безпосередньо стосується) та на тих умовах, які вони вкажуть. Відповідно до Ст. 21 ЗУ "Про інформацію" конфіденційна інформація разом із службовою та таємною інформацією належить до *інформації з обмеженим доступом*.

Вважається [1], що конфіденційність виробничої та комерційної діяльності підприємства – *категорія* більше *економічна*, ніж *технічна*, ніж технічна. Захищені ІР підприємства від конкурентів чи зловмисників мають приносити певну користь її власникові та виправдовувати засоби, що витрачаються на забезпечення її цілісності та конфіденційності [2]. Якщо зловмисники прагнуть порушити цілісність інформації чи її спотворити, то конкуренти, навпаки, хочуть отримати тільки достовірну інформацію.

Ступінь конфіденційності інформації з плином часу зменшується і рідше збільшується (здебільшого, це секретна документація на технологічні процеси чи винаходи тощо). Тому конфіденційність інформації з плином часу має переглядатися її власниками, тобто вона має захищатися до тих пір, поки цього вимагають інтереси комерційної діяльності підприємства або національної безпеки держави [2, 4, 9].

Для найбільш ефективного використання інформації в той чи інший період її життєвого циклу (ЖЦ), протягом якого вона є актуальною для потенційних конкурентів, необхідно вибрати такий *режим її конфіденційності*, при якому ефект від її використання досягав би максимальної величини з урахуванням позитивних і негативних наслідків [8].

Зазвичай оцінювання позитивних і негативних наслідків від обмеженого доступу до інформації представляє значні труднощі. Ці наслідки можуть проявлятися в різних сферах діяльності підприємства, оцінюватися різними шкалами (кількісними і якісними) і різними одиницями вимірювання [11].

Доступність інформації – це властивість інформації при її обробленні технічними засобами, що забезпечує безперешкодний доступ до неї для проведення санкціонованих операцій ознайомлення, модифікації або знищення [14]. Для встановлення обмеженого доступу до ІР підприємства потрібно вирішити такі основні завдання:

- оцінити наявну інформацію за ступенем прояву різних загроз і визначити:
  - *можливі збитки* власника у разі її вільного використання;
  - *необхідні витрати* на захист інформації при встановленні обмеженого доступу до неї;
  - *упущеної вигоди* при вільному та обмеженому доступі до інформації;
- ранжувати інформацію та визначити величину збитків, витрат і вигод з тим, щоб отримати єдину систему оцінок, які характеризують інтегральний ефект від вільного та обмеженого доступу до інформації.

Для вирішення цих завдань необхідно вибрати такий *режим доступу до інформації*, який би протягом періоду її активного ЖЦ забезпечував максимальний ефект від використання.

Встановлення певної *конфіденційності ІР підприємства*, а також певних *обмежень на доступ до інформації* протягом деякого періоду її ЖЦ є одним із способів ефективного ***управління об'єктами інформаційної безпеки підприємства***, спрямованого на досягнення максимального ефекту від впровадження КСЗІ на підприємстві [12].

Можливість прояву зловмисників у динаміці ЖЦ інформації оцінюється суб'єктивною ймовірністю. Для визначення потенційних збитків від витоку інформації, упущених вигод від обмеженого її використання та необхідних витрат на надійний захист ІР застосовується суб'єктивне оцінювання інформації експертами, що добре розуміють її цінність, а також взаємозв'язок з вказаними чинниками [4, 8].

На підставі порівняння експертних оцінок окремих чинників (збитку, витрат і вигод) з урахуванням можливості позитивного та негативного їх прояву обчислюється значення ***інтегрального показника вибраного режиму доступу до інформації*** за формулою

$$W(t) = U(t) \cdot p_t - V(t) \cdot q_t - Z(t),\ t = \overline{1,T},$$

де: T – тривалість ЖЦ інформації; $U(t)$, $V(t)$ – потенційно можлива величина відповідно збитку та вигод при вільному використанні інформації в t-ий період її ЖЦ; p_t, q_t – ймовірність прояву потенційного збитку і прояву упущених вигод в t-ий період ЖЦ інформації; $Z(t)$ – величина необхідних витрат на захист інформації в t-ий період її ЖЦ.

У випадку, якщо розраховане значення інтегрального показника $W(t)$ виявиться більшим від нуля, то доцільно внести цю інформацію до *переліку відомостей з обмеженим доступом*. Приналежність інформації до ІР підприємства, що підлягають надійному захисту від несанкціонованих і ненавмисних дій, вважається тоді, коли величина заподіяного збитку $U(t)$ внаслідок реалізації загроз перевищує величину витрат на її захист $Z(t)$, тобто $U(t) > Z(t)$.

Однак, як зазначалося вище, секретність чи конфіденційність інформації – категорія економічна, тому з плином часу вимагає перегляду. Спробуємо дещо детальніше з'ясувати сутність економічної категорії інформації, а також розібратися у основних причинах потреби перегляду її цінності з плином часу.

Для наочної ілюстрації залежності параметрів і характеристик ІР підприємства, що визначають умови їх захисту, може слугувати *модель оцінювання параметрів системи захисту ІР підприємства*, наведена на рис. 1. В цій моделі показано якісний взаємозв'язок таких параметрів системи захисту ІР підприємства: їх цінність (G), необхідний рівень захисту (P), тривалість забезпечення конфіденційності (T). Модель також враховує економічні характеристики впровадження таких захисних заходів, як витрати на забезпечення потрібного рівня захисту інформації та можливі втрати (збитки) унаслідок недосконалості системи її захисту.

На рис. 1 введено такі позначення: G – цінність ІР підприємства – об'єкта конфіденційності (наприклад, науково-технічного звіту чи проектно-конструкторської документації, що містить опис нової технології); $G(T)$ – характеристика старіння інформації – зменшення цінності ІР підприємства з плином часу; P

– рівень (ймовірність) забезпечення захисту інформації (практично $0{,}5 \le P < 1{,}0$, оскільки абсолютно надійний її захист неможливий); $Z_1(P)$ – допустимі витрати на захист інформації як функція від необхідного рівня її захисту. Ці витрати зростають при підвищенні вимог до рівня захисту інформації. Прагнення досягти дуже високого рівня захисту інформації зазвичай призводить до різкого зростання витрат, які можуть перевищити цінність самої інформації, що захищається.

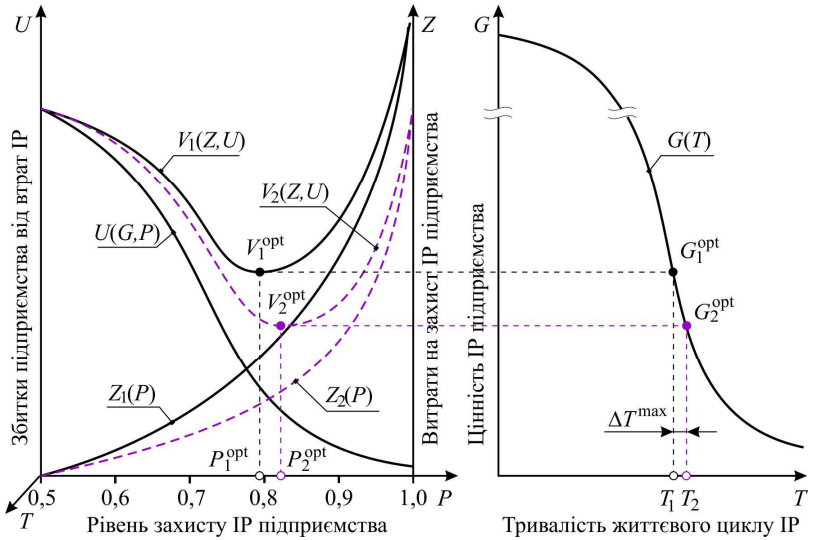

Рис. 1. Модель оцінювання параметрів системи захисту IP підприємства

Можливі втрати (збитки) власника інформації $U(G,P)$, понесені унаслідок неналежного рівня її захисту, є функцією від цінності самої інформації $G(T)$ та наявного рівня її захисту P. У нульовому наближенні ці втрати апроксимуються добутком цінності інформації $G(T)$ на ймовірність її витоку H, тобто $G(T)\cdot H$. Ймовірність витоку інформації знаходиться в зворотній залежності до досягнутого рівня її захисту, $H = (1 - P)$. При такому допущенні $U(G,P) = G(T)\cdot(1 - P)$.

З рис. 1 видно, що витрати, пов'язані із забезпеченням конфіденційності інформації, становлять

$$V(Z,U) = Z_1(P) + U(G,P).$$

При цьому, оптимальний рівень захисту інформації відповідає мінімуму суми витрат на захист $Z_1(P)$ і можливих втрат $U(G,P)$ унаслідок неповноти захисту інформації, а саме

$$V^{opt}(Z,U) = Z_1(P) + U(G,P) \to \min.$$

Прагнення перевищити цей рівень може призвести до різкого зростання витрат $Z_1(P)$ на забезпечення захисту інформації. Зниження ж рівня захисту призведе до збільшення можливих втрат $U(G,P)$ унаслідок недосконалості системи захисту IP підприємства.

Якщо прийняти, що $\Delta T = T_2 - T_1$ – часовий інтервал, впродовж якого конфіденційність інформації може бути економічно виправданою, то його максимальне значення становить $\Delta T^{max} = \Delta T(G(T), V^{opt}(Z, U))$. При цьому, як показано на рис. 1, величина витрат на захист інформації $Z_1(P)$ в сумі з можливими збитками від її втрати $U(G,P)$ менша від вартості самої інформації $G(T)$ з урахуванням її знецінення. Для спрощення викладення матеріалу, нехтуємо залежністю $Z(P,T)$, тобто зростанням сумарних витрат на захист IP підприємства з плином часу. Це можна легко побачити, подавши ліву частину рисунка в тривимірних координатах, а саме $PT0U$.

З викладеного вище матеріалу видно, що значення величини досягнутого рівня захисту інформації $Z(P)$ залежить як мінімум від двох параметрів: R_{pi} – використовуваних ресурсів (зокрема, матеріальних витрат на забезпечення захисту) і E_{pim} – ефективності механізму захисту інформації (використання цих ресурсів). Тому в рамках математичної моделі $Z(P) = f(R_{pi}, E_{pim})$ можлива така постановка оптимізаційної задачі.

Фактично E_{pim} – показник досконалості створеної та наявної системи захисту IP підприємства. При дещо якіснішому проектуванні КСЗІ та практичній реалізації необхідної множини засобів і механізмів захисту, тобто максимально ефективному залученні всіх наявних ресурсів, один і той же рівень забезпечення захисту інформації може бути досягнутий при менших матеріальних витратах. На рис. 1 це переконливо ілюструє крива $Z_2(P)$. При цьому відповідно оптимальний рівень захисту інформації P_2^{opt} може бути вищим порівняно з P_1^{opt}, а економічно виправдана тривалість конфіденційності інформації ΔT – більшою, тобто $T_2 = T_1 + \Delta T$.

Практичну реалізацію цієї задачі спробуємо показати нижче. Однак, на рис. 2 показано деякі результати моделювання параметрів системи захисту IP фірми "Світанок" АТЗТ – Львів.

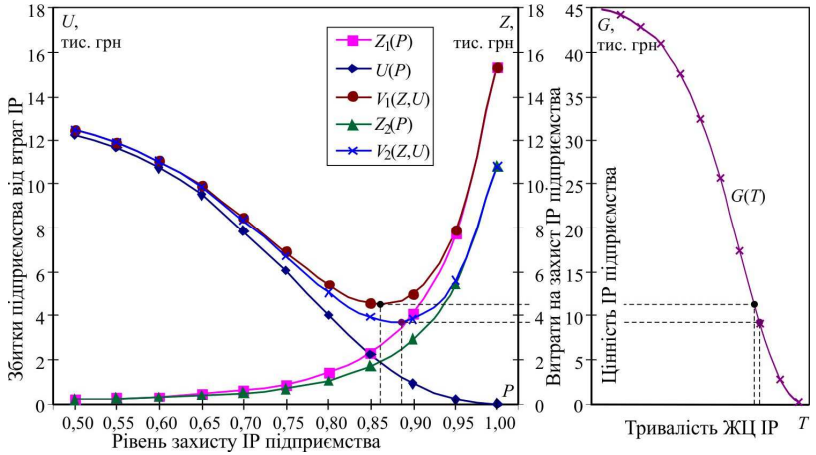

Рис. 2. Результати моделювання параметрів системи захисту IP підприємства

2. Моделі вибору раціонального варіанту КСЗІ на підприємстві

Відомо [5], що при визначенні раціонального варіанта впровадження КСЗІ на підприємстві широко використовуються методи порівняльного аналізу, які ґрунтуються на співставленні обсягу допустимих витрат (*S*) на побудову ефективної системи захисту ІР з нормативним значенням рівня їх захисту (*R*). Обидві задачі математично еквівалентні та можуть розв'язуватися методами багатопараметричної оптимізації. Традиційно в таких задачах застосовується методика формування множини Парето-оптимальних рішень [13]. Шкода, але він має обмежене практичне застосування, зумовлене значною розмірністю отримуваної множини не домінантних рішень і забороною компромісу при допустимих значеннях параметрів {*S*, *R*}.

Нехай $\tilde{\Pi} = \{\pi_j,\ j = \overline{1, p}\}$ – множина Парето-оптимальних проектних рішень щодо побудови системи захисту ІР; $\tilde{D} = \{d_j,\ j = \overline{1, n}\}$ – множина допустимих рішень, при реалізації яких виконуються *функціональні* та *критеріальні обмеження* $G(\tilde{\tilde{X}}^*) \le 0$ (зокрема, обмеження на рівень залишкового ризику реалізації інформаційних атак та ін.). Тоді пошук раціонального варіанту КСЗІ зводиться до такої постановки багатопараметричної задачі вибору [5]: знайти такий варіант системи захисту ІР підприємства $\tilde{\tilde{X}}^* \in \tilde{\Pi} \subset \tilde{D}$, який відповідає умові однієї із таких задач:

- мінімізація витрат на побудову системи захисту ІР підприємства

$$S = f_S(\tilde{\tilde{X}}^*) \to \min_{\tilde{\tilde{X}}^* \in \tilde{\Pi} \subset \tilde{D}} \Rightarrow i^*,\ j^*,\ \tilde{\tilde{X}}^* \mapsto x_{i^*, j^*} \in \tilde{\tilde{X}};\ R \ge R_{\text{доп}}; \qquad (1)$$

- максимізація рівня захисту ІР підприємства, що забезпечується вибраним варіантом

$$R = f_R(\tilde{\tilde{X}}^*) \to \max_{\tilde{\tilde{X}}^* \in \tilde{\Pi} \subset \tilde{D}} \Rightarrow i^*,\ j^*,\ \tilde{\tilde{X}}^* \mapsto x_{i^*, j^*} \in \tilde{\tilde{X}};\ S \ge S_{\text{доп}}, \qquad (2)$$

де: M – кількість ІР підприємства; $\tilde{N} = \{N_i, i = \overline{1, M}\}$ – кількість засобів, які можуть захищати *i*-ий ІР; $\tilde{\tilde{X}} = \{\tilde{X} = \{x_{ij} \in \{0;1\},\ j = \overline{1, N_i}\},\ i = \overline{1, M}\}$ – можливість використання *j*-го засобу для захисту *i*-го ІР; $S_{\text{доп}}$ – допустима вартість побудови КСЗІ; $R_{\text{доп}}$ – нормативне значення захисту ІР підприємства [8]: < 0,50 – слабкий захист; 0,51-0,75 – середній захист; 0,76-0,87 – підвищений захист; 0,88-0,95 – сильний захист; 0,96-0,98 – надмірний захист; 0,99-0,9999 – абсолютний захист

Для розв'язання задачі пошуку раціонального варіанту КСЗІ доцільно використати метод послідовних поступок [5]. В цьому методі виділяється множина часткових показників рівня захисту ІР, що мають перевагу над рештою показниками, які переводяться в систему обмежень. *Метод послідовних поступок* дає змогу контролювати значення критеріїв оптимізації, тобто на кожному етапі розрахунку можна встановити, за рахунок якої поступки в одному частковому критерії отримується виграш за іншими критеріями. Така можливість базується на розташуванні часткових критеріїв у порядку убування їх важливості й призначенні поступок (тобто максимальних відхилень від оптимального значення), допустимих для кожного критерію.

Модель мінімізації витрат на побудову системи захисту ІР підприємства [5]. Нехай $x_{ij} = 1$, якщо *j*-ий засіб використовується для захисту *i*-го ІР, і $x_{ij} = 0$ – інакше (при цьому допускається, що *j*-ий засіб використовується для захисту від *i*-ої загрози). Потрібно мінімізувати витрати на побудову ефективної системи захисту ІР підприємства

$$S = \sum_{i=1}^{M} \left(c_i + \sum_{j=1}^{N_i} s_{ij} x_{ij} \right) \to \min_{\tilde{\tilde{X}}^* \in \tilde{\Pi} \subset \tilde{D}} \Rightarrow i^*,\ j^*,\ \tilde{\tilde{X}}^* \mapsto x_{i^*, j^*} \in \tilde{\tilde{X}}, \qquad (3)$$

при дотриманні таких обмежень:

$$\sum_{i=1}^{M} \alpha_i \sum_{j=1}^{N_i} r_{ij} x_{ij} \ge R_{\text{доп}};\ \sum_{i=1}^{M} \alpha_i = 1;\ \sum_{j=1}^{N_i} x_{ij} = 1;\ x_{ij} \in \{0;1\},\ \forall j \in N_i,\ \forall i \in M, \qquad (4)$$

де: $\tilde{C} = \{c_i, i = \overline{1, M}\}$ – одноразові витрати на захист *i*-го ІР; $\tilde{\text{A}} = \{\alpha_i, i = \overline{1, M}\}$ – ваговий коефіцієнт важливості *i*-го ІР; $\tilde{\tilde{S}} = \{\tilde{S}_i = \{s_{ij},\ j = \overline{1, N_i}\}, i = \overline{1, M}\}$ – розрахункові витрати на побудову *j*-го засобу для захисту *i*-го ІР; $\tilde{\tilde{R}} = \{\tilde{R}_i = \{r_{ij},\ j = \overline{1, N_i}\}, i = \overline{1, M}\}$ – розрахункове значення якості роботи *j*-го програмного-технічного засобу при захисті *i*-го ІР (вказує на те, яка частина інформаційних атак відбивається *j*-им засобом).

Модель максимізації рівня захисту ІР підприємства описує двоїну задачу за відношенням до моделі мінімізації витрат на побудову ефективної системи захисту ІР. В цьому випадку обмеження на рівень захисту ІР стає критерієм оптимізації, а критерій – обмеженням. Отже, в цій постановці задачі потрібно максимізувати рівень захисту ІР підприємства

$$R = \sum_{i=1}^{M} \alpha_i \sum_{j=1}^{N_i} r_{ij} x_{ij} \to \max_{\tilde{\tilde{X}}^* \in \tilde{\Pi} \subset \tilde{D}} \Rightarrow i^*,\ j^*,\ \tilde{\tilde{X}}^* \mapsto x_{i^*, j^*} \in \tilde{\tilde{X}} \qquad (5)$$

при дотриманні таких обмежень:

$$S = \sum_{i=1}^{M} \left(c_i + \sum_{j=1}^{N_i} s_{ij} x_{ij} \right) \le S_{\text{доп}};\ \sum_{i=1}^{M} \alpha_i = 1;\ \sum_{j=1}^{N_i} x_{ij} = 1;\ x_{ij} \in \{0;1\},\ \forall j \in N_i,\ \forall i \in M. \qquad (6)$$

Порівняння варіантів побудови системи захисту ІР підприємства базується на аналізі багатопараметричного критерію, значення якого залежить від множини часткових показників якості роботи КСЗІ. Як випливає з постановки початкової задачі оптимізації (1) або (2), підставою для отримання висновку про абсолютну перевагу одних показників комерційної діяльності підприємства над іншими слугує ступінь відмінності окремих показників за важливістю. При цьому, згідно з методом послідовних поступок, порівняння ефективності варіантів системи захисту ІР з іншими здійснюється тільки за найважливішим показником без урахування останніх, потім тільки за другим показником і т.д. У загальному вигляді задача багатокритеріальної оптимізації еквівалентна задачі знаходження умовного екстремуму тільки за основним критерієм:

$$\tilde{F} = \left\{ F_i = \arg_i \left\{ \min\{v_{ij},\ j = \overline{1, N_i^{\text{пр}}}\} \right\},\ i = \overline{1, M^{\text{пя}}} \right\},\ v_{ij}^{\min} \le v_{ij} \le v_{ij}^{\max}, \qquad (7)$$

де: $M^{\text{пя}}$ – кількість показників захисту ІР підприємства; $\tilde{N}^{\text{пр}} = \{N_i^{\text{пр}}, i = \overline{1, M^{\text{пя}}}\}$ – кількість проектних рішень побудови системи захисту ІР за *i*-им показником її

якості роботи; $\tilde{\tilde{V}} = \{\tilde{V}_i = \{v_{ij}, j = \overline{1, N_i^{\text{пр}}}\}, i = \overline{1, M^{\text{пя}}}\}$ – значення i-го показники рівня захисту ІР за j-им варіантом проектного рішення її побудови.

Інформація про абсолютну перевагу окремих показників комерційної діяльності підприємства дає змогу проранжувати ($F_1 \succ F_2 \succ ... \succ F_{M^{\text{пя}}}$) можливі варіанти проектних рішень побудови системи захисту ІР з використанням процедури лексикографічного оцінювання. Реалізація цієї процедури передбачає декомпозицію початкової багатокритеріальної задачі оптимізації методом послідовних поступок [5] у певну послідовність задач оптимізації за ієрархічно впорядкованими скалярними показниками $\tilde{V}_i, i = \overline{1, M^{\text{пя}}}$.

Отже, передбачається, що перший показник v_1 є важливішим від другого v_2, другий v_2 – від третього v_3, і т.д. до $v_{M^{\text{пя}}}$, так що $\boldsymbol{G}_F \supseteq F_1 \supseteq F_2 \supseteq ... \supseteq F_{M^{\text{пя}}}$, за умови, що $F_{M^{\text{пя}}} \neq 0$. Водночас, кожен подальший частковий показник звужує множину варіантів проектних рішень $\boldsymbol{G}_F$, які отримуються за допомогою всіх попередніх показників. Це означає, що якщо в початковій задачі багатокритеріальної оптимізації з одним скалярним показником є декілька рішень і для подальшого вибору послідовно застосовуються додаткові показники, то отримувані внаслідок прийнятої стратегії розв'язання задачі рішення будуть оптимальними для відповідної лексикографічної задачі з векторним показником, що складається зі всіх цих по черзі взятих показників. Очевидно, для прийнятої моделі мінімізації витрат на побудову ефективної системи захисту ІР вирішальне правило вибору конкретного варіанту проектного рішення має такий вигляд

$$\hat{i} = \underset{i \in M^{\text{пя}}}{\arg} \left\{ \min\{s_{ij} \big| r_{ij} \geq R_{\text{доп}}, j = \overline{1, N_i^{\text{пр}}}\} \right\}. \quad (9)$$

Аналогічно в моделі максимізації рівня захисту ІР підприємства вирішальне правило вибору конкретного варіанту проектного рішення має такий вигляд:

$$\hat{i} = \underset{i \in M^{\text{пя}}}{\arg} \left\{ \max\{r_{ij} \big| s_{ij} \geq S_{\text{доп}}, j = \overline{1, N_i^{\text{пр}}}\} \right\}. \quad (10)$$

Оцінювання значення величини $S_{\text{доп}}$ не викликає труднощів і визначається фінансовою спроможністю підприємства, а також ризиками (збитком) від реалізації інформаційних атак на структуру системи захисту ІР підприємства.

Висновки

1. З'ясовано, що для вирішення завдань захисту ІР підприємства впроваджується КСЗІ, головною метою роботи якої є забезпечення безперервності бізнес-процесів підприємства, стійкого його функціонування та запобігання потенційним збиткам підприємства від реалізації інформаційних атак.

2. Виявлено, що для ефективного використання інформації в той чи інший період її ЖЦ, протягом якого вона є актуальною для потенційних конкурентів, необхідно вибрати такий режим доступу до неї, при якому ефект від її використання досягав би максимальної величини. Встановлення певної конфіденційності ІР підприємства, а також певних обмежень на доступ до інформації протягом деякого періоду її ЖЦ є одним із способів ефективного управління об'єктами інформаційної безпеки підприємства, спрямованого на досягнення максимального ефекту від впровадження КСЗІ на підприємстві.

3. Проаналізовано наявні математичні моделі пошуку раціонального варіанта впровадження КСЗІ на підприємстві, вибрано серед них найбільш придатні, які зводиться до багатопараметричної задачі вибору такого варіанту проектного рішення, який би відповідав умові мінімізації витрат на побудову ефективної системи захисту ІР або умові максимізації рівня захисту ІР. Обидві задачі математично еквівалентні та можуть розв'язуватися методом послідовних поступок.

Література

1. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій / Г.Я. Аніловська. [Електронний ресурс]. – Доступний з http://nbuv.gov.ua/portal/chem_biol/nvnltu/18_9/270_Anilowska_18_9.pdf

2. Бармута Андрей. Утечка информации в корпоративной сети: угроза виртуальная, защита реальная / Андрей Бармута. [Электронный ресурс]. – Доступный с http://www.itsec.ru/articles2/in-ch-sec/ytechka-informacii-v-korporativnoi-seti-ygroza-virtyalnaya-zashita-realnaya

3. Грицюк Ю.І. Обгрунтування принципу розумної достатності функціонування КСЗІ на підприємстві / Ю.І. Грицюк // Захист інформації і безпека інформаційних систем : матер. IV-ої Міжнар. наук.-техн. конф., м. Львів, 04–05 червня 2015 р. – Львів : Вид-во НУ "Львівська політехніка". – 2015. – С. 39-40.

4. Грицюк Юрій. Обгрунтування потреби захисту інформаційних ресурсів підприємства / Юрій Грицюк, Ольга Сівець // Інформаційна безпека в сучасному суспільстві : матер. II Міжнар. наук.-техн. конф., 24-25 листопада 2016, м. Львів, Україна. – Львів : Вид-во ЛДУ БЖД, 2016. – С. 41-43.

5. Гатчин Ю.А. Математические модели оценки инфраструктуры системы защиты информации на предприятии / Ю.А. Гатчин, И.О. Жаринов, А.Г. Коробейников // Научно-технический вестник информационных технологий, механики и оптики. – СПб. : Изд-во Университета ИТМО. – 2012. – Т. 12, № 2(78). – С. 92-05.

6. Герасименко О.В. Інформаційна безпека підприємства: поняття та методи її забезпечення / О.В. Герасименко, А.В. Козак. [Електронний ресурс]. – Доступний з http://intkonf.org/ken-gerasimenko-ov-kozak-av-informatsiyna-bezpeka-pidpriemstva-ponyattya-ta-metodi-yiyi-za-bezpechennya/

7. Глобальное исследование инцидентов внутренней информационной безопасности. [Электронный ресурс]. – Доступный с http://www.securitylab.ru/analytics/291018.php

8. Грибунин В.Г. Комплексные системы защиты информации на предприятии / В.Г. Грибунин, В.В. Чудовский. – М. : Изд. центр "Академия", 2009. – 416 с.

9. Гриджук Г.С. Систематизація методів інформаційної безпеки підприємства / Г.С. Гриджук. [Електронний ресурс]. – Доступний з http://www.nbuv.gov.ua/portal/natural/Vntu/2009_19_1/pdf/64.pdf

10. Корпоративная информационная безопасность: виды IT-угроз. [Электронный ресурс]. – Доступный с http://www.razumny.ru/stat/it-ugrozy.html

11. Кунинець А.І. Інформаційні загрози та проблеми забезпечення інформаційної безпеки промислових компаній / А.І. Кунинець, Ю.І. Грицюк // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2013. – Вип. 22.2. – С. 352-360.

12. Мальцев А. Методика оценки состояния инженерно-технической защищенности объектов / А. Мальцев // Технологии защиты : сб. науч. тр. – 2010. – № 4. – С. 15-21.

13. Ногин В.Д. Проблема сужения множества Парето: подходы к решению / В.Д. Ногин // Искусственный интеллект и принятие решений : сб. науч. тр. – 2008. – № 1. – С. 98-112.

14. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко. [Електронний ресурс]. – Доступний з http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf

15. Утечка информации – угроза корпоративной безопасности. [Электронный ресурс]. – Доступный с http://www.staffcop.ru/articles/Information_leakage.php

Надійшла до редакції 16.11.2016 р.

Грыцюк Ю.И., Сивец О.О. **Обоснование разумной достаточности структуры системы защиты информационных ресурсов предприятия**

Рассматриваются особенности обоснования разумной достаточности структуры системы защиты информационных ресурсов (ИР) предприятия, обеспечивающая непрерывность бизнес-процессов предприятия, устойчивость его функционирования и предотвращающая потенциальные убытки предприятия от реализации информационных атак. Выявлено, что для эффективного использования информации в тот или иной период ее жизненного цикла, в течение которого она актуальна для потенциальных конкурентов, необходимо выбрать такой режим доступа к ней, при котором эффект от ее использования достигал бы максимальной величины.

Ключевые слова: информационная безопасность (ИБ), комплексная система защиты информации (КСЗИ), информационные ресурсы (ИР), организационная и математическая модель ИБ предприятия.

Gryciuk Yu.I., Sivec O.O. **Ground of Reasonable Sufficientness of Structure of the System of Defence of Informative Resources of Enterprise**

The features of ground of principle of reasonable sufficientness of the system of defence are examined of the informative resources (IR) of the enterprise, what would provide continuity of business processes of the enterprise, firmness of its functioning and prevention of potential losses of the enterprise from realization of informative attacks. It was discovered that for the effective use of information in one or another period of its life cycle during which it is an actual for the potential competitors, it is necessary to choose such access mode, at which an effect from its use would reach a maximal value to it.

Keywords: information protection (IP), complex system of information protection (CIPS), information resources (IR), organizational and mathematical model of enterprise information protection.

УДК 004.03

ОЦІНЮВАННЯ АСПЕКТНОЇ РЕОРГАНІЗАЦІЇ ПРОГРАМНОГО КОДУ ЗА ХАРАКТЕРИСТИКОЮ СУПРОВОДЖУВАНОСТІ

Є.В. Левус[1], О.М. Вітоль[2], О.Б. Бода[3]

Розглянуто проблему складності супроводу програмного забезпечення. Проаналізовано застосування аспектно-орієнтованого програмування для забезпечення якісної характеристики програм – супроводжуваності. Проведено дослідження на прикладі прототипу програмної системи онлайн-банкінг для випадку об'єктно-орієнтованої та аспектно-орієнтованої реалізації. Отримані результати свідчать про підвищення індексу супроводжуваності для випадків локалізації наскрізної функціональності – логування, опрацювання виняткових ситуацій, перевірка прав доступу. Індекс супроводжуваності можна розглядати як вагове оцінювання на основі кількості рядків коду (*LOC*), цикломатичної складності (*CC*) та об'єму холстеда (*HV*). Є потреба у вдосконаленні вагового оцінювання супроводжуваності.

Ключові слова: супровід програмного забезпечення, модуль системи, об'єктно-орієнтоване програмування, аспектно-орієнтована реалізація, аспект, наскрізна функціональність, метрика коду, індекс супроводжуваності.

Вступ. Актуальність супроводу ПЗ і проблема його складності. Одна з найголовніших стратегій інженерії програмного забезпечення (ПЗ) – повторне використання компонент – покликана зменшити витрати часу та коштів у процесі розроблення ПЗ. У ракурсі рентабельного розроблення ПЗ особливу увагу приділяють супроводу – етапу життєвого циклу розроблення програмних систем. Однак складність супроводу настільки велика, що зумовлює найчастіше розгляд його як окремого проекту і напряму залежить від складності раніше розробленої системи [1]. Виникає питання, чи можна передбачити в ході первинного розроблення програмної системи певні її властивості, які забезпечать у майбутньому ефективний супровід.

Управління складністю типово здійснюється на основі декомпозиції системи на логічно-змістовні модулі [2]. Від критерію декомпозиції залежить наскільки легко буде модифікувати систему, тобто чи вона здатна до розвитку.

Модуль можна розглядати в найпростішому випадку як безсистемне угруповання, що є штучним об'єднанням різних програмних об'єктів. *ООП*-декомпозиція системи є більш гнучкою, вона відповідає сутностям предметної області. Проте все ж недоліком є нелокалізована функціональність, що затрудняє внесення змін у вже готову систему. У такому випадку говорять про наскрізну функціональність як перешкоду для зручного розширення функціональних можливостей системи [3, 4]. Ідею локалізації наскрізної функціональності реалізовано у пост-об'єктних технологіях. Однією з таких перспективних технологій є аспектно-орієнтоване програмування (*АОП*) [5].

Отже, існує проблема зростання складності супроводу ПЗ. Актуальним є пошук рішення для програмного відокремлення наскрізної функціональності від основної логіки програми, що зменшить складність програмної системи, і, відповідно, знизить вартість і складність її супроводу.

Стан вирішення проблеми зростання складності ПЗ внаслідок використання *АОП*. Дослідження ефективності застосування *АОП* проводять фахівці академічних установ, працівники дослідницьких лабораторій при відомих корпораціях індустрії ПЗ. Особливістю цих досліджень є те, що оцінювання ефективності застосування *АОП* здійснюється за різними критеріями.

У [4, 6, 7] доведено ефективність застосування ПООТ, де в розумінні авторів ефективність – це зменшення коефіцієнта питомої ваги наскрізної функціональності (Crosscuting Ratio – CR). Зокрема, у [4] відображено, що *ООП* недостатньо для вирішення проблеми наскрізної функціональності (ефективність всього 6,7 %), а найкращим рішенням є *АОП*, результат використання якого забезпечив більше 70 % ефективності.

У [8] проведено порівняння ефективності застосування *АОП* з *ООП* для модуля захисту розподіленої системи теплового проектування за рядом метрик. Аспектна реалізація має меншу кількість стрічок коду, є кращою з точки зору топологічної складності, має кращу функціональну декомпозицію. Проте є складність розуміння *АОП*-коду. Зроблено висновок, що використання *АОП* покращує надійність ПЗ завдяки меншій складності проекту.

У [9] *АОП* застосовано для покращення захисту програмної системи. Також проаналізовано слабкі та сильні сторони *АОП*. Зроблено висновок, що *АОП* – це надійна парадигма програмування для покращення рівня захисту систем. Серед недоліків автори зазначили те, що в *АОП* є деякі обмеження, спричинені недостатнім розвитком мовних засобів.

[1] доц. Є.В. Левус, канд. техн. наук – НУ "Львівська політехніка";
[2] магістр О.М. Вітоль – НУ "Львівська політехніка";
[3] магістрант О.Б. Бода – НУ "Львівська політехніка"