УДК 004.056.52

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 3, pp. 240-248

КРИТЕРІЇ ОЦІНКИ ЙМОВІРНОСТІ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ТЕХНІЧНІ КАНАЛИ

М.Г. Романюков

Головне управління міністерства внутрішніх справ України в Одеській області,
вул. Єврейська, 12, Одеса, 65014, Україна; e-mail: kolyanr21@gmail.com

Проведена класифікація сучасних технічних каналів витоку інформації та аналіз їх особливостей з врахуванням сучасних можливих ризиків. Запропонований спосіб кількісного визначення інтегрального показника, що характеризує ступінь безпеки інформації на об'єкті та визначає ймовірність витоку інформації, враховуючи всі фактори, що здійснюють значний вплив на його формування. На основі даного показника проводиться оцінка стану системи захисту інформації. Приведений строго-теоретичний та теоретико-емпіричний підхід для визначення рівня очікуваних втрат при порушенні захисту інформації, що дозволяє, при наявності можливостей, зібрати достатню кількість фактичних даних щодо проявлених загроз та їх наслідків, застосовувати розглянуті в статті моделі для вирішення широкого кола задач по захисту інформації. Обчислюється емпірична величина рівнів затрат, при якій забезпечується мінімізація повної очікуваної вартості захисту інформації.

Ключові слова: технічні канали витоку інформації, модель процесу захисту, ймовірність забезпечення безпеки.

Вступ

Забезпечення інформаційної безпеки є важливим завданням для будь-якої системи захисту, оскільки від збереження конфіденційності, цілісності та доступності інформаційних ресурсів залежать якість і оперативність прийняття технічних рішень, ефективність їх реалізації.

В умовах різних форм власності завдання забезпечення інформаційної безпеки повністю лягає на плечі підприємців, керівників організацій, різних комерційних структур. За підрахунками американських фахівців, втрата 20% інформації веде до розорення організації протягом місяця в 60 випадках зі 100. Інформація є основою для прийняття рішень людиною і від її достовірності, повноти та системної організованості залежить ризик прийняття неефективних і небезпечних рішень [1, 2].

Мета статті

На основі класифікації технічних каналів витоку інформації, запропонувати кількісне визначення інтегрального показника, що характеризує ступінь безпеки інформації на об'єкті та визначає ймовірність витоку інформації, враховуючи всі фактори, що здійснюють значний вплив на його формування. На основі даного показника провести оцінку стану системи захисту інформації. Визначити оптимальний варіант витрат, при яких забезпечується мінімізація повної очікуваної вартості захисту інформації.

Основна частина

Основною класифікаційною ознакою технічних каналів витоку інформації є фізична природа носія інформації. Носії інформації поділяються на польові (фізичні поля), речовинно-польові (потоки частинок), речовинні (матеріали, речовини, структурні елементи та інші макрооб'єкти). На рис. 1 представлена ієрархічна схема фізичних полів, що відносяться до електромагнітної взаємодії.

З використанням фотоелектричних перетворювачів здійснюється перетворення фізичних полів, які випромінюють джерело інформативного сигналу, в інші фізичні поля. Це пов'язано як із взаємодією інформаційних сигналів з об'єктами навколишнього середовища, так із застосуванням технічних засобів. У зв'язку з цим інформативний сигнал може розповсюджуватись одночасно в різних середовищах, може прийматися приймачами, основаними на різноманітних фізичних принципах.

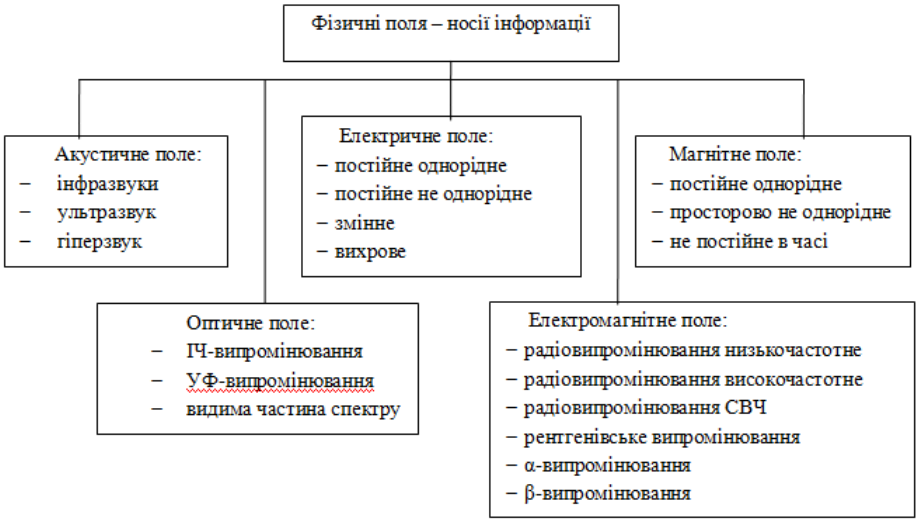

Рис. 1. Схема різновидів фізичних полів – носіїв інформації

В табл. 1 приведений взаємозв'язок між носіями інформаційного сигналу та фізичними середовищами [3].

Таблиця 1.

Взаємозв'язок між носіями інформаційного сигналу та фізичними середовищами

Фізичне середовище / Носії інформації	Газоподібна	Рідка	Тверда
Польові			
Акустичне поле	+	+	+
Електричне поле		+	+
Магнітне поле		+	+
Оптичне поле	+	+	+
Електромагнітне поле	+		
Речовинно-польові			
Електрони	+		
Іони	+	+	
α-, β-, γ-випромінювання	+	+	+
Речовинні			
Гази	+	+	+
Рідини	+	+	+
Тверді тіла	+	+	
Структурні елементи	+	+	

Сучасні підходи до аналізу захищеності інформації і побудови систем захисту інформації (СЗІ) базуються на методах аналізу та управління ризиками. Ризик – прогнозована векторна величина збитку, що може виникнути внаслідок ухвалення рішень в умовах невизначеності та реалізації загроз. Він є кількісною мірою безпеки, що дорівнює добутку ймовірності реалізації даної загрози, помноженій на ймовірність величини можливого збитку від неї. Традиційно неповна інформація щодо загроз, втрат (збитків), їх ймовірностей, інтенсивності та рівнів обумовлює доцільність використання моделі "невизначеність – ризик", в основі походження якої – гіпотеза існування вихідної природної невизначеності в результатах виконання певних дій (операцій). Якщо на цю вихідну невизначеність накладається ситуативна багатоваріантність можливих наслідків (рішень) з кількісною оцінкою ймовірності кожного з них, отримуємо типову ситуацію ризику.

За прикладом звернемося до сфери технічних вимірювань. Припустимо, що контролюються значення певної фізичної величини – напруги *U*, яка в процесі вимірювання має певне незмінне в часі значення *u*, невідоме досліднику. Для вимірювання застосовується цифровий вольтметр, покази якого містять випадкову похибку. Результат вимірювань – вибірка даних з *W* послідовно отриманих відліків виміру приладу $\{u_t\}, t = 1,2...,W$. Аналіз цієї вибірки приводить до ранжованого ряду варіантів $u_1 \le u_2 \le ... \le u_n$ з відповідними відносними частотами варіантів $W_{ri}, i = \overline{1,n}, де\, W_{ri} = \frac{W_i}{W}$, де W_i – частість варіанту $u_{(i)}$ у вибірці $\{u_{(i)}\}$, а $W = \sum_{i=1}^{n} W_i$.

Вважаючи відносні частоти оцінками ймовірностей $p_{(i)}$ варіантів, отримуємо ймовірнісний розподіл $\{u_{(i)}, p_{(i)}\}, i = \overline{1,n}$. Маємо типову ризикову ситуацію: у якості невідомого значення u можемо взяти будь-який з варіантів, комбінацію цих варіантів.

Природно припустити, що невідоме значення напруги u лежить в межах замкненого проміжку $[u_1, u_n]$. Зокрема, якщо у якості невідомого значення u приймемо u_1, ми з ймовірністю p_1 ризикуємо припуститися помилки: $e_1 = u_1 - u.$

Відповідно при виборі варіанту u_2 з ймовірністю p_2 можлива помилка: $e_2 = u_2 - u,$ а в загальному випадку для варіанта u_i матимемо з ймовірністю p_i помилку: $e_i = u_i - u, i = \overline{1,n}.$

Невірний вибір варіанту результату вимірювань спричиняє до певних втрат, збитків, причому, чим більше помилка e, тим суттєвіші втрати. Обсяг цих втрат (збитків) обчислюється за так званою функцією втрат, яка для даної задачі є фактично функцією помилки обраного варіанту результату вимірювань: $L(e_i), i = \overline{1,n}$. За своєю структурою частіше за все $L(e_i)$ – квадратична функція аргументу: $L(e_i) = (e_i)^2 = (u_i - u)^2 = L(u_i - u).$

Використовуючи саме цей вид функції втрат, проаналізуємо ризики нашої задачі. Вибір довільного варіанту результату вимірювань u_i супроводжується виникненням ймовірних втрат, величина яких визначається відповідним ризиком: $r_i = p_i(u_i - u)^2.$

Інтегровану оцінку можливих втрат за всіма варіантами вибору дає середній ризик:

$$R = \sum r_i \sum_{i=1}^{n} p_i (u_i - u)^2, \qquad (1)$$

тобто середній ризик – це середні втрати у ситуації ризику (за всіма можливими варіантами і відповідними їм втратами). Кількісні значення p_i, u_i, $i=\overline{1,n}$, у (1) відомі, тому фактично ризик R є функцією одного аргументу – u, кількісна оцінка значення якого є метою оптимальної обробки отриманої вибірки $\{u_i\}$. Очевидно, що найкращою буде та оцінка u, яка мінімізує середні втрати $R(u)$. Застосувавши стандартну процедуру пошуку екстремуму, отримаємо:

$$\frac{d}{du}R(u)=\frac{d}{du}\left\{\sum_{i=1}^{n}p_i(u_i-u)^2\right\}=2\sum_{i=1}^{n}p_i(u_i-u)=0,$$

звідки

$$u_{opt}=\sum_{i=1}^{n}p_iu_i=\frac{1}{W}\sum_{t=1}^{w}u_t=\bar{u},$$

тобто оптимальною оцінкою буде звичайне середнє $\bar{u}$ [1].

Модель процесу захисту в загальному вигляді задається наступними множинами: K – множина показників безпеки інформації; $P^{(C)}$ – множина параметрів зовнішнього середовища; $P^{(3)}$ – множина параметрів впливу зловмисників; $P^{(O)}$ – множина параметрів системи обробки та системи захисту інформації, що підлягає оцінці; $P^{(У)}$ – множина параметрів системи обробки та системи захисту інформації, якими можна управляти; $P^{(0)}$ – множина загальних ресурсів управління; $S^{(У)}$ – множина засобів та ресурсів управління. Тоді для вирішення задачі аналізу, тобто для визначення показників безпеки інформації, можна представити наступний вираз:

$$K=f\left(P^{(C)},P^{(3)},P^{(O)},P^{(У)},P^{(O)},S^{(У)}\right),$$

де f вказує на існуючу залежність між множиною різнорідних параметрів і множиною показників безпеки інформації.

Аналіз даної моделі показує складність моделювання процесу захисту інформації. Одним з найбільш складних з точки зору формалізації є процес моделювання впливу зловмисника у зв'язку із низьким ступенем передбачуваності його характеристик. Для реалізації процесу частіше всього використовують метод вибору найгіршого варіанту.

Загальний підхід до побудови інтегрального показника безпеки інформації на об'єкті Q можна представити у вигляді послідовності наступних кроків:

1. Формується вектор $X=(x_1,....,x_n)$ вихідних характеристик об'єкту, де циркулює інформація з обмеженим доступом, кожна з яких необхідна, а всі вони разом достатні для повного і всебічного контролю та оцінювання ступеня захищеності даної конфіденційної інформації.

2. Формується вектор $Q=(q_1,....,q_m)$ окремих комплексних показників захищеності, що представляють собою функції $q_i(x), i=1,...,m$ вектора вихідних характеристик $x=x_1,...,x_n$ і оцінюючих різних складових захищеності досліджуваного об'єкту із використанням m різних критеріїв.

3. Формується вектор $H=(h_1,...,h_k)$ параметрів захищеності, що характеризує кожний окремий показник $q_i(x)$.

4. Обчислюється значення вектора $W = (w_1,...,w_m)$, де $w_1,...,w_m$ - вагові коефіцієнти, що визначають значимість окремих показників $q_1,...,q_m$ для інтегральної оцінки Q та задають степінь впливу окремих показників $q_1,...,q_m$ на цю оцінку.

5. Вибирається вид синтезуючих функцій $Q(q)$, співставних вектору окремих показників $Q = (q_1,...,q_m)$, інтегральна оцінка Q (значення Q інтегрального показника $Q(q)$, що характеризує ступінь захищеності інформації досліджуваного об'єкта в цілому):

$$Q = Q(q) = Q(q;w), \quad W = (w_1,...,w_m).$$

Оскільки оптимальне вирішення питання про доцільний рівень затрат на захист полягає в тому, що він повинен бути прирівняний до рівня очікуваних втрат при порушенні захищеності, достатньо визначити тільки розмір втрат. Так спеціалістами фірми IBM запропонована наступна емпірична залежність очікуваних втрат від i-ої загрози для інформації:

$$R_i = 10^{(S_i+V_t-4)},$$

де S_i – коефіцієнт, що характеризує можливу частоту виникнення відповідної i-ої загрози;

V_i – коефіцієнт що характеризує значення можливого збитку під час її виникнення.

Запропоновані значення коефіцієнтів приведені у таблицях 2 та 3 відповідно.

Для обчислення рівня витрат, що забезпечують необхідний рівень захищеності інформації, необхідно насамперед знати, по-перше, повний перелік загроз інформації, по-друге, потенційну небезпеку для інформації кожної із загроз, і, по-третє, розмір витрат, необхідний для нейтралізації кожної із загроз.

Таблиця 2.

Можливі значення коефіцієнтів S_i

Очікувана (можлива) частота появи загрози	Запропоноване значення S_i
Майже ніколи	0
1 раз на 1000 років	1
1 раз на 100 років	2
1 раз на 10 років	3
1 раз на рік	4
1 раз на місяць (приблизно 10 разів на рік)	5
2 рази на тиждень (100 разів на рік)	6
3 рази на день (1000 разів на рік)	7

Таблиця 3.

Можливі значення коефіцієнтів V_i

Значення можливого збитку при виявленні загрози (у.о.)	Запропоноване значення V_i
1	0
10	1
100	2
1000	3
10000	4

Строго теоретичний підхід заснований на тому, що потенційно можливі прояви загроз та рівні потенційно можливих збитків є випадковими подіями, саме тому можуть

бути охарактеризовані законами розподілу та числовими характеристиками. Суть даної моделі на змістовному рівні може бути представлена у наступному вигляді:

1. Введене поняття «середній коефіцієнт можливого вияву загрози» кожного типу, при чому воно розглядається як випадкова змінна з відомим розподілом ймовірностей f. Функція розподілу повинна визначатися на основі обробки статистичних даних, що збираються в процесі реального функціонування системи.

2. Зроблено припущення, що кількість проявів загрози r_t на протязі фіксованого періоду часу (наприклад, одного року) залежить тільки від тривалості періоду спостереження і середнього коефіцієнту прояву, в силу чого для числа прояву загроз справедливим визнано розподіл Пуассона:

$$P(\bar{r} = r / \lambda) = \frac{(\lambda t) r e^{-\lambda t}}{r!}.$$

3. По ряду значень числа загроз, отриманих для інтервалів різної тривалості, розподіл середнього коефіцієнта представлено у вигляді гамма-розподілу з параметрами, що характеризують ефективність захисту і визначеними по цілком певним рекурентним залежностям.

4. На основі інтегрування двох названих вище розподілень отримано безумовне розподілення ймовірностей числа прояву загроз за заданий період часу.

Розрахунки для оцінки очікуваних збитків полягають у наступному:

- спочатку розглядається середній збиток від прояву загроз і приймається нормальна функція його розподілу;
- по даним спостереження за проявами загроз і розміром збитків, що мали місце на інтервалах часу різної тривалості, корегуються параметри розподілу середнього збитку;
- виділяючи невизначені параметри із функції розподілу ймовірностей збитку, будується кінцевий розподіл розміру очікуваного збитку.

Теоретико-емпіричний підхід у відомій мірі оснований на синтезі основних положень теоретичного та емпіричного підходів. Суть синтезу полягає в тому, що на основі теоретико-ймовірносних методів будуються моделі, необхідні для визначення та прогнозування показників захищеності, а на основі збору та обробки статистичних даних, отриманих в ході теоретичних досліджень і практичних розробок проблем захисту інформації, формуються вихідні дані, необхідні для практичного використання моделей.

Розглянемо один з методів оцінки безпеки інформації, що відноситься до теоретико-емпіричного підходу. Комплексним показником оцінки безпеки при цьому обрано рівень безпеки інформації, що циркулює на об'єкті та характеризує можливість надання достатньої протидії виникненню каналів несанкціонованого отримання інформації (КНОІ) та причин порушення цілісності інформації (ППЦІ), що визначається як ймовірність забезпечення захисту інформації $P_{зі}$ на об'єкті:

$$P_{зі} = P_{кноі} \cdot P_{ппці},$$

де $P_{кноі}$ – ймовірність захисту інформації від витоку через КНОІ; $P_{ппці}$ – ймовірність забезпечення цілісності інформації.

Забезпечити захист інформації від зазначених видів загроз можна, вирішивши, як вказувалось вище, комплекс задач захисту інформації. Для вирішення даних задач повинні бути обрані типові методи та засоби. Рівень безпеки інформації в кінцевому випадку визначається здатністю застосованих засобів захисту перекрити характерні для об'єкта КНОІ та усунути ППЦІ (рис. 2).

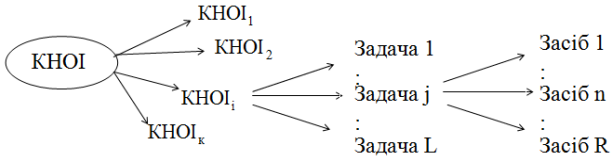

Рис. 2. Схематичне вирішення питання КНОІ об'єкту

Ймовірність захисту інформації на об'єкті від витоку через КНОІ визначається множиною каналів $\overline{K}$, характерних для даного об'єкту.

Виходячи з припущення про незалежність виникнення каналів, значення $P_{кноі}$ можна виразити як:

$$P_{кноі} = \prod_{i-1}^{\overline{K}} P_{кноі}.$$

Проблему перекриття КНОІ можна вирішити реалізацією різного роду задач із множини L, характерного для *i*-го КНОІ:

$$P_{кноі} = 1 - \prod_{j-1}^{L} (1 - P_З),$$

де $P_з$ – ймовірність забезпечення безпеки перекриття *i*-го КНОІ при вирішенні *j*-ої задачі захисту інформації. Це можливо зробити різними засобами із множини, що є в наявності на об'єкті:

$$P_з = 1 - \prod_{n-1}^{R} (1 - P_{ср}),$$

де $P_{ср}$ – ймовірність забезпечення безпеки *n*-м засобом захисту інформації. З урахуванням ризиків можна сформулювати:

$$P_з = 1 - \prod_{n-1}^{R} (1 - P_{ср}) - \frac{\sum_{i=1}^{n} n_i}{\sum_{i=1}^{n} (u_i - u)^2}.$$

Аналогічні залежності можна сформулювати і для розрахунку $P_{\text{ппці}}$. Розрахунок даних ймовірностей може проводитися по відомим методикам на основі статистичних оцінок коефіцієнтів безпеки, що виражають відношення поточного значення небезпечного сигналу до нормованого значення для відповідного каналу витоку інформації [4].

Емпірична залежність між фінансовими затратами на захист інформації і фінансовими збитками від несанкціонованого доступу до неї має вигляд:

$$C = 10^2 / \overline{R},$$

де C – фінансові затрати на захист інформації (у.о.) та $\overline{R}$ – фінансові збитки від несанкціонованого доступу до інформації (у.о.). Звідси можна сформулювати графічну залежність (рис.3) для C та $\overline{R}$, де $C+\overline{R}$ – повна очікувана вартість захисту інформації (у.о.), $S+V$ – інтегральний коефіцієнт, що враховує частоту появи можливих загроз та викликаних ними збитків:

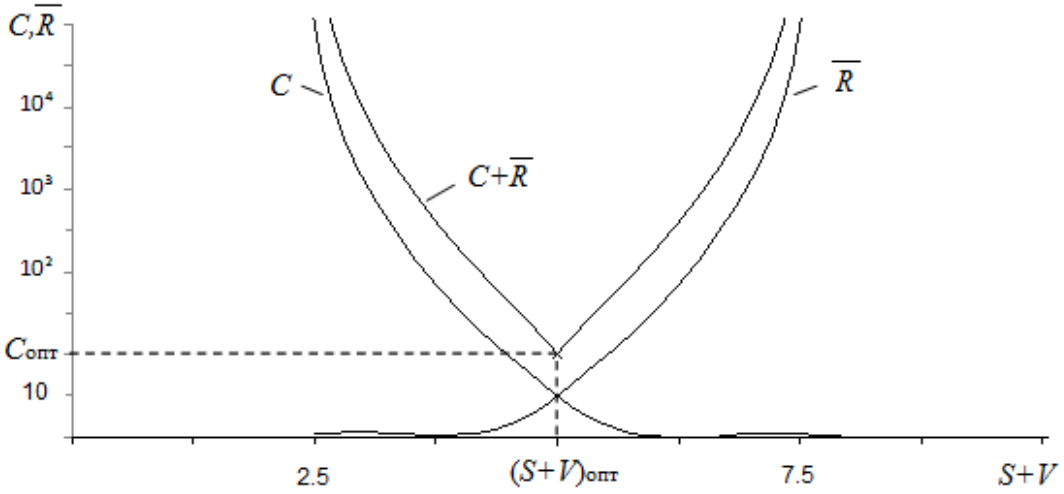

Рис. 3. Вартісні залежності захисту інформації від витоку через технічні канали витоку

Характеризуючи криву фінансових затрат на захист інформації (C), можна сказати, що зі зростанням інтегрального коефіцієнту $S+V$, що враховує частоту появи можливих загроз та викликаних ними збитків, спостерігається зменшення витрат на захист інформації. Для кривої фінансових збитків від несанкціонованого доступу до інформації ($\overline{R}$), є характерним збільшення витрат у випадку несанкціонованого доступу. Оптимальне значення досягається в точці екстремуму $C_{опт}$, оскільки саме при даному рівні затрат забезпечується мінімізація повної очікуваної вартості захисту інформації.

Висновки

В даній статті проведена класифікація технічних каналів витоку інформації з урахуванням можливих сучасних ризиків та аналіз їх особливостей. Приведена можливість кількісного визначення інтегрального показника, що характеризує ступінь безпеки інформації на об’єкті та визначає ймовірність витоку інформації, враховуючи всі фактори, що здійснюють значний вплив на його формування. На основі даного показника проводиться оцінка стану системи захисту інформації. Приведений строго-теоретичний та теоретико-емпіричний підхід для визначення рівня очікуваних втрат при порушенні захисту інформації. Якщо зібрати достатню кількість фактичних даних про проявлені загрози та їх наслідки, то розглянуті в статті моделі можна використовувати для вирішення широкого кола завдань по захисту інформації. Оптимальним варіантом вирішення поставленої задачі є витрати на захист інформації від витоку через технічні канали витоку фінансових коштів в розмірі $C_{опт}$, оскільки саме при даному рівні затрат забезпечується мінімізація повної очікуваної вартості захисту інформації.

Список літератури

1. Архипов, О.Є. Концептуалізація моделей ризиків / О.Є. Архипов, С.А. Архіпова // Захист інформації. – 2011. – №4. – С. 5–14.
2. Заячук, Я.І. Аналіз та оцінка ризиків інформаційної безпеки локальної обчислювальної мережі / Я.І. Заячук // Восточно-Европейский журнал передовых технологий. – 2012. – № 4/9(58). – С. 40-43.
3. Соболев, А.Н. Физические основы технических средств обеспечения информационной безопасности / А.Н. Соболев, В.М. Кирилов. – Москва: Гелиос АРВ, 2004. – 215 с.
4. Сёмкин, С.Н. Основы организационного обеспечения информационной безопасности объектов информатизации / С.Н. Сёмкин, Э.В. Беляков, С.В. Гребенев, В.И. Козачок. – Москва: Гелиос АРВ, 2005. – 183 с.

КРИТЕРИИ ОЦЕНКИ ВЕРОЯТНОСТИ УТЕЧКИ ИНФОРМАЦИИ ЧЕРЕЗ ТЕХНИЧЕСКИЕ КАНАЛЫ

Н.Г. Романюков

Главное управление министерства внутренних дел Украины в Одесской области,
ул. Еврейская, 12, Одесса, 65014, Украина; e-mail: kolyanr21@gmail.com

Проведена классификация современных технических каналов утечки информации и анализ их особенностей с учетом современных возможных рисков. Предложен способ количественного определения интегрального показателя, характеризующего степень безопасности информации на объекте и определяющего вероятность утечки информации, учитывая все факторы, которые осуществляют значительное влияние на его формирование. На основе данного показателя проводится оценка состояния системы защиты информации. Приведен строго-теоретический и теоретико-эмпирический подход для определения уровня ожидаемых потерь при нарушении защиты информации, что позволяет, при наличии возможностей сбора достаточного количества фактических данных о проявленных угрозах и их последствия, применять рассмотренные в статье модели для решения широкого круга задач по защите информации. Вычисляется эмпирическая величина уровней затрат, при которой обеспечивается минимизация полной ожидаемой стоимости защиты информации.

Ключевые слова: технические каналы утечки информации, модель процесса защиты, вероятность обеспечения безопасности.

CRITERIA FOR EVALUATING THE PROBABILITY OF INFORMATION LEAKAGE THROUGH TECHNICAL CHANNELS

N.G. Romanykov

General directorate of the ministry of internal affairs of Ukraine in Odessa region,
12 Evrejskaja Str., Odessa, 65014, Ukraine; e-mail: kolyanr21@gmail.com

Classification of modern technical channels of information leakage and the analysis of their characteristics, taking into account today's risks. A method for the quantitative determination of the integral index, which characterizes the degree of safety information on the object and determines the probability of leakage of information taking into account all the factors that exercise a significant influence on its formation. On the basis of this indicator assesses the status of information security systems. We have a strictly theoretical and theoretical-empirical approach to determine the level of expected losses in violation of the protection of information, allowing, where possible, to gather sufficient evidence of the manifestation of threats and their consequences, are considered to apply to become a model for a wide range of applications for protection information. Calculate the empirical value of the cost levels at which minimizes the total expected cost of information protection.

Keywords: technical channels of information leakage protection process model, the probability of safety.