

УДК 004.621.3

Л.М. Скачек

ПРАКТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОЇ БЕЗПЕКИ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Нині для об'єкта захисту (підприємства) обов'язковою умовою успіху його діяльності є постановка завдання забезпечення безпеки конфіденційної інформації про об'єкт його захисту.

Ключові слова: об'єкт захисту, конфіденційна інформація (КІ), видова і сигнальна КІ, технічне рішення ОЗ.

На сьогоднішній день для объекта защиты (предприятия) обязательным условием его успешной деятельности является постановка задания обеспечения безопасности конфиденциальной информации об объекте его защиты.

Ключевые слова: объект защиты, конфиденциальная информация (КИ), видовая и сигнальная КИ, техническое решение ОЗ.

Today for an object of the protection (an enterprise) an indispensable condition of its successful activity is the statement of the task of safety of the confidential information on the object of its protection.

Keywords: object of protection, confidential information, specific and alarm confidential information, technical decision.

За сучасних умов на об'єкті захисту (ОЗ) та в його діяльності застосовується комплекс методів та засобів захисту інформації від можливих зловмисних дій конкурентів із метою збереження її цілісності, доступності та конфіденційності. Ця інформація є інтелектуальною власністю об'єкта.

Як засвідчила низка досліджень, необхідно здійснити процедуру обґрунтування технології забезпечення безпеки конфіденційної інформації (КІ) з новизни ОЗ та технічних засобів промислового шпигунства (ТЗПШ).

З кожним роком промисловий шпонаж розвивається паралельно з розвитком технологій і появою нових технічних засобів зняття інформації.

Істотне утруднення можливості отримання інформації з об'єкта захисту (ОЗ) сприяє збереженню науково-технічного пріоритету підприємства у відповідній сфері його діяльності, а також підтримці на заданому рівні, у разі потреби, потенційної якості функціонування ОЗ в розрахункових умовах його застосування [1, 2].

Методичні підходи до організації захисту конфіденційної інформації (КІ) на підприємстві, обґрунтовані технологією безпеки ОЗ та технічних засобів промислового шпигунства (ТЗПШ), розглянуто нижче:

– вибір показників кількісної оцінки чинника значущості видової і сигнальної КІ з ОЗ;

– формування показників часової оцінки інформативності КІ з новизни ОЗ;

– формування й аналіз показника ефективності технології забезпечення безпеки КІ з новизни ОЗ в умовах підприємства.

Значущість КІ для підприємства визначається новизною сукупності реалізованих в ОЗ індивідуальних інженерно-технічних і (або) схемотехнічних рішень (далі – індивідуальні технічні рішення ОЗ), інформація про які може бути представлена у вигляді двох класифікаційних груп:

– видова КІ ІБ, яка містить якісні дані щодо особливостей показників новизни ОЗ;

– сигнальна КІ, що містить змістову виміряну інформацію з енергетичних, потокових або інших параметрів полів випромінювань ОЗ, виражених у загальноприйнятних одиницях фізичних величин [7].

$$\begin{cases} K_B = \sum_{i=1}^S \frac{z_i \varphi_i}{B}, \\ B = \max \sum_{i=1}^S z_i \varphi_i. \end{cases} \quad (1)$$

$$K_C = \frac{\sum_{i=1}^S k_i \varphi_i}{\sum_{i=1}^S \varphi_i} \quad (2)$$

де

i – порядковий номер ознаки або параметра аналізованого технічного рішення ОЗ (далі – характеристика ОЗ) у початковому наборі характеристик;

z_i – експертна кількісна оцінка значущості i -ї характеристики ОЗ, заснована на видовій КІ з ОЗ;

$k_i = x_i / x_0$ – розрахункова оцінка значущості i -ї характеристики ОЗ, заснована на сигнальній КІ з ОЗ;

(x_i, x_0) – відповідно величини визначальних параметрів аналізованого ОЗ і його прототипу вітчизняної або зарубіжної розробки, підбраного за функціонально-однорідними ознаками);

$\varphi_i = i/2^{i-1}$ – функція, яка вимірює вагову значущість часткових оцінок – k_i і z_i ;

S – загальне число часткових оцінок.

Між показниками (1) і (2) існує простий лінійний зв'язок

$$K_C = (1 - \psi) + K_B,$$

де

ψ – коефіцієнт повноти інформації, що міститься в демаскуючих її чинниках.

Використовуючи комплексні показники (1) і (2), запишемо вирішальне правило управління чинника значущості технічного рішення ОЗ:

$$\left. \begin{aligned} d(K_B) &: \{ K_B \Rightarrow K_{B_i} \} \\ d(K_C) &: \{ K_C \Rightarrow K_{C_j} \} \end{aligned} \right\} \quad (3)$$

де

K_{B_i} і K_{C_j} – значення базового або нормативного показника новизни (технічного рівня) конкретного рішення ОЗ для видової і сигнальної КІ відповідно, задані в технічному завданні на створення зразка ОЗ.

Розглядаючи вираз (3), можна зробити такі висновки:

– якщо $K_B > K_{B_i}$ ($K_C > K_{C_j}$), то технічне рішення ОЗ є значущим, а отже, становить практичний інтерес для протиборчої сторони;

– якщо $K_B = K_{B_i}$ ($K_C = K_{C_j}$), то технічне рішення ОЗ відповідає своєму рівню, прийнятому до розгляду прототипу, і не має істотної переваги над конкуруючими групами;

– якщо $K_B < K_{B_i}$ ($K_C < K_{C_j}$), то технічне рішення ОЗ доцільно розглядати як неперспективне, якщо немає яких-небудь спеціальних міркувань.

Передбачається, що кожному індивідуальному технічному рішенню ОЗ, а отже, ОЗ в цілому, властиві специфічні технічні демаскуючі ознаки (ТДО), що розкривають тією чи іншою мірою повноту КІ з новизни ОЗ, а також що КІ з новизни ОЗ зберігає первинну значущість тільки протягом певного прогнозованого інтервалу часу [5].

Для кількісної оцінки інформативності КІ з об'єкта захисту, введемо показники ймовірності, що розкривають КІ з новизни ОЗ.

ТДО, що розкривають КІ з новизни ОЗ, є інформативним, якщо розрахункова ймовірність відповідає можливості їх виявлення ТЗПШ відповідними видами. У загальному випадку, враховуючи незалежність технічних каналів витоку видової і сигнальної КІ з ОЗ, ймовірність виявлення ($P_{обн}$) інформаційних ТДО об'єкта захисту може бути представлена у вигляді

$$P_{обн} = 1 - (1 - B_{ij})(1 - C_{ij}),$$

де

B_{ij} , C_{ij} відповідно значення ймовірності виявлення ТЗПШ інформативних ТДО, що відносяться до видової і сигнальної інформації з ОЗ, при диференційному підході до організації утаєння вказаних ТДО на підприємстві.

У випадку, якщо кожний енергетичний контакт системи “ТЗПШ–ОЗ” на i -му етапі пошуку ОЗ протиборчою стороною здійснюється в незмінних фізичних умовах, а дискретні акти виявлення конкретного інформативного ТДО за допомогою ТЗПШ є незалежними подіями, ймовірність R_{ij} визначається за формулою

$$R_{ij} = \sum_{i=1}^n q_i \prod_{j=1}^m [1 - r_j(1 - R_0)], \quad (4)$$

де

q_i – ймовірність здійснення протиборчою стороною i -го етапу пошуку відповідного інформативного ТДО, ймовірність застосування підприємством j -ї технології утаєння у згаданого вище ТДО;

R_0 – ймовірність виявлення інформативного ТДО за допомогою ТЗПШ;

З огляду на зазначене вище і вважаючи, що межі зміни ймовірності $0 \leq R_{ij} \leq 1$ і $0 \leq R_{обн} < 1$, оберемо як шукані показники I кількісної оцінки інформативності КІ з ОЗ такого виразу:

$$\left. \begin{aligned} I &= \frac{R_{ij}}{1 - R_{ij}} \\ \bar{I} &= \frac{P_{обн}}{1 - P_{обн}} \end{aligned} \right\}, \quad (5)$$

Перший із зазначених показників назвемо частковим, другий – загальним показником інформативності КІ з ОЗ в умовах підприємства. Проведемо оцінку інтервалу часу T_{\max} , протягом якого КІ з новизни ОЗ зберігає свою значущість, тобто задовольняє складену вище умову

$$K_B > K_{B_0} \quad (K_C > K_{C_0}).$$

З цією метою зробимо такі припущення:

– кожний акт несанкціонованого витоку інформативного ТДО (за наявності відповідного технічного каналу його витоку) супроводжується адекватною зміною значущості ОЗ, іншими словами, $K_B \rightarrow 0$ і $K_C \rightarrow 0$;

– технологія захисту КІ з новизни ОЗ ґрунтується лише на методах утаєння інформативних ТДО;

– приріст Δ_k значущості технічного рішення ОЗ, забезпечуваний утаєнням інформативних ТДО, оцінюється величиною

$$\Delta_K = K_{nm_{ck}} - K_{nm_{yT}}, \quad (6)$$

де

$K_{nm_{ck}}, K_{nm_{yT}}$ – значення показника новизни K_B або K_C для m -го аналізованого технічного рішення ОЗ, якому властивий n -й інформативний ТДО, відповідно з прихованого ТДО і несанкціонованого його витоку.

Абстрагуючись від вигляду КІ з ОЗ згідно з розглянутими вище класифікаційними групами, що в цьому випадку непринципово, представимо процес зміни значущості КІ з новизни ОЗ так:

$$\begin{aligned} K_{nm} &= 1, \text{ якщо } t \leq t_{обн}, \\ 0 < K_{nm} < 1, \text{ якщо } t_{обн} < t \leq t_{рас}, \end{aligned}$$

де

t – поточний час, початком відліку якого є момент затвердження технічного завдання на створення ОЗ,

$t_{обн}$, $t_{рас}$ – час, відповідно, виявлення й розпізнавання протиборчою стороною інформативного ТДО (початок відліку збігається з часом t).

Керуючись принципом урівноваження наслідків недосконалості норм захисту КІ ступенем впливу випадкових чинників на достовірність інформації, що здобувається за допомогою ТЗПШ, можна записати:

$$(1 - \delta K_{nm}) K_{nmck} = [1 - P_{рас}(t)] K_{nmck}, \quad (7)$$

δK_{nm} – відносний приріст значущості КІ з новизни ОЗ, забезпечуватиме утаєння інформативного ТДО;

$P_{рас}(t)$ – імовірність розпізнавання до заданого терміну по n -му інформативному ТДО конфіденційної інформації з ОЗ.

Відносний приріст виражається залежністю

$$\delta K_{nm} = \frac{\Delta K}{K_{nmck}} = 1 - \frac{K_{nmym}}{K_{nmck}}. \quad (8)$$

Ймовірність $P_{рас}(t)$ визначається в загальному вигляді формулою

$$P_{рас}(t) = 1 - \exp\left[-\left(\frac{t - t_{обн}}{\tau_{рас}}\right)\right], \quad t \geq t_{обн} \quad (9)$$

де

$\tau_{рас} = (t_{рас} - t_{обн})$ – інтервал часу, протягом якого протиборча сторона в змозі ідентифікувати отриману нею КІ з ОЗ.

В результаті рішення рівності (4) щодо шуканої величини з урахуванням залежності (2) одержуємо наступний вид часового показника інформативності КІ з ОЗ

$$T_{max} = t_{обн} + \tau_{рас} \left[-1n(1 - \delta K_{nm}) \right].$$

Для ефективного забезпечення техніко-економічної ефективності технології (ТЕЕ) безпеки підприємства вводимо показник

E_{nm} – КІ з m -м технічним рішенням ОЗ, який розкриває в n -му інформативному ТДО, становить, відповідно до загальнотехнічних представлень, залежність

$$E_{nm} = \frac{\Delta K}{C_{r,mck}}, \quad (10)$$

де

Δ_K – приріст значущості технічного рішення ОЗ, забезпечуваний утаєнням зазначеного вище ТДО;

C_{nm}^{ck} – асигнування (ресурси) на технологію його здійснення.

Приведемо залежність (10) до вигляду, що враховує вирішальне правило запобігання потенційним збиткам на підприємстві за відповідного показника інформативності КІ з ОЗ.

Відповідно до принципу еквівалентності кількісної оцінки інформативності КІ з ОЗ, що виражаються, з одного боку, через енергетичні можливості ТЗПШ, а з іншого – через повноту відповідності реальних умов утаєння КІ з ОЗ на робочих місцях підприємства розрахунковим умовам, що виключають несанкціонований витік інформативних ТДО, на підставі (9) і (10) маємо

$$I_{nm} = 1 - \delta K_{nm}. \quad (11)$$

Передбачається, що $\delta K_{nm} \geq 0$, в іншому випадку вплив обізнаності протидіючої сторони про КІ з ОЗ на зниження її первинної значущості відсутній.

З урахуванням (9) і (10) залежність (11) приймає вигляд

$$E_{nm} = (1 - I_{nm}) \frac{K_{nm}^{ck}}{C_{nm}^{ck}}. \quad (12)$$

Аналіз виразу (12) свідчить про те, що основним резервом підвищення ТЕЕ технології забезпечення безпеки КІ з новизни ОЗ за заданих асигнувань (ресурсів) на здійснення утаєння КІ є зниження величини показника I_{nm} інформативності КІ з ОЗ, що досягається за рахунок оптимізації системи захисту КІ, наприклад, згідно з рекомендаціями [3, 4].

У загальному випадку показник ТЕЕ технології забезпечення безпеки КІ з новизни ОЗ

$$\bar{E}_{O3} = \sum_{m=1}^M \sum_{n=1}^N \xi_{nm} (1 - I_{nm}) \frac{K_{nm}^{ck}}{C_{nm}^{ck}}, \quad (13)$$

де

ξ_{nm} – вагова функція внеску в загальну ефективність утаєння КІ з новизни ОЗ m -го технічного рішення ОЗ ($m \in 1, M$), якому властивий n -й інформаційний ТДО ($n \in 1, N$) [5].

Отже, в ході здійсненого дослідження було визначено, що постановка завдання забезпечення безпеки КІ з новизни ОЗ є повністю сформульованою, якщо задано (визначено) такі початкові дані:

– мета захисту КІ від сукупності загроз її безпеки у сферах обігу на підприємствах;

– перелік, що охороняються від ТЗПШ, характеристик ОЗ, з оцінкою повноти віддзеркалення їх інформативними ТДО, які належать до видової й сигнальної КІ;

– вимоги до ефективності захисту КІ з новизни ОЗ, як сектора інформаційного ресурсу підприємства.

Процедура обґрунтування технології забезпечення безпеки КІ з новизни ОЗ передбачає:

– кількісну оцінку значущості технічного рішення ОЗ на базовому (нормативному) показнику технічного рівня ОЗ;

– кількісну оцінку інформативності КІ з ОЗ стосовно умов утаєння інформаційних ТДО від протиборчої сторони;

– кількісну оцінку ТЕЕ заходів щодо організації і здійснення утаєння КІ ОЗ при виділених асигнуваннях (ресурсах) на здійснення захисту значущих технічних рішень ОЗ;

– порівняльний аналіз розглянутих варіантів ТЕЕ технології захисту КІ з ОЗ і прогнозу оцінку інтервалу часу, протягом якого гарантується безпека КІ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Скачек Л.Н. Информационная безопасность предприятия / Л.Н. Скачек // Сучасний захист інформації. – 2011. – № 2. – С. 68–78.

2. Скачек Л.Н. Построение моделей функционально-экономического анализа информационных систем / Л.Н. Скачек, В.О. Хорошко // Сучасні інформаційно-комунікаційні технології : Матеріали IV міжнародної науково-технічної конференції COMINFO 2008, 5–9 жовтня 2008 р. – Ялта, 2008. – С. 197–200.

3. Кривицкая Н.Я. Математическое моделирование социально-экономических процессов в Украине. Часть 1 / Н.Я. Кривицкая, Л.Н. Скачек, А.В. Титов, В.А. Хорошко // Вісник ДУІКТ. – 2010. – № 4. – С. 363–375.

4. Кривицкая Н.Я. Математическое моделирование социально-экономических процессов в Украине. Часть 2 / Н.Я. Кривицкая, Л.Н. Скачек, А.В. Титов, В.А. Хорошко // Вісник ДУІКТ. – 2011. – Т. 9 (2). – С. 170–180.

5. Хорошко В.А. Экспертная система для оценки эффективности применения средств защиты информации / В.А. Хорошко, В.А. Швец // Вісник ДУІКТ. – 2000. – № 4. – С. 7–10.

6. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А.Чекатков. – К. : Юниор, 2003. – 504 с.

7. Хорошко В.А. Модель системы защиты информации / В.А. Хорошко // Захист інформації. – 1999. – № 1. – С. 5–11.

Отримано 9.12.2011