УДК 004.056.2

МЕТОДИКИ ОЦІНЮВАННЯ ВЕЛИЧИН ЗАЛИШКОВИХ РИЗИКІВ У ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМАХ. ОЦІНКА ЗАЛИШКОВОГО РИЗИКУ ПРИ ЗАБЕЗПЕЧЕННІ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЙНИХ ОБ'ЄКТІВ

В. С. Василенко, канд. техн. наук, доц., ***О. В. Дубчак, М. Ю. Василенко***

bbc1@voliacable.com

У статті з використанням графічної моделі взаємодії загроз конфіденційності інформаційних ресурсів локальних обчислювальних систем з елементами системи захисту запропоновано процедури визначення як величини відповідного залишкового ризику, так і вихідних даних для його розрахунку, що дає змогу оцінити можливі умови застосування засобів захисту та їх склад.

Ключові слова: конфіденційність, цілісність, доступність інформації, залишкові ризики, локальні обчислювальні мережі.

In this paper, using graphical models of interaction threats Privacy Information Resource LAN with elements of protection proposed procedure for determining the values corresponding residual risk and the basic data for its calculation, to assess the possible conditions for the use of remedies and their composition.

Keyword: confidentiality, integrity, residual risk, LAN.

Вступ

Як відомо [1–3], основним завданням системи технічного захисту є забезпечення потрібного рівня функціональних властивостей конфіденційності, цілісності та доступності інформаційних ресурсів. Для оцінювання якості такої системи захисту методика визначення кількісних показників системи захисту у вигляді величин залишкових ризиків — імовірностей порушення згаданих функціональних властивостей передбачає виконання таких етапів:

1. Побудова графічних моделей взаємодії загроз функціональним властивостям захищеності із засобами захисту інформаційних ресурсів локальних обчислювальних мереж (ЛОМ).

2. Розроблення методик оцінювання величин залишкових ризиків у ЛОМ.

3. Розроблення методик визначення вихідних даних для оцінки залишкових ризиків у ЛОМ.

Методика виконання першого етапу викладена в праці [3]. Наступним є етап розроблення методик оцінки величин залишкових ризиків у ЛОМ.

Постановка задачі та результати досліджень

Отже, для визначення залишкового ризику при забезпеченні конфіденційності (імовірність отримання інформації порушником з розкриттям змісту) із урахуванням висновків, отриманих при розгляді графічної моделі взаємодії засобів [4] реалізації атак із засобами протидії цим загрозам — засобами забезпечення конфіденційності інформації (рис. 1), подію, пов'язану з порушенням конфіденційності, слід розглядати як складну та таку, що містить події:

– несанкціонованого отримання користувачем інформації тим чи іншим чином (несанкціонований доступ) з метою ознайомлення з нею чи будь-якого подальшого використання;

– розкриття змісту інформації з обмеженим доступом (ІзОД) після отримання її тим чи іншим чином. Останнє слід трактувати як можливість подолання порушником відповідних засобів криптозахисту.

При цьому ймовірність несанкціонованого доступу q_1 можна визначити з виразу:

$$q_1 = q_{\text{а.д}}\left[1-(1-q_{\text{о.с}})(1-q_{\text{у.ф.д}})(1-q_{\text{о.о.д}})(1-q_{\text{к.т.к.м}})\right], \quad (1)$$

де $q_{\text{а.д}}$ — імовірність подолання засобів адміністрування доступом; $q_{\text{о.с}}$ — імовірність подолання засобів охоронної сигналізації; $q_{\text{у.ф.д}}$ — імовірність подолання засобів управління фізичним доступом; $q_{\text{о.о.д}}$ — імовірність подолання засобів організаційного обмеження доступу; $q_{\text{к.т.к.м}}$ — імовірність порушення конфіденційності в засобах телекомунікаційної мережі (в разі використання ЛОМ, яка підключена до інших ЛОМ чи є елементом розподіленої мережі більш високого рівня).

Окрім того, несанкціоноване отримання користувачем інформації є можливим і через засоби віддаленого доступу до інформаційних об'єктів, використовуючи витоки інформації технічними каналами, вірусні атаки та засоби телекомунікаційної мережі за умови подолання неавторизованим користувачем відповідних засобів захисту.

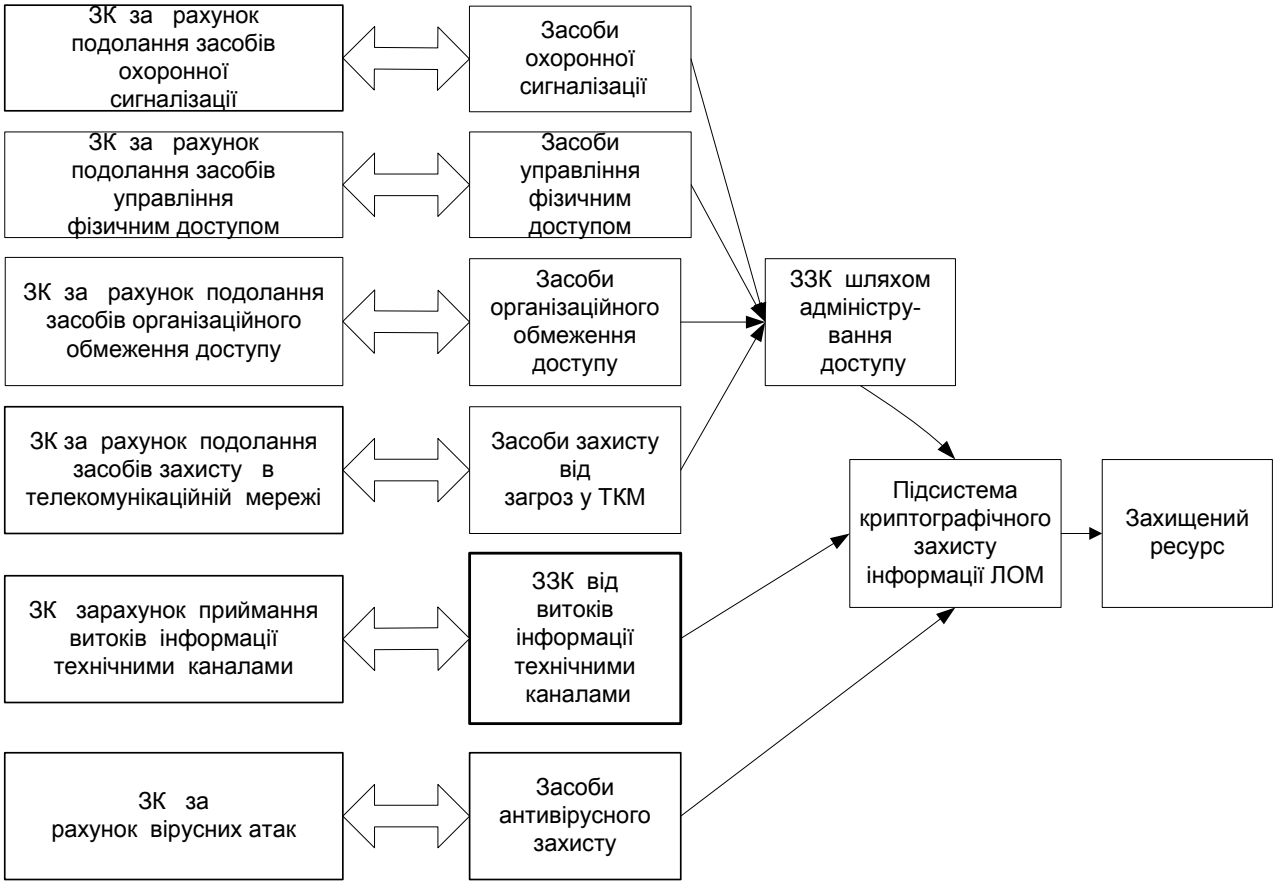

Рис. 1. Графічна модель процесу взаємодії засобів реалізації атак із засобами забезпечення конфіденційності інформації в ЛОМ

Примітка. Тут і надалі ймовірність подолання відповідного захисту за відсутності певних загроз того чи іншого виду вважається такою, що дорівнює нулю, а за відсутності засобів захисту від таких загроз — такою, що дорівнює одиниці.

Нехай імовірність подолання засобів захисту від витоків інформації технічними каналами дорівнює $q_{\text{зв}}$, а ймовірність подолання засобів антивірусного захисту — $q_{\text{ав}}$.

Після отримання ІзОД тим чи іншим шляхом порушнику необхідно здійснити розкриття її змісту. Подія, яка полягає в тому, що порушник може розкрити зміст ІзОД (за умови подолання системи захисту даного інформаційного об'єкта) є також складною і складається з трьох подій: першої — порушник знає мову, якою подається інформація; другої — порушник знає і може застосувати програмні засоби або апаратуру для криптографічного перетворення (для дешифрування закритої інформації); третьої — має необхідні ключі (ключові набори) для такого перетворення. Імовірності цих подій $P_{\text{з.м}}, P_{\text{з.к.п}}, P_{\text{к.н}}$ відповідно.

При цьому $q_{\text{к.з.і}}$ — імовірність подолання неавторизованим користувачем засобів криптозахисту (можливість розкрити зміст ІзОД) інформації можна визначити з виразу

$$q_{\text{кз.і}} = P_{\text{з.м}} \cdot P_{\text{з.к.п}} \cdot P_{\text{к.н}}.$$

Тоді вираз для розрахунку залишкового ризику при забезпеченні конфіденційності інформаційних об'єктів — імовірності порушення конфіденційності інформації q_{nk} з подоланням розглянутих засобів захисту можна записати у вигляді

$$q_{nk} = q_{\text{к.з.і}}\left[1-(1-q_1)\cdot(1-q_{\text{зв}})\cdot(1-q_{\text{ав}})\right].$$

Визначення вихідних даних для розрахунку залишкового ризику при забезпеченні конфіденційності інформації в ЛОМ

Отже, виходячи з викладеного, для розрахунків залишкового ризику при забезпеченні конфіденційності інформаційних об'єктів як вихідні дані необхідно визначити оцінки ймовірностей подолання порушником (відповідною загрозою) засобів:

– адміністрування доступом $q_{\text{а.д}}$;

– охоронної сигналізації $q_{\text{о.с}}$;

– управління фізичним доступом $q_{\text{у.ф.д}}$;

– організаційного обмеження доступу $q_{\text{о.о.д}}$;

– фільтрації зовнішніх (віддалених) загроз конфіденційності із телекомунікаційних мереж $q_{\text{к.т.к.м}}$;

– криптографічного захисту $q_{\text{кз.і}} = q_{\text{з.м}} \cdot q_{\text{з.к.п}} \cdot q_{\text{к.н}}$;

– захисту від витоків інформації технічними каналами $q_{\text{зв}}$;

– антивірусного захисту $q_{\text{а.в}}$.

Величина ймовірності $q_{\text{а.д}}$ *подолання засобів адміністрування доступом* з використанням механізмів базового та прикладного програмного забезпечення визначається можливостями системи автентифікації з використанням паролів відповідних користувачів. Величину цієї ймовірності можна визначити через кількість символів у паролі (довжину паролю)

$$q_{\text{а.д}} = 2^{-8n},$$

де n — кількість символів у паролі користувача.

Величина $q_{\text{о.с}}$ — імовірність *подолання засобів охоронної сигналізації* залежить від їх наявності у відповідних підрозділах, кількості меж виявлення, паспортних даних відповідних засобів виявлення (кутові та дальнісні параметри діаграм спрямованості) та умов їх застосування.

Величина ймовірності *подолання засобів управління фізичним доступом* $q_{\text{у.ф.д}}$ визначається наявністю та можливостями системи автоматичної автентифікації. Така автентифікація є можливою з використанням засобів контролю антропологічних характеристик (за папілярними візерунками пальців, райдужною оболонкою ока, особливостями голосу та ін.), носіїв Pin-кодів тощо. Наприклад, при використанні для управління фізичним доступом носіїв Pin-кодів величина ймовірності подолання засобів управління фізичним доступом визначається кількістю символів у Pin-коді (довжиною Pin-коду) та кількістю символів додаткової інформації для автентифікації користувача

$$q_{\text{у.ф.д}} = 2^{-8n},$$

де n — сумарна кількість символів у Pin-коді.

При використанні носіїв Pin-кодів типу безконтактних ідентифікаторів (чи інших, наприклад, карток контролю санкціонованого доступу) $q_{\text{у.ф.д}} = 2^{-k}$, де k — довжина коду, використаного для розміщення ідентифікаційної інформації (наприклад, при довжині унікального Pin-коду в 8 символів (байтів) $q_{\text{у.ф.д}} = 2^{-64}$, при використанні носіїв Pin-кодів з довжиною унікального Pin-коду в 8 символів та трьома областями пам'яті (ідентифікатор — 8 байтів, пароль — 8 байтів, області Secure — 48 байти $q_{\text{у.ф.д}} = 2^{-544}$).

Порядок визначення можливостей системи автоматичної автентифікації з використанням засобів контролю антропологічних характеристик виходить за межі цієї статті.

Величину $q_{\text{о.о.д}}$ — імовірності *подолання засобів організаційного обмеження доступу* (імовірність недотримання порушниками, у тому числі персоналом відповідних підрозділів, у яких використовуються ЛОМ, посадових інструкцій, наказів та розпоряджень керівництва щодо забезпечення безпеки інформації тощо) можна визначити методом експертних оцінок і взяти, наприклад, на рівні $q_{\text{о.о.д}} \approx 10^{-3}$.

Імовірність *подолання порушником (відповідною віддаленою загрозою) засобів фільтрації зовнішніх (віддалених) загроз конфіденційності із телекомунікаційних мереж* $q_{\text{к.т.к.м}}$ визначається характеристиками засобів та протоколів внутрішньо та зовнішньо мережевого обміну на транспортному, мережному та канальному рівнях семирівневої моделі взаємодії відкритих систем OSI.

Імовірність *подолання засобів криптографічного захисту* можна визначити з таких міркувань. Виходячи з моделей загроз та порушника, будемо вважати ймовірність знання порушником мови документу $q_{\text{з.м}} = 1$, та ймовірність наявності в нього засобів криптографічного перетворення, особливо у зв'язку із вимогами застосування в Україні засобів криптографічного захисту лише за алгоритмами по ГОСТ 28147-89,

$$q_{\text{з.к.п}} = 1.$$

Якщо в складі засобів ТЗІ *не використовуються засоби криптографічного перетворення* усієї критичної інформації, то величину ймовірності $q_{\text{к.н}}$ знання (наявності в порушника) ключових наборів також слід уважати такою, що $q_{\text{к.н}} = 1$.

У разі використання в складі засобів ТЗІ засобів криптографічного перетворення усієї критичної інформації, величину ймовірності того, що порушник має необхідні ключі для засобів криптографічного перетворення $q_{\text{к.н}}$, виходячи з умови їх надійного приховування відповідними користувачами, слід визначати з

урахуванням необхідності прямого перебору всіх можливих ключових наборів. Наприклад, якщо засобами криптографічного перетворення реалізується алгоритм, який аналогічний алгоритму за ГОСТ 28147-89 з кількістю варіантів ключів $N_{\text{кл}} = 2^{256}$, то закон розподілу цієї ймовірності можна вважати рівномірним, і ймовірність подолання засобів криптозахисту $P_{\text{к.з.і}}$ можна взяти рівною $q_{\text{к.н}} = N^{-1}_{\text{кл}} = 2^{-256}$. При цьому ймовірність порушення конфіденційності $q_{\text{п.к}}$ слід уважати знехтовно малою, незалежно від застосування інших засобів забезпечення конфіденційності.

Але такий варіант побудови системи захисту може бути неефективним у разі необхідності користувачам працювати з критичною інформацією: уводити з клавіатури, відображати на екранах моніторів тощо, — коли порушення конфіденційності може бути здійснено за рахунок витоків інформації технічними каналами.

Захист інформації від її витоків технічними каналами в ЛОМ слід розглядати [3] як сукупність заходів та засобів захисту від таких видів витоків:

– електромагнітних (каналами побічного електромагнітного випромінювання);

– електричних (за рахунок нерівномірності споживання струму);

– параметричних (паразитної генерації шляхом застосування спеціального «ВЧ- опромінювання», електромагнітне поле якого взаємодіє з елементами засобів обчислювальної техніки і модулюється інформаційним сигналом);

– при передачі інформації мережними кабелями (витік через мережні кабелі, особливо в разі розташування елементів ЛОМ у різних приміщеннях) з використанням індукційного перехоплення інформації.

За даними відкритого друку, сучасні індукційні датчики здатні знімати інформацію не тільки з ізольованих кабелів, але й з кабелів, захищених подвійною бронею зі сталевої стрічки й сталевого дроту.

Зрозуміло, що ймовірність подолання порушником (відповідною загрозою) засобів захисту від витоків інформації технічними каналами $q_{\text{з.в}}$ слід розглядати як імовірність складної події, яка полягає в наявності витоків тим чи іншим технічним каналом та в подоланні засобів захисту кожного із цих видів витоків.

Для визначення необхідності та можливостей із захисту від витоків ***технічними каналами*** в ЛОМ спочатку слід здійснити обстеження засобів ЛОМ на наявність та рівні потужності відповідних витоків. При цьому можливі принаймні два варіанти.

1. Нехай у результаті обстеження засобів обчислювальної техніки ЛОМ встановлено, що значення потужності $P_{\text{с}}$ витоку в діапазоні (у смузі) частот відповідних джерел витоку інформації (екрани, клавіатура, магнітні диски тощо) є близькими до нуля. При цьому як сервери, робочі станції, додаткові периферійні пристрої ЛОМ повинні бути застосовані такі засоби обчислювальної техніки, на яких проведено комплекси інженерно-технічних заходів із захисту від витоків технічними каналами відповідно до встановленої категорії обмеження доступу до інформації і які мають бути оформлені згідно з нормативними документами із захисту інформації приписи на експлуатацію. За цих умов імовірність подолання засобів захисту від витоків інформації технічними каналами можна вважати такою, що $P_{\text{з.в}} = 0$.

2. За відсутності умов за п. 1 інформація ЛОМ у точці її приймання повинна бути незрозумілою для порушника. При цьому ймовірність $P_{\text{з.в}}$ подолання засобів захисту від витоків інформації технічними каналами необхідно розглядати як імовірність такої події, коли під час приймання інформації порушник має змогу розуміти її зміст. Тобто запобігти витоку інформації технічними каналами можна шляхом забезпечення її надійного спотворення засобами створення (генерації) на вузлі ЦР ЄДАПС шуму, яким маскуються інформаційні сигнали.

Для визначення таких умов позначимо ймовірності наявності витоків електромагнітним, електричним, параметричним каналами та через мережні кабелі через $P_{\text{е.м.в}}, P_{\text{е.в}}, P_{\text{п.в}}$ та $P_{\text{м.к}}$ відповідно, а *умовні ймовірності* подолання засобів захисту кожного із цих видів витоків (за умови наявності відповідних витоків) — через $P_{\text{е.м.в}}, P_{\text{е.в}}, P_{\text{п.в}}, P_{\text{м.к}}$ тоді

$$q_{\text{з.в}} = P_{\text{е.м.в}} \cdot q_{\text{е.м.в}} + P_{\text{е.в}} \cdot q_{\text{е.в}} + P_{\text{п.в}} \cdot q_{\text{п.в}} + P_{\text{м.к}} \cdot q_{\text{м.к}}.$$

Методику розрахунку ймовірностей подолання засобів захисту кожного із цих видів витоків розглянемо на прикладі методики розрахунку ймовірностей подолання засобів захисту від електромагнітних витоків, яка складається з трьох етапів.

На першому етапі необхідно визначити ймовірності наявності кожного із видів витоків інформації ЛОМ. Це здійснюється за результатами обстеження приміщень та ЛОМ підприємства (їх засобів), під час якого встановлюються наявність, рівні відповідних витоків та здійснюється оцінювання їх імовірностей.

На етапі попередньої оцінки ймовірності наявності кожного із видів витоку визначаються службою захисту інформації підприємства методом експертних оцінок.

Як приклад, з урахуванням особливостей відокремленої ЛОМ підприємства (живлення підприємства від окремої підстанції, живлення кожної із ЛОМ окремими фідерами, наявність мережних фільтрів у фідерах живлення, надійного заземлення тощо, відсутність зв'язку з іншими ЛОМ) методом експертних оцінок можуть бути встановлені такі значення ймовірностей наявності:

– електромагнітних (каналами побічного електромагнітного випромінювання) витоків становить $P_{\text{е.м.в}} = 0{,}8$;

– електричних (за рахунок нерівномірності споживання струму) витоків становить $P_{\text{е.в}} = 0{,}2$;

– параметричних витоків дорівнює $P_{\text{п.в}} = 0$;

– витоків через мережні кабелі $P_{\text{м.к}} = 0\,P$.

Увага! При визначенні величин даних імовірностей слід дотримуватися нормуючої умови:

$$P_{\text{е.м.в}} + P_{\text{е.в}} + P_{\text{п.в}} + P_{\text{м.к}} = 1\,.$$

На другому етапі слід визначити умовні ймовірності подолання порушником засобів захисту за кожним із видів витоків — $q_{\text{е.м.в}}$, $q_{\text{е.в}}$, $q_{\text{п.в}}$, $q_{\text{м.к}}$.

Наведені нижче міркування щодо визначення умовних імовірностей подолання порушником засобів захисту для визначеності прив'язані до засобів захисту від витоків каналами побічного електромагнітного випромінювання, хоча, зрозуміло, цей підхід може бути застосованим і до засобів захисту від витоків й іншими технічними каналами витоку з урахуванням їх певних особливостей.

Оскільки умовою захисту інформації є запобігання приймання порушником без спотворень такої частки інформаційного об'єкта, яка є достатньою для сприйняття (розуміння) ним змісту даного інформаційного об'єкта (наприклад, повідомлення чи частки тексту), то не важко помітити, що така задача є класичною задачею визначення ймовірності приймання порушником сигналів в умовах впливу шумів (завад). Звідси витікає й методика визначення необхідних вихідних даних — умовних ймовірностей подолання порушником засобів захисту за кожним із видів витоків — $q_{\text{е.м.в}}, q_{\text{е.в}}, q_{\text{п.в}}, q_{\text{м.к}}$.

При цьому слід ураховувати, що основними засобами захисту конфіденційності інформації є засоби зниження в точці приймання співвідношення сигнал/шум (засоби екранування приміщень, де розташовані елементи ЛОМ, чи власне елементів ЛОМ та генератори шумів). У цьому випадку при забезпеченні захисту від витоків інформації технічними каналами умовну ймовірність подолання порушником засобів захисту можна трактувати як імовірність правильного приймання порушником інформаційних сигналів, спотворених шумами $q_{\text{е.м.в}} = 1 - P_{\text{сп}}$, де $P_{\text{сп}}$ — імовірність спотворення в одному символі (імовірність помилки).

Відомо, що ймовірність спотворення в одному біті (імовірність помилки) $P_{\text{сп}}$ є функцією співвідношення сигнал/шум h^2 (рис. 2):

$$P_{\text{сп}} = 1 - \Phi(\alpha)\,,$$

де $\alpha = \sqrt{h^2/2}$, а $\Phi(\alpha) = 1/\sqrt{2\pi}\int_{-\infty}^{\alpha} e^{-t^2/2}dt$ — функція Лапласа (інтеграл імовірності помилки).

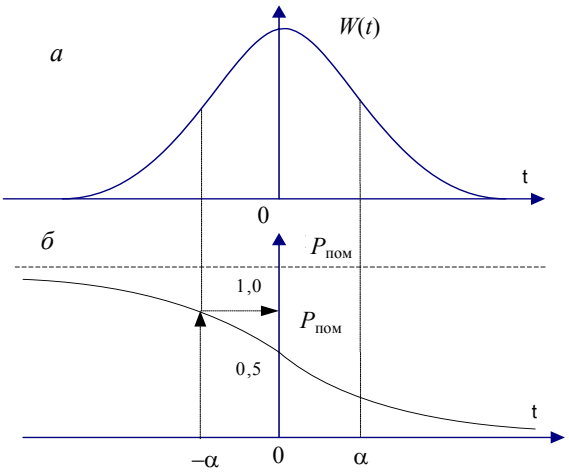

Рис. 2. Розрахунок імовірності спотворення символів:
а — центрована нормована щільність нормального закону ймовірностей; *б* – імовірність спотворення символу

Для обчислення цієї функції слід скористатися наступними відомими співвідношеннями. Для випадку $P_{\text{сп}} \le 0{,}5$:

$$\Phi(\alpha) = 1/\sqrt{2\pi}\int_{-\infty}^{\alpha} e^{-t^2/2}dt =$$

$$= 1/\sqrt{2\pi}\int_{-\infty}^{0} e^{-t^2/2}dt + 1/\sqrt{2\pi}\int_{0}^{\alpha} e^{-t^2/2}dt =$$

$$= 0{,}5 + 1/\sqrt{2\pi}\int_{0}^{\alpha} e^{-t^2/2}dt\,,$$

де $\Phi_0 = 1/\sqrt{2\pi}\int_{0}^{\alpha} e^{-t^2/2}dt$ — функція Лапласа–Гаусса, яка є табульованою.

Для цього випадку достатньо великих значень цього співвідношення $(h^2 \geq 3)$, а вираз для розрахунку цієї ймовірності матиме вигляд:

$$P_{\text{сп}} = 0,5 \cdot \exp\left(-\alpha^2 h^2 / 2\right),$$

де h^2 — співвідношення сигнал/шум; $h^2 = P_{\text{с}} / P_{\text{ш}}$; $P_{\text{с}}$ — потужність сигналу (у даному випадку — електромагнітного витоку) у діапазоні (в смузі) частот відповідного джерела витоку інформації (екрани, клавіатура, магнітні диски тощо); $P_{\text{ш}}$ — потужність адитивної суміші спеціальних шумів (шумів, які в даному випадку створюються спеціальними генераторами для маскування витоку сигналів), природних, індустріальних та інших шумів; α^2 — коефіцієнт, який залежить від виду модуляції сигналу ($\alpha^2 = 0,5$ для амплітудної модуляції, сигналів типу відеосигнал, що є притаманними локальним обчислювальним мережам).

Для випадку маскування сигналів (запобігання витоку інформації технічними каналами) з урахуванням природної надлишковості мови, яка перевищує 50 %, величину $P_{\text{пом}}$ за рахунок застосування генераторів шуму відповідної потужності чи за рахунок застосування засобів екранування приміщень або окремих елементів ЛОМ необхідно забезпечувати на рівні, який значно перевищує 0,5 і тоді (див. рис. 1):

$$\Phi(\alpha) = 1/\sqrt{2\pi} \int_{-\infty}^{\alpha} e^{-t^2/2}\, dt =$$

$$= 1/\sqrt{2\pi} \int_{-\infty}^{0} e^{-t^2/2}\, dt - 1/\sqrt{2\pi} \int_{0}^{\alpha} e^{-t^2/2}\, dt =$$

$$= 0,5 - 1/\sqrt{2\pi} \int_{0}^{\alpha} e^{-t^2/2}\, dt,$$

$$P_{\text{сп}} = 0,5 + 1/\sqrt{2\pi} \int_{0}^{\alpha} e^{-t^2/2}\, dt; \qquad (1)$$

$$q_{\text{е.м.в}} = 1 - P_{\text{сп}} = 0,5 - 1/\sqrt{2\pi} \int_{0}^{\alpha} e^{-t^2/2}\, dt,$$

причому при $P_{\text{сп}} \geq 0,5$ значення h^2 у виразі $\alpha = \sqrt{h^2/2}$ повинно відображати співвідношення потужностей не сигналу і шуму, а навпаки, — співвідношення потужностей шуму і сигналу.

Вираз (1) доцільно використовувати при $P_{\text{сп}} \leq 0,997$ $(h^2 \leq 3)$, коли можна скористатися таблицями інтегралу Гаусса.

Неважко зрозуміти, що для даного випадку й достатньо великих значень цього співвідношення $(h^2 \geq 3, P_{\text{сп}} \geq 0,997)$ вираз (1) для розрахунку останньої ймовірності набуде вигляду:

$$P_{\text{сп}} = 1 - 0,5 \cdot \exp\left(-\alpha^2 / 4\right).$$

Отже, для випадку застосування генераторів маскуючих шумів і $P_{\text{сп}} \geq 0,5$ при $h^2 \geq 3$:

$$q_{\text{е.м.в}} = 0,5 \cdot \exp\left(-h^2 / 4\right). \qquad (2)$$

Зауважимо, що оскільки генератори шуму та джерела витоків інформації відносно до засобів їх перехоплення (приймання) розташовані практично в одному місці (враховуючи, що відстань від точки приймання витоків до джерела витоків практично дорівнює відстані від точки приймання витоків до генератора), то співвідношення сигнал/шум у точці приймання є близьким до ***співвідношення сигнал/шум у точці, яка розташована в безпосередній близькості до джерела витоків***.

Визначення величин $P_{\text{с}}$ — потужності сигналу (у даному випадку – електромагнітного витоку) в діапазоні (у смузі) частот відповідного джерела витоку інформації (системні блоки, монітори, клавіатура, магнітні диски та таке інше) та $P_{\text{ш}}$ — потужності адитивної суміші спеціальних шумів (шумів, які в цьому випадку створюються спеціальними генераторами для маскування витоку сигналів), природних, індустріальних та інших шумів, а відтак — і співвідношення h^2 **здійснюється за результатами обстеження приміщень та елементів ЛОМ підприємства.**

Захист інформації від електричних витоків (за рахунок нерівномірності споживання струму), паразитної генерації та від витоків через мережні кабелі з використанням індукційного перехоплення інформації тощо, слід забезпечувати спеціальними елементами захисту інформації ЛОМ від витоку технічними каналами та спеціального впливу на неї (мережні та інші фільтри, надійне заземлення тощо) Склад цих засобів, їх компонентів, механізмів, функцій та їх необхідні характеристики (коефіцієнти ослаблення сигналів витоку) визначаються на підставі обстеження відповідних джерел витоку інформації з урахуванням вимог Плану ТЗІ та політики безпеки організації як складової Плану ТЗІ.

Методика визначення умовної ймовірності подолання порушником засобів захисту від

електричних витоків $q_{\text{е.в}}$, паразитної генерації $q_{\text{п.г}}$, витоків через мережні кабелі з використанням індукційного перехоплення інформації $q_{\text{м.к}}$ та відповідних вихідних даних не відрізняється від вище наведеної методики щодо визначення умовної ймовірності подолання порушником засобів захисту від електромагнітних витоків

Третій етап передбачає визначення шуканої ймовірності подолання порушником засобів захисту від порушення конфіденційності інформації за рахунок приймання витоків інформації технічними каналами:

$$q_{\text{з.в}} = P_{\text{е.м.в}} \cdot q_{\text{е.м.в}} + P_{\text{е.в}} \cdot q_{\text{е.в}} + P_{\text{п.в}} \cdot q_{\text{п.в}} + P_{\text{м.к}} \cdot q_{\text{м.к}} .$$

Приклади. Визначимо ймовірності подолання порушником засобів захисту від порушення конфіденційності інформації за рахунок приймання витоків інформації технічними каналами для умов визначених на підставі обстежень співвідношень **шум/сигнал** h^2.

У таблиці наведено деякі проміжні результати та результати визначення шуканої ймовірності для значень $h^2 = (0,54; 1,41; 3,24; 22)$. В останньому рядку таблиці наведено результати з використанням виразу (2).

h^2	$h^2/2$	$\Phi_0^{-1} = \alpha = \sqrt{h^2/2}$	Φ_0	$P_{\text{сп}}$	$q_{\text{з.в}}$
0,54	0,27	0,52	0,2	0,7	0,3
1,41	0,706	0,84	0,3	0,8	0,2
3,24	1,64	1,28	0,4	0,9	0,2
22	11	–	–	0,998	0,002

Звернемо увагу на те, що значення співвідношення сигнал/шум на виході відповідних засобів захисту дорівнює практично коефіцієнту ослаблення сигналів витоку даного засобу.

Методика визначення умовної ймовірності подолання порушником засобів захисту від електричних витоків $q_{\text{е.в}}$, паразитної генерації $q_{\text{е.в}}$, від витоків через мережні кабелі $q_{\text{м.к}}$ та відповідних вихідних даних не відрізняється від вище наведеної методики щодо визначення умовної ймовірності подолання порушником засобів захисту від електромагнітних витоків.

Отже, для випадку необхідності застосування маскування сигналів (запобігання витоку інформації технічними каналами) потужність шуму відповідних генераторів повинна бути не меншою, ніж

$$P_{\text{ш}} \geq -2P_{\text{с}} \left(2\ln 2 + 0,25 \ln q_{\text{кр.прип}}\right),$$

де $q_{\text{кр.прип}}$ — припустиме для ЛОМ з відповідним грифом обмеження доступу значення ймовірності розкриття змісту інформації.

Це значення встановлюється власником інформації. В разі відсутності встановленого власником значення такої ймовірності її слід вважати такою, що дорівнює ймовірності розкриття змісту інформації, яку забезпечують засоби криптографічного перетворення за ГОСТ 28147 $P_{\text{кр.прип}} = 2^{-256}$.

Під час застосування генераторів шуму з меньшою потужністю $P_{\text{ш}}$ імовірність подолання неавторизованим користувачем засобів захисту інформації від її витоків технічними каналами визначається за виразом

$$q_{\text{е.м.в}} = \left(0,5\exp\left[-1/(4h^2)\right]\right)^s ,$$

де $h^2 = P_{\text{ш}}/P_{\text{с}}$.

Імовірності подолання порушником (відповідною загрозою) засобів антивірусного захисту $q_{\text{а.в}}$ можна визначити, якщо відомо співвідношення між кількістю вірусів, занесених у базу засобів антивірусного захисту та загальною кількістю існуючих, точніше відомих на час оцінки вірусів. Наприклад, якщо кількість вірусів, занесених у базу засобів антивірусного захисту, дорівнює $N_{\text{в.з}}$, а загальна кількість відомих вірусів — $N_{\text{в.в}}$, то величину $q_{\text{а.в}}$ можна визначити за формулою

$$q_{\text{з.в}} = 1 - N_{\text{в.з}}/N_{\text{в.в}} .$$

Висновки

У статті з метою оцінки захищеності конфіденційності інформації в ЛОМ запропоновано використання методик оцінювання величини залишкового ризику в ЛОМ та відповідних вихідних даних для його розрахунку. Такі методики дають змогу здійснювати обґрунтований вибір сукупностей засобів захисту конфіденційності та в подальшому оцінити ймовірності порушення конфіденційності відповідних інформаційних об‘єктів ЛОМ.

ЛІТЕРАТУРА

1. *Загальні* положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу (НД ТЗІ 1.1-002-99);

2. *Критерії* оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу (НД ТЗІ 2.5-004-99);

3. *Матов О. Я.* Визначення залишкового ризику при оцінці захищеності інформації в інфор-

маційно-телекомунікаційних системах // Реєстрація, зберігання і обробка даних / О. Я. Матов, В. С. Василенко, М. М. Будько. — 2004. — Т. 6, № 2. — С. 62–74.

4. *Василенко В. С.* Методика оцінки захищеності інформації в ЛОМ. Графічні моделі взаємодіїзагроз функціональним властивостям захищеності інформаційних ресурсів ЛОМ із елементами системи захисту. / В. С. Василенко, О. В. Дубчак, М. Ю. Василенко // Безпека інформації — № 1 (17). — 2012. — С. 49–54.

REFERENCES

1. *Zagalni* polozhennja schodo zakhystu informazii v komputernykh systemakh vid nesankzionovanogo dostupu (ND TZI 1.1 – 002-99).

2. *Kryterii* ozinky zakhyschenosti informazii v komputernykh systemakh vid nesankzionovanogo dostupu (ND TZI 2.5 – 004 – 99).

3. *Matov O. Ja*. Vyznachennja zalyshkovogo ryzyku pry ozinzi zakhyschennosti informazii v informazijno-komunikazijnykh systemakh / O. Ja. Matov, V. S. Vasylenko, M. M. Budko // Reestrazija, zberigannja i obrobka danykh, 2004, T. 6, #2. — S. 62–74.

4. *Vasylenko V. S.* Metodyka ozinky zakhyschenosti informazii v LOM. Graphichnimodeli vzaemodii zagroz funkzionalnym vlastyvostjam zakhyschennosti informazijnykh resursiv LOM z elementamy systemy zakhystu / V. S. Vasylenko, O. V. Dubchak, M Ju. Vasylenko// Bezpeka informazii. — #1 (17). — 2012. — S. 49–54.

Стаття надійшла до редакції 14.10.2013