Особливості впровадження системи захисту інформаційних ресурсів на підприємстві

Грицюк П.Ю.[1], Грицюк Ю.І.[2]

[1]Магістр, здобувач кафедри інформаційних технологій, Національний лісотехнічний університет України,
вул. Ген. Чупринки 103, м. Львів, Україна, pgrytsiuk1992@gmail.com
[2]Проф., д.т.н., професор кафедри програмного забезпечення, Національний університет "Львівська політехніка", вул. С. Бандери, 28-а, м. Львів, Україна, yurii.i.hrytsiuk@lpnu.ua

Анотація **– Розглянуто особливості впровадження системи захисту інформаційних ресурсів (ІР) на підприємстві, яка має забезпечити безперервність ведення бізнес-процесів підприємства, стійкість його функціонування до зовнішніх загроз та запобігання потенційним збиткам підприємства від реалізації інформаційних атак. Виявлено, що для ефективного використання ІР в той чи інший період їх життєвого циклу, протягом якого вони є актуальною для потенційних конкурентів, необхідно вибрати такий режим доступу до них, при якому ефект від їх використання досягав би максимальної величини.**

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

Features of introduction of system of protection of information resources in the enterprise

Grytsyuk P.Yu.[1], Gryciuk Yu.I.[2]

[1] MSC, postgraduate of the Information Technology Department, Ukrainian National Forestry University,
Gen. Chuprynka str., 103, Lviv, Ukraine, pgrytsiuk1992@gmail.com
[2] Prof., Professor of Software Department, Lviv Polytechnic National University,
S. Bandery str., 28a, Lviv, Ukraine, yurii.i.hrytsiuk@lpnu.ua

Abstract **– Considers specific features of introduction of the system of protection of information resources (IR) in the enterprise. This system should ensure the continuity of business processes of the enterprise, stability of its operation of external threats and avoid potential losses of the enterprise from the implementation of information attacks. It is revealed that for the effective use of IR in different periods of their life cycle, during which they are relevant to potential competitors, you must choose the mode in which the effect of the use of these resources reach the maximum value.**

Keywords*: information security (IS), complex system of information security (CSIS), information resources (IR), organizational and mathematical model of enterprise information security.*

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 [9, 14]. Наслідками таких атак можуть стати розголошення конфіденційної або спотворення цілісної інформації, нав'язування керівництву підприємства помилкової інформації, порушення доступу до достовірної інформації, а також відмови і збої роботи програмно-технічних систем [2]. Глобальні дослідження інформаційної безпеки [6] свідчать про те, що кількість дій зловмисників стосовно певних ІР підприємства не тільки постійно зростають, але й мають набагато згубніші наслідки для нього [13]. Розуміючи це, керівники підприємств вимушені запроваджувати різні організаційні та програмно-технічні заходи щодо захисту важливих ІР [5, 8, 10].

Для вирішення поточних завдань захисту ІР підприємства впроваджується комплексна система захисту інформації (КСЗІ) [7]. 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 істотне значення для замовника ІР підприємства. Системи захисту ІР також мають нейтралізувати чи послабити інформаційні атаки конкурентів 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 функціонального профілю КСЗІ для реалізації необхідної множини засобів і механізмів захисту.

Однак, у доступній науковій літературі [1, 5, 8, 11, 13] не повністю з'ясовано основні особливості

визначення допустимих витрат на захист ІР підприємства, не наведено досконалі математичні моделі вибору раціонального варіанту КСЗІ. Тому обґрунтування особливостей впровадження системи захисту ІР на підприємстві є актуальним науково-практичним завданням, що сприяло виконанню цієї роботи та вимагає реалізації подальших досліджень.

Особливості визначення витрат на захист інформаційних ресурсів

Секретність комерційної діяльності підприємства – категорія більше економічна, ніж технічна [1]. 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. Водночас, 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 національної безпеки держави або комерційної діяльності підприємства [2, 8].

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 доступу до неї, при якому ефект від її використання досягав би максимальної величини з урахуванням позитивних і негативних наслідків [7]. Встановлення певних обмежень на доступ до інформації протягом деякого періоду її ЖЦ є одним із способів ефективного управління об'єктами інформаційної безпеки з боку ІТ-персоналу, спрямованого на досягнення максимального ефекту від впровадження КСЗІ на підприємстві [11].

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 [10].

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 витрат на її захист при встановленні обмеженого доступу до інформації; 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. 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 захист ІР застосовується суб'єктивне оцінювання інформації експертами, що добре розуміють її цінність, а також взаємозв'язок з вказаними чинниками [7].

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; потенційно можлива величина збитку $U(t)$ та величина вигод $V(t)$ при вільному використанні інформації в t-ий період її ЖЦ; ймовірність прояву потенційного збитку (p) і прояву упущених вигод (p) 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 виявиться більшим від нуля, то доцільно внести цю інформацію до переліку відомостей з обмеженим доступом. Приналежність інформації до ІР підприємства, що підлягають захисту від несанкціонованих і ненавмисних дій, вважається тоді, коли величина заподіяного збитку внаслідок реалізації загроз перевищує величину витрат на її захист. 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 графічна модель, наведена на рис. 1. В цій моделі показано якісний взаємозв'язок таких параметрів системи захисту ІР підприємства: їх цінність, необхідний рівень захисту, тривалість забезпечення конфіденційності. 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 $0{,}5 \le P < 1$, 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. 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 $U(G,P) = G(T)\cdot(1- P)$.

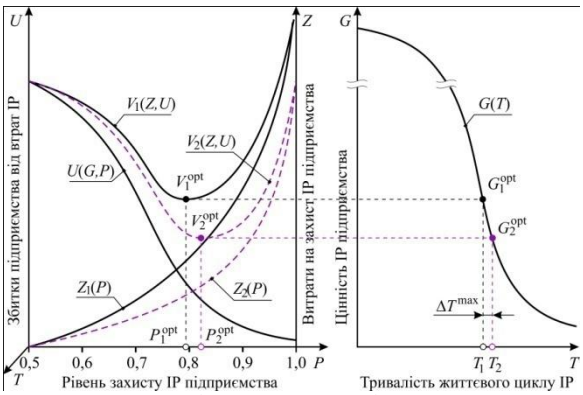

Рис. 1. Модель оцінювання параметрів системи захисту IP підприємства

З рис. 1 видно, що сума $Z_1(P) + U(G,P)$ визначає витрати $V(Z,U)$, пов'язані із забезпеченням конфіденційності інформації. При цьому оптимальний рівень захисту інформації $V^{opt}(Z, U)$ відповідає мінімуму суми витрат на захист $Z_1(P)$ і можливих втрат $U(G,P)$ унаслідок неповноти захисту інформації. Прагнення перевищити його призведе 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.

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.

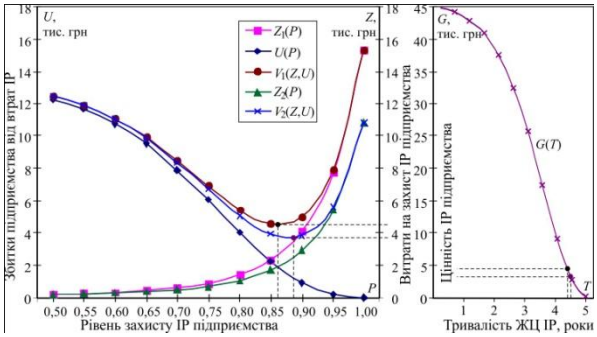

Рис. 2. Результати моделювання параметрів системи захисту IP підприємства

Моделі вибору раціонального варіанту КСЗІ на підприємстві

Відомо [4], 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 IP 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 [12]. 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 IP; $\tilde{D} = \{d_j,\ j = \overline{1,n}\}$ – 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 [4]: знайти такий варіант системи захисту IP 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

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

– максимізація рівня захисту ІР підприємства, що забезпечується вибраним варіантом

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

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 [7]: < 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 [4]. 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 [4]. 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

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

при дотриманні таких обмежень:

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

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

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

при дотриманні таких обмежень:

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

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:

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

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 ($F_1 \succ F_2 \succ \ldots \succ F_{M^{\text{пя}}}$) можливі варіанти проектних рішень побудови системи захисту ІР з використанням процедури лексикографічного оцінювання. Реалізація процедури передбачає декомпозицію початкової багатокритеріальної задачі оптимізації методом послідовних поступок [4] 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

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

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

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

Оцінювання значення величини Sдоп 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 з урахуванням позитивних і негативних наслідків. Встановлення певних обмежень на доступ до інформації протягом деякого періоду її ЖЦ є одним із способів ефективного управління об'єктами інформаційної безпеки з боку ІТ-служби, 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 REFERENCES

[1] Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. – 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. – 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 // 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] Гатчин Ю.А., Жаринов И.О., Коробейников А.Г. Математические модели оценки инфраструктуры системы защиты информации на предприятии // Научно-технический вестник информационных технологий, механики и оптики. – СПб. : Изд-во Университета ИТМО. – 2012. – Т. 12, № 2(78). – С. 92-05.

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

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

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

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

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

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

[11] Мальцев А. Методика оценки состояния инженерно-технической защищенности объектов // Технологии защиты. – 2010. – № 4. – С. 15-21.

[12] Ногин В.Д. Проблема сужения множества Парето: подходы к решению // Искусственный интеллект и принятие решений. – 2008. – № 1. – С. 98-112.

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

[14] Утечка информации – угроза корпоративной безопасности. – Доступный с http://www.staffcop.ru/articles/Information_ leakage.php