УДК 004.623.624

Невойт Я.В., д.т.н., проф. Хорошко В.О.,
Чередниченко В.С. (ДУІКТ)

ПРАКТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Введення

Конфіденційна інформація (КІ) об'єкту захисту, може відноситися до категорій військової, економічної, промислової, інтелектуальної і до інших таємниць. Безпека вказаної інформації об'єкту зумовлюється повнотою і правильністю вибору технології захисту КІ, направленої на запобігання несанкціонованого витоку інформації.

Мається на увазі, що виключення або істотне утруднення можливості отримання КІ визначається системою захисту об'єкту (СЗО) і її потенційної якості функціонування в мовних умовах її застосування.

Тому для вирішення цього завдання необхідно розглянути наступні аспекти:

- вибір показників кількісної оцінки чинника значущості видової і сигнальної КІ про об'єкт захисту (ОЗ);
- формування імовірнісного і тимчасового показників інформативності КІ про ОЗ;
- формування і аналіз показника техніко-економічної ефективності технології забезпечення безпеки КІ щодо ОЗ в існуючих умовах.

Мета роботи

Розробка спільного підходу і принципів забезпечення мотиваційної і обґрунтованої технологій забезпечення безпеки КІ щодо ОЗ від технічних засобів несанкціонованого отримання інформації (ТЗНОІ) на користь запобігання збитку ОЗ.

Основна частина

Значущість КІ для ОЗ може бути різною: інженерно-технічних і (або) схемотехнічних рішеннях, індивідуальних технічних рішень і так далі, інформація про які може бути представлена у вигляді двох класифікаційних груп:

- видова КІ, що містить якісні дані про особливості ОЗ;
- сигнальна КІ, що містить вимірювальну інформацію про енергетичні, потокові або інші параметри полів випромінювань ОЗ, виражених в загальноприйнятих одиницях фізичних величин.

Кількісна оцінка значущості видової і сигнальної КІ щодо ОЗ може бути проведена за допомогою безрозмірних величин K_B і K_C відповідно, що є по суті комплексними показниками ОЗ:

$$\begin{cases} K_B = \sum\limits_{i=1}^{S} \dfrac{z_i \varphi_i}{B}, \\ K_C = \max \sum\limits_{i=1}^{S} z_i \varphi_i, \end{cases} \tag{1}$$

$$K_C = \frac{\sum\limits_{i=1}^{S} k_i \varphi_i}{\sum\limits_{i=1}^{S} \varphi_i}, \tag{2}$$

де i – порядковий номер ознаки або параметра технічного рішення, що аналізується ОЗ в початковому наборі характеристик;

z_i – дискретна кількісна оцінка значущості i -ої характеристики ОЗ, заснована на видовій КІ щодо ОЗ;

$k_i = x_i / x_0$ – розрахункова оцінка значущості i -ої характеристики ОЗ, заснована на сигнальній КІ щодо ОЗ (x_i і x_0 – відповідно величини визначальних параметрів того, що аналізує ОЗ);

$\varphi_i = i / 2^{i-1}$ – функція, що нормує вагову значущість приватних оцінок z_i і k_i;

S – загальне число окремих оцінок.

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

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

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

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

$$\left.\begin{array}{l} d\left(K_B\right): \left\{K_B \Rightarrow K_{Вб}\right. \\ d\left(K_C\right): \left\{K_C \Rightarrow K_{Сб}\right. \end{array}\right\}, \qquad (3)$$

де $K_{Вб}$ і $K_{Сб}$ – значення базового або нормативного показника технічного рівня конкретного рішення ОЗ для видової і сигнальної КІ відповідно.

Розглядаючи вираз (3) можна зробити наступні висновки:

- якщо $K_B \succ K_{Вб}\left(K_C \succ K_{Сб}\right)$, то технічно рішення ОЗ є значним, а, отже представляє практичний інтерес і перевищує існуючий рівень техніки;

- якщо $K_B = K_{Вб}\left(K_C = K_{Сб}\right)$, то технічне рішення ОЗ відповідає заданому рівню техніки;

- якщо $K_B \prec K_{Вб}\left(K_C \prec K_{Сб}\right)$, то технічне рішення ОЗ доцільно розглядати як неперспективне, якщо не висувається якихось спеціальних вимог.

Можна припустити, що кожному індивідуальному технічному рішенню ОЗ, а отже ОЗ в цілому, властиві специфічні технічні демаскуючі ознаки (ТДО), що розглядають з того або іншого ступеня повноти КІ щодо ОЗ, а також, що КІ щодо ОЗ зберігає первинну значущість протягом певного інтервалу часу [2].

Нехай істине значення сигнальної КІ щодо ОЗ оцінюється величиною U_0, а оцінкою ТДО в розмірності U_0 є величина $U_{ТДП}$. У випадку, якщо розподіл відхилень $U_{ТДП}$ про U_0 при n-кратних вимірах величини $U_{ТДП}$ підпорядковано закону Лапласа-Гауса, то можна записати:

$$\Delta_{ІНФ} = t(H)\frac{\delta_{ТДП}}{\sqrt{n}} , \qquad (4)$$

де $\Delta_{ІНФ} = |U_0 - U_{ТДЛ}|$ – абсолютна інформаційна погрішність, що характеризує повноту віддзеркалення ТДО СЗО розкриваною ним КІ;

$t\left(H\right)$ – табульована функція, що визначається по заданій довірчій вірогідності H з умови $2\Phi\left(t\right) = H$ (тут $\Phi\left(t\right)$ – інтеграл вірогідності);

$\delta_{ТДП}$ - середнє квадратичне відхилення результатів вимірів.

З іншого боку, якщо вважати, що інформаційна погрішність пов'язана з повнотою КІ, що розкривається інформативним ТДО, лінійним чином, то вказана погрішність, зрештою, буде пропорційна величині $U_{ТДП}$:

$$\delta_{ІНФ} = \delta_{ІНФ} U_{ТДЛ} \tag{5}$$

Коефіцієнт пропорційності $\delta_{ІНФ}$ має цілком певний фізичний зміст, що характеризує неповноту КІ, що розкривається інформативним ТДО:

$$\delta_{ІНФ} = 1 - T_{ТДЛ}\,, \tag{6}$$

де $T_{ТДП}$ – коефіцієнт, який відображає повноту інформації, що міститься в інформативному ТДО (чим ближче до одиниці величина $T_{ТДП}$, тим вище повнота віддзеркалення СЗО ТДО величини U_0).

Прирівнюючи ліві частини залежностей (1) і (2), після нескладних перетворень із залученням залежності (3) маємо

$$\delta_{ТДП} = \left(1 - T_{ТДП}\right) U_{ТДП} \frac{\sqrt{n}}{t(H)} \tag{7}$$

Вираз (7) дозволяє, задавшись значеннями величин H і n отримати шкалу прогнозної значущості інформативного ТДО аналізованого ОЗ.

Тепер проведемо визначення показників кількісної оцінки інформативності конфіденційної інформації про ОЗ.

Імовірнісні показники. Припустимо, що ТДО, що розкривають КІ щодо ОЗ, є інформативними, якщо розрахункова вірогідність виявлення їх відповідними видами ТЗНОІ перевищує нормоване в установленому порядку значення вказаної вірогідності.

У загальному випадку, враховуючи незалежність технічних каналів витоку видової і сигнальної КІ щодо ОЗ, вірогідність виявлення ($P_{обн}$) інформаційних ТДО об'єкту захисту може бути представлена у вигляді

$$P_{обн} = 1(1 - R_{Bij})(1 - R_{Cij})\,,$$

де R_{Bij} і R_{Cij} – відповідно значення вірогідності виявлення ТЗНОІ інформативних ТДО, що відноситься до видової і сигнальної інформації про ОЗ при диференціальному підході до організації приховування вказаних ТДО на об'єкті.

У випадку, якщо кожен енергетичний контакт системи «ТЗНОІ-03» на *i*-ому етапі пошуку СЗО і каналів витоку з об'єкту зловмисниками здійснюється в незмінних фізичних умовах, а дискретні акти виявлення конкретного інформативного ТДО за допомогою ТЗНОІ є незалежними подіями, вірогідністю R_{ij} визначається за формулою [3]

$$R_{ij} = \sum_{i=1}^{n} q_i \prod_{j=1}^{M} \left[1 - r_j \left(1 - R_0\right)\right],$$

де q_i – вірогідність здійснення зловмисником *i*-го етапу пошуку відповідного інформативного ТДО;

r_j – вірогідність застосування на об'єкті j-ї технології приховування ТДО СЗО;

R_0 – вірогідність виявлення інформативного ТДО за допомогою ТЗНОІ в ідеальних умовах.

Беручи до уваги викладене і вважаючи, що межі виміру вірогідності $0 \le R_{ij} \prec 1$ і $0 \le P_{обн} \prec 1$ виберемо як шукані показники I кількісної оцінки інформативності КІ щодо ОЗ наступні вирази

$$\left.\begin{aligned} I &= \frac{R_{ij}}{1-R_{ij}}, \\ \bar{I} &= \frac{P_{обн}}{1-P_{обн}}. \end{aligned}\right\} \tag{8}$$

Перший із вказаних показників називається приватним, другий – узагальненим показником інформативності КІ щодо ОЗ в умовах об'єкту.

Часовий показник. Проведемо оцінку інтервалу часу $T_{\max}$, у перебігу якого КІ щодо ОЗ зберігає свою значущість, тобто задовольняє сформульовані умови: $K_B \succ K_{Bб}\left(K_C \succ K_{Cб}\right)$. З цією метою приймемо наступні припущення:

- кожен акт несанкціонованого витоку інформативного ТДО (за наявності відповідного технічного каналу його витоку) супроводжується адекватною зміною значущості ОЗ, інакше кажучи $K_B \to 0$ і $K_C \to 0$;

- технологія захисту КІ щодо ОЗ базується тільки на методах приховування інформативних ТДО;

- приріст Δ_k значущості ОЗ, забезпечуваний приховуванням інформативних ТДО, оцінюється величиною

$$\Delta_k = K_{nm_{CK}} - K_{nm_{УТ}} \ , \tag{9}$$

де $K_{nm_{CK}}$ і $K_{nm_{УТ}}$ – значення показників або для m–го аналізованого технічного рішення ОЗ, якому властива n–а інформативна ТДО, відповідно при приховуванні ТДО і несанкціонованому витоку його.

Абстрагуючись від виду КІ щодо ОЗ, згідно запропонованим і розглянутим вище класифікаційним групам, що в даному випадку непринципово, представимо процес зміни значущості К про цінність ОЗ так:

$$K_{nm} = 1 \text{ , якщо } t \le t_{обн};$$

$$0 \prec K_{nm} \prec 1 \text{ , якщо } t_{обн} \prec t \prec t_{рас}\_$$

де t – поточний час, початком відліку якого є момент початку робіт на ОЗ;

$t_{обн}, t_{рас}$ – відповідно час виявлення і розпізнавання зловмисником 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 ТЗНОІ, можна записати:

$$\left(1-\delta K_{nm}\right) K_{nm_{CK}} = \left[1-P_{рас}\left(t\right)\right] K_{nm_{CK}} \ , \tag{10}$$

де δK_{nm} – відносний приріст значущості КІ щодо ОЗ, забезпечуване приховуванням інформативного ТДО;

$P_{рас}\left(t\right)$ – вірогідність розпізнавання до заданого рядка по n-му інформативному ТДО КІ щодо ОЗ.

Відносний приріст δK_{nm} можна виразити залежністю

$$\delta K_{nm} = \frac{\Delta_k}{K_{nm_{CK}}} = 1 - \frac{K_{nm_{УТ}}}{K_{nm_{CK}}}. \tag{11}$$

Вірогідність $P_{роз}(t)$ визначається в загальному вигляді за формулою

$$P_{роз}(t) = 1 - \exp\left[-\left(\frac{t - t_{одн}}{\tau_{роз}}\right)\right], t \succ t_{одн}, \quad (12)$$

де $\tau_{роз} = (t_{роз} - t_{одн})$ – інтервал часу, протягом якого зловмисники в змозі ідентифікувати отриману ними КІ щодо ОЗ.

У результаті вирішення рівності (10) щодо шуканої величини з урахуванням залежності (8) отримуємо наступний вид тимчасового показника інформативності КІ щодо ОЗ

$$T_{\max} = t_{обн} + \tau_{роз}\left[-\ln(1 - \delta - K_{пт})\right].$$

Після проведених досліджень можна оцінити показник техніко-економічної ефективності технології забезпечення безпеки КІ щодо ОЗ.

Оскільки, показник $Э_{пт}$ техніко-економічної ефективності (ТЕЕ) технології забезпечення безпеки КІ про m–ий ОЗ, що розкривається по n-му інформативному ТДО, є, відповідно до загальнотехнічних уявлень, залежність

$$Э_{пт} = \frac{\Delta_k}{C_{пт_{СК}}}, \quad (13)$$

де Δ_k – приріст значущості ОЗ, що забезпечується приховуванням вказаного вище ТДО;

$C_{пт_{СК}}$ – матеріальні ресурси, виділені на технологію його здійснення.

Відповідно до принципу еквівалентності кількісної оцінки інформативності КІ щодо ОЗ, що виражається, з одного боку через енергетичні можливості ТЗНОІ, а з іншого – через повноту відповідності реальних умов приховування КІ щодо ОЗ на об'єкті розрахунковим умовам, що виключають несанкціонований виток інформації ТДО, на підставі (8) і (11) маємо

$$I_{пт} = 1 - \delta K_{пт} \quad (14)$$

Припустимо, що $\delta K_{пт} \geq 0$, в іншому випадку вплив обізнаності зловмисників про КІ щодо ОЗ на зниження її первинної значущості відсутній. З урахуванням (11) і (14), залежність (13) набуде вигляду

$$Э_{пт} = (1 - I_{пт})\frac{K_{пт_{УТ}}}{C_{пт_{СК}}} \quad (15)$$

Аналіз виразу (15) показує: основним резервом підвищення ТЕЕ технології забезпечення безпеки КІ щодо ОЗ при заданих матеріальних ресурсах на здійснення приховування КІ є зниження величини показника $I_{пт}$ інформативності КІ відповідно ОЗ, СЗО, що досягається за рахунок оптимізації.

У загальному випадку показник ТЕЕ технології забезпечення безпеки КІ щодо ОЗ

$$Э_{оз} = \sum_{m=1}^{M}\sum_{n=1}^{N}\xi_{пт}(1 - I_{пт})\frac{K_{пт_{УТ}}}{C_{пт_{СК}}}$$

де $\xi_{пт}$ – вагова функція вкладу в спільну ефективність приховування КІ щодо ОЗ m-ої значущості ОЗ ($m \in \overline{1, M}$), якій властивий n-й інформаційний ТДО ($n \in \overline{1, N}$).

Висновки

1. Забезпечення безпеки КІ щодо ОЗ у контексті запропонованого підходу до вирішення задачі є однією з основних умов захисту інформації.

2. Постановка задачі забезпечення безпеки КІ щодо ОЗ повністю сформульована, якщо задані (визначені) наступні початкові дані:

- мета захисту КІ від сукупності загроз її безпеці в сферах звернення на об'єктах;

- перелік охороняючих від ТЗНОІ характеристик ОЗ з оцінкою повноти віддзеркалення їх інформативними ТДО, що відносяться до видової і сигнальної КІ;

- вимоги по ефективності захисту КІ щодо ОЗ в умовах сектора інформаційного ресурсу, що є на об'єкті.

3. Процедура обґрунтування технології забезпечення безпеки КІ щодо ОЗ передбачає:

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

- кількісну оцінку інформативності КІ щодо ОЗ, що застосовується в умовах приховування інформативних ТДО від зловмисників;

- кількісну оцінку ТЕЕ заходів щодо організації і здійснення приховування КІ щодо ОЗ при виділених матеріальних ресурсах на здійснення захисту об'єкту;

- порівняльний аналіз розглянутих варіантів ТЕЕ технології захисту КІ щодо ОЗ прогнозну оцінки інтервалу часу, протягом якого гарантується безпека КІ.

Список літератури

1. Егоров Ф.И. – Задачи защиты информации / Егоров Ф.И., Тискина Е.О., Хорошко В.А. // Захист інформації, №1, 2009. – с.5-12.

2. Тискина Е.О. – Принципи построения систем управления безопасностью информации / Тискина Е.О., Хорошко В.А. // Вісник ДУІКТ, том 7, №3, 2009. – с.284-293.

3. Барткив Н.И. – Количественная оценка эффективности информационного обеспечения управления системой защиты информации / Барткив Н.И., Тискина Е.О., Хорошко В.А. // Захист інформації, №4, 2009. – с.25-29.

4. Кобозева А.А. – Анализ информационной безопасности / Кобозева А.А., Хорошко В.А. – К.: Изд. ГУИКТ, 2009. – 251с.

Представлені загальний підхід і принципи забезпечення захисту інформації від сукупності загроз її безпеки в умовах застосування зловмисником технічних засобів несанкціонованого отримання інформації.

Ключові слова: конфіденційна інформація, система захисту об’єкту, технічні засоби несанкціонованого отримання інформації, технічні демаскуючі ознаки.

Представлены общий подход и принципы обеспечения защиты информации от совокупности угроз ее безопасности в условиях применения злоумышленником технических средств несанкционированного получения информации.

Ключевые слова: конфиденциальная информация, система защиты объекта, технические средства несанкционированного получения информации, технические демаскирующие признаки.

General approach and principles of providing of priv is presented from the aggregate of threats its safety in the conditions of application of hardwares of unauthorized receipt of information a malefactor.

Key words: confidencial information, system for protection of an object, technical means for unauthorized receipt of information, technical disclosuring features.

Надійшла 20.01.2010

УДК 004.683

Печень С.А. (ГУИКТ)

СОВРЕМЕННЫЕ АНТИКРИЗИСНЫЕ МЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: БЛОКИРОВКА УТЕЧЕК ИНФОРМАЦИИ, КРИТИЧНЫХ ДЛЯ БИЗНЕС-ПРОЦЕССОВ ПРЕДПРИЯТИЯ

Как показывают современные исследования, чтобы сохранить работу, служащие готовы буквально на все, но если их все-таки уволят, ничто не остановит их от кражи ценной информации, принадлежащей работодателю, причем некоторые сотрудники уже имеют копию такой информации.

Например, в ходе последнего исследования American Management Association и ePolicy Institute 14% из 586 опрошенных сотрудников крупных американских компаний признались