УДК 004.056.2

В. С. Василенко[1], О. Я. Матов[2]
[1]Національний авіаційний університет
вул. Космонавта Комарова, 1, 03058 Київ, Україна
[2]Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна

Методики визначення вихідних даних для оцінки залишкових ризиків при забезпеченні конфіденційності інформаційних об'єктів

Для аналізу захищеності інформації автоматизованих систем запропоновано застосування кількісних характеристик у вигляді величин залишкового ризику чи ймовірностей подолання порушником засобів захисту тих чи інших властивостей захищеності. Для оцінки захищеності конфіденційності інформації телекомунікаційних мереж з використанням відповідних систем захисту інформації запропоновано математичні моделі для визначення ймовірностей подолання порушником складових системи захисту конфіденційності.

Ключові слова: *загроза, захист, конфіденційність, модель, порушник, ресурси, телекомунікаційна мережа.*

Вступ

Загально відомо, що на сучасному етапі розвитку телекомунікаційних мереж (ТКМ) захист їхніх ресурсів, насамперед інформації, є дуже важливою і актуальною проблемою. Для цього розробляються чи використовуються системи захисту, які забезпечують той чи інший рівень захищеності інформації Нормативними документами Системи технічного захисту України [1]. Визначено наступні властивості захищеності інформації: конфіденційність, цілісність, доступність. Відомо розробки щодо оцінки цих властивостей захищеності. Так, у роботі [2] запропоновано методику оцінки загроз ресурсам інформаційних систем на основі аналізу моделей порушника, можливих каналів і видів загроз ресурсам інформаційних систем, моделі загроз і методику аналізу можливих контрзаходів для забезпечення припустимої захищеності та залишкового ризику. Окрім того, в [3] для оцінки захищеності інформації автоматизованих систем запропоновано моделі відповідних систем захисту інформації і методики визначення ймовірностей подолання порушником засобів захисту тих чи інших властивостей захищеності — величин залишкового ризику. Як величину залишкового ризику при забезпеченні конфіденцій-

ності у цих роботах запропоновано ймовірність порушення конфіденційності — $q_{пк}$. Показано, що для забезпечення безпеки інформаційних об'єктів необхідним є застосування певних засобів захисту, а для визначення згаданого ризику — знання їхніх відповідних характеристик у вигляді ймовірностей їхнього подолання потенційними порушниками. Цими засобами є засоби захисту від несанкціонованого доступу з імовірністю їхнього подолання q_1 у складі засобів адміністрування доступом (з імовірністю подолання $q_{ад}$); засобів охоронної сигналізації (з імовірністю подолання $q_{ос}$); засобів управління фізичним доступом (з імовірністю подолання $q_{уфд}$); засобів організаційного обмеження доступу (з імовірністю подолання q_{ood}); засобів захисту конфіденційності у засобах телекомунікаційної мережі (в разі використання ТКМ, яка є підключеною до інших ТКМ підприємства чи є елементом розподіленої мережі більш високого рівня) (з імовірністю подолання $q_{кткм}$)). Окрім того, для виключення несанкціонованого отримання користувачем інформації через засоби віддаленого доступу до інформаційних об'єктів, використовуючи витоки інформації (з імовірністю подолання $q_{зві}$), та вірусні атаки (з імовірністю їм протидії $q_{ав}$), а також засобів контролю цілісності (з імовірністю подолання $q_{кц}$) та засобів забезпечення доступності (з імовірністю їм протидії $q_{пд}$).

Чисельні значення відповідних змінних для розрахунку згаданих показників захищеності інформації (величин залишкового ризику — ймовірностей порушення тієї чи іншої властивості захищеності інформації), можуть бути або розрахованими (більшість з них), якщо відомі їхні складові чи закони розподілу відповідних ймовірностей, або можуть бути визначеними методом експертних оцінок. В останньому випадку ці показники потребують уточнення чи корегування службою захисту інформації, виходячи з досвіду експлуатації чи застосування системи захисту інформації з відповідною корекцією Планів захисту інформації, заходів із захисту, складу та можливостей засобів захисту тощо.

У цій статті, у більшості випадків, розподіл імовірностей подій, що пов'язані зі спробами несанкціонованого доступу до інформаційних ресурсів, вважається рівномірним. Це пов'язано з тим, що, по-перше, такий закон розподілу є найскладнішим для функціонування систем захисту, а по-друге, з відсутністю підстав для використання математичних апаратів інших законів розподілу. У разі можливості визначення параметрів потоків випадкових величин потрібні значення ймовірностей, що визначені із використанням відповідного математичного апарату.

Нижче викладено співвідношення для практичного визначення показника захищеності конфіденційності інформації з урахуванням попередніх зауважень.

Методики визначення вихідних даних для оцінки залишкових ризиків при забезпеченні захисту конфіденційності інформації

Нагадаємо, що в [3] величину залишкового ризику — ймовірність порушення конфіденційності $q_{пк}$ — визначено як

$$q_{пк} = q_{кзі}\cdot[1 - (1 - q_1)\cdot(1 - q_{зв})\cdot(1 - q_{ав1})],$$

де

$$q_1 = q_{ад}\cdot[1 - (1 - q_{ос})\cdot(1 - q_{уфд})\cdot(1 - q_{ood})\cdot(1 - q_{кткм})].$$

Тому як вихідні дані для визначення показників конфіденційності інформації необхідно визначити ймовірності подолання порушником (відповідною загрозою) засобів:

1) криптографічного захисту $q_{кзі}$;

2) захисту інформації від несанкціонованого доступу q_1, для чого, у свою чергу, слід визначити ймовірності подолання: засобів управління фізичним доступом $q_{уфд}$ адміністрування доступом $q_{ад}$, організаційного обмеження доступу q_{ood}, охоронної сигналізації $q_{ос}$, засобів захисту від впливів з телекомунікаційної мережі $q_{кткм}$;

3) захисту від витоків інформації технічними каналами $q_{зв}$;

4) антивірусного захисту $q_{ав}$.

Визначення ймовірності подолання засобів криптографічного захисту

При визначенні ймовірності подолання порушником (відповідною загрозою) засобів криптографічного захисту для випадку використання у відповідній ТКМ підприємства певних алгоритмів криптозахисту (наприклад, за ГОСТ 28147–89)

$$q_{кзі} = q_{зм} \cdot q_{зкп} \cdot q_{кн}$$

будемо вважати ймовірність знання порушником мови документу $q_{зм} = 1$, та ймовірність $q_{зкп}$ наявності в нього засобів криптографічного перетворення $q_{зкп} = 1$.

Примітка. При використанні у складі засобів технічного захисту інформації (ТЗІ) засобів криптографічного перетворення критичної інформації, величину ймовірності того, що порушник має необхідні ключі для засобів криптографічного перетворення $q_{кн}$, виходячи з умови їхнього надійного приховування відповідними користувачами, слід визначати з врахуванням необхідності прямого перебору всіх можливих ключових наборів.

Приклад. Якщо засобами криптографічного перетворення реалізується алгоритм за ГОСТ 28147–89, або аналогічний йому, з кількістю варіантів ключів $N_{кл} = 2^{256}$, то закон розподілу цієї імовірності можна вважати рівномірним, і ймовірність подолання засобів криптозахисту $P_{кзі}$ може бути прийнятою рівною $q_{кн} = N_{кл}^{-1} = 2^{-256}$. При цьому ймовірність порушення конфіденційності $q_{пк}$ слід вважати знехтувано малою, незалежно від застосування інших засобів забезпечення конфіденційності.

За таких умов: $q_{кзі} = 2^{-256}$.

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

В останньому випадку, а також у разі відсутності у складі засобів ТЗІ засобів криптографічного перетворення *критичної інформації*, величину ймовірності $q_{кн}$ знання (наявності в порушника) ключових наборів слід вважати такою, що $q_{кн} = 1$, і тоді $q_{кзі} = 1$.

Визначення ймовірності подолання засобів захисту інформації від несанкціонованого доступу

Нагадаємо, що ймовірність подолання засобів захисту інформації від несанкціонованого доступу

$$q_1 = q_{ад}\cdot[1 - (1 - q_{ос})\cdot(1 - q_{уфд})\cdot(1 - q_{ood})\cdot(1 - q_{кткм})],$$

Величина $q_{ад}$ ймовірності 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)

$$q_{ад} = 2^{-8n},$$

де n — кількість символів у паролі користувача.

Приклад. При довжині пароля користувача у 8 символів $q_{ад} = 2^{-64}$.

Величина $q_{ос}$ — ймовірності подолання засобів охоронної сигналізації визначається їхньою наявністю у відповідних підрозділах, кількістю рубежів виявлення, паспортними даними відповідних засобів виявлення (надійність пульта охоронної сигналізації, датчиків (перш за все, їхніх контактних груп), ліній сполучення датчиків з пультом, кутові та дальностні параметри діаграм направленості, чутливість на рух і т.п.) та умовами їхнього застосування.

Не важко зробити висновок що в разі використання у якості засобів охоронної сигналізації приміщень, де використовується елементи ТКМ, s рубежів виявлення з імовірністю $q_{осj}$ подолання j-го із цих рубежів будуть:

$$q_{ос} = \prod_{j=1}^{s} q_{осj}\ .$$

Наприклад, у разі використання одного рубежу виявлення (контактні групи на вхідних дверях і датчики порушення цілісності на вікнах), як імовірність подолання засобів охоронної сигналізації можна використати показники надійності цього засобу (контактних груп і пульта охоронної сигналізації), тобто — ймовірність безвідмовної роботи на інтервалі використання $P_1(t)$, де t — тривалість інтервалу використання:

$$q_{ос1} = P_1(t) = \exp(-\lambda t),$$

де λ — інтенсивність відмов засобів охоронної сигналізації.

Приклад. При $\lambda = 10^{-7}$ 1/с, $t = 56880$ с (15 год. 48 хв.) $\lambda t = 5{,}688\cdot10^{-3}$. Врахуємо ту властивість експоненційних функцій, що при $x << 1$ $\exp(-x) \approx 1 - x$, а відтак $1 - \exp(-x) \approx x$:

$$q_{ос} = 1 - P_1(t) = 5{,}688\cdot10^{-3}.$$

При використанні двох рубежів охоронної сигналізації, наприклад, окрім вищенаведеної, системи з використанням датчиків руху з аналогічною ймовірністю безвідмовної роботи на інтервалі використання:

$$q_{ос} = 1 - (1 - P_1(t))\cdot(1 - P_2(t)) \approx (5{,}688\cdot10^{-3})^2 = 3{,}2\cdot10^{-5}.$$

Величина $q_{уфд}$ ймовірності подолання засобів управління фізичним доступом визначається можливостями системи автоматичної автентифікації з використанням 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:

$$q_{уфд} = 2^{-8k},$$

де k — довжина коду, використаного для розміщення ідентифікаційної інформації у персональному ідентифікаторі (Pin-коді) та в додатковій інформації для автентифікації користувача при використанні носіїв Pin-кодів.

Приклад. Для носіїв Pin-кодів з довжиною унікального Pin-коду у 8 символів (байтів) $q_{уфд} = 2^{-64}$, при використанні носіїв Pin-кодів з довжиною унікального Pin-коду у 8 символів і трьома областями пам'яті (ідентифікатор — 8 байтів, пароль — 8 байтів, області Secure — 48 байти) — $q_{уфд} = 2^{-544}$.

Величину q_{ood} — ймовірності подолання засобів організаційного обмеження доступу (ймовірність недотримання порушниками, в тому числі персоналом відповідних підрозділів підприємства, у яких використовуються ТКМ, посадових інструкцій, наказів і розпоряджень керівництва щодо забезпечення безпеки інформації тощо) можна визначити *методом експертних оцінок.*

Приклад. Нехай величина ймовірності подолання засобів організаційного обмеження доступу методом експертних оцінок прийнята на рівні

$$q_{ood} = 10^{-3}.$$

Величину $q_{кткм}$ — ймовірності подолання засобів захисту від впливів із телекомунікаційної мережі для випадку підприємства при використанні ізольованих ТКМ слід вважати такою, що

$$q_{кткм} = 0.$$

Приклад. Нехай величини подолання відповідних засобів захисту інформації від несанкціонованого доступу визначено такими, як і раніше, тобто:

$$q_{ад} = 2^{—64} = 10^{-19},\ q_{ос} = 3{,}2\cdot 10^{-5},\ q_{уфд} = 2^{-544},\ q_{ood} = 10^{-3},\ q_{кткм} = 0.$$

Тоді, використовуючи те, що $q_{кткм} = 0$ та приблизну рівність $\prod_{j=1}^{s}(1-q_j) \approx 1-\sum_{j=1}^{s} q_j$ (розклад добутку в ряд Маклорена при обмеженні першими двома членами ряду), отримаємо:

$$q_1 = q_{ад}\cdot[1-(1-q_{ос})\cdot(1-q_{уфд})\cdot(1-q_{ood})\cdot(1-q_{кткм})] \approx$$
$$\approx 2^{-64}\cdot(q_{ос}+q_{уфд}+q_{ood}) \approx 10^{-19}\cdot 10^{-3} \approx 10^{-22} \approx 2^{-74}.$$

Визначення ймовірності подолання засобів захисту інформації від її витоків технічними каналами

Захист інформації від її витоків технічними каналами в ТКМ слід розглядати як сукупність заходів і засобів захисту від наступних видів витоків:

— електромагнітних (по каналам побічного електромагнітного випромінювання);

— електричних (за рахунок нерівномірності споживання струму);

— параметричних (паразитної генерації шляхом застосування спеціального ВЧ-опромінювання, електромагнітне поле якого взаємодіє з елементами захисту і модулюється інформаційним сигналом);

— при передачі інформації мережними кабелями (витік через мережні кабелі, особливо в разі розташування елементів ТКМ 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, які захищені подвійною бронею зі сталевої стрічки та сталевого дроту.

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

Позначимо ймовірності наявності витоків електромагнітним, електричним, параметричним каналами та через мережні кабелі через $P_{емв}$, $P_{ев}$, $P_{пв}$ та $P_{мк}$ відповідно, а умовні ймовірності подолання засобів захисту кожного із цих видів витоків (за умови наявності відповідних витоків) — через $q_{\text{емв}}$, $q_{\text{ев}}$, $q_{\text{пв}}$, $q_{\text{мк}}$. Тоді:

$$q_{зв} = P_{емв} \cdot q_{\text{емв}} + P_{ев} \cdot q_{\text{ев}} + P_{пв} \cdot q_{\text{пв}} + P_{мк} \cdot q_{\text{мк}}.$$

При цьому методика розрахунку ймовірностей подолання засобів захисту кожного із цих видів витоків полягає в наступному.

Перш за все, необхідно визначити ймовірності наявності кожного із видів витоків інформації кожної із ТКМ підприємства. Це здійснюється за результатами обстеження приміщень і ТКМ підприємства (їхніх засобів), під час якого встановлюються наявність, рівні відповідних витоків і здійснюється оцінка їхніх імовірностей.

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

Звернемо увагу, що при визначенні величин даних імовірностей слід дотримуватися нормуючої умови:

$$P_{емв} + P_{ев} + P_{пв} + P_{мк} = 1.$$

Приклад. З урахуванням особливостей ТКМ деякого підприємства (наприклад, живлення підприємства від окремої підстанції, живлення кожної із ТКМ окремими фідерами, наявність мережних фільтрів у фідерах живлення, надійного заземлення тощо) методом експертних оцінок можуть бути встановлені наступні значення ймовірностей:

1) імовірність наявності електромагнітних витоків (по каналам побічного електромагнітного випромінювання) становить $P_{емв} = 1$;

2) імовірність наявності електричних витоків (за рахунок нерівномірності споживання струму) становить $P_{ев} = 0$;

3) імовірність наявності параметричних витоків дорівнює $P_{пв} = 0$;

4) імовірність витоків через мережні кабелі $P_{мк} = 0$.

Також необхідно визначити *умовні ймовірності* подолання порушником засобів захисту по кожному із видів витоків $q_{емв}$, $q_{ев}$, $q_{пв}$, $q_{мк}$.

Нижче наведено міркування щодо визначення умовних імовірностей подолання порушником засобів захисту для визначеності прив'язані до засобів захисту від витоків по каналам побічного електромагнітного випромінювання, хоча, зрозуміло, цей підхід може бути застосованим і до засобів захисту від витоків й іншими технічними каналами витоку з урахуванням їхніх 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). Звідсіля витікає й методика визначення необхідних вихідних даних — умовних імовірностей подолання порушником засобів захисту по кожному із видів витоків — $q_{емв}$, $q_{ев}$, $q_{пв}$, $q_{мк}$.

При цьому слід враховувати, що основними засобами захисту конфіденційності інформації є засоби зниження в точці приймання співвідношення сигнал/шум (засоби екранування приміщень, де розташовані елементи ТКМ, чи власне елементів ТКМ і 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, які спотворені шумами $q_{емв} = 1 - P_{сп}$, де $P_{сп}$ — ймовірність спотворення в одному біті (ймовірність спотворення).

Відомо [5], що ймовірність спотворення в одному біті (ймовірність спотворення) $P_{сп}$ є функцією співвідношення сигнал/шум h^2 (див. рисунок [6, 7]):

$$P_{сп} = 1 - \Phi(\alpha),$$

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

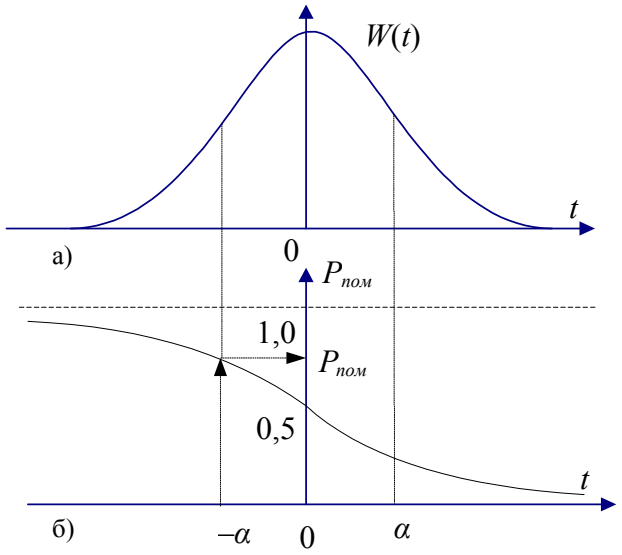
$$\Phi(\alpha) = 1/\sqrt{2\pi}\int_{-\infty}^{\alpha} e^{-t^2/2}dt = 1/\sqrt{2\pi}\int_{-\infty}^{0} e^{-t^2/2}dt + 1/\sqrt{2\pi}\int_{0}^{\alpha} e^{-t^2/2}dt = 0{,}5 + 1/\sqrt{2\pi}\int_{0}^{\alpha} e^{-t^2/2}dt,$$

де $\Phi_0 = 1/\sqrt{2\pi}\int_{0}^{\alpha} e^{-t^2/2}dt$ — функція Лапласа-Гауса, яка є табульованою. Для даного випадку та достатньо великих значень цього співвідношення ($h^2 \ge 3$) вираз для розрахунку цієї імовірності може бути наданим у вигляді [5]:

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

де h^2 — співвідношення сигнал/шум; $h^2 = P_c/P_ш$, $P_с$ — потужність сигналу (в даному випадку – електромагнітного витоку) у діапазоні (у смузі) частот відповідного джерела витоку інформації (екрани, клавіатура, магнітні диски та таке інше); $P_ш$ — потужність адитивної суміші спеціальних шумів (шумів, які в даному випад-

ку 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).



До розрахунку ймовірності спотворення символів: а) центрована нормована щільність нормального закону ймовірностей; б) ймовірність спотворення символу

Для випадку маскування сигналів (запобігання витоку інформації технічними каналами) з урахуванням природної надлишковості мови, яка перевищує 50 %, величину $P_{сп}$ за рахунок застосування генераторів шуму відповідної потужності чи за рахунок застосування засобів екранування приміщень або окремих елементів ТКМ необхідно забезпечувати на рівні, який значно перевищує 0,5, і тоді [6, 7]:

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

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

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

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

Вираз (1) слід і доцільно використовувати при $P_{сп} \leq 0{,}997$ ($h^2 \leq 3$), коли можна скористатися таблицями інтегралу Гауса. Неважко зрозуміти, що для даного випадку та достатньо великих значень цього співвідношення ($h^2 \geq 3$, $P_{сп} \geq 0{,}997$) вираз (1) для розрахунку останньої імовірності може бути наданим у вигляді:

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

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

$$q_{емв} = 0{,}5\exp(-h^2/4). \quad (3)$$

Зауважимо, що оскільки генератори шуму по відношенню до джерел витоків інформації розташовані практично в одному місці (враховуючи, що відстань від точки приймання витоків до джерела витоків і відстань від точки приймання витоків до генератору шуму практично однакові), 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_c — потужності сигналу (в даному випадку електромагнітного витоку) в діапазоні (у смузі) частот відповідного джерела витоку інформації (системні блоки, монітори, клавіатура, магнітні диски тощо) та $P_ш$ — потужності адитивної суміші спеціальних шумів (шумів, які в даному 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 ТКМ підприємства.*

Захист інформації від електричних витоків (за рахунок нерівномірності споживання струму), паразитної генерації тощо, слід забезпечувати спеціальними елементами захисту інформації ТКМ від витоку технічними каналами та спеціального впливу на неї (мережні та інші фільтри, надійне заземлення та т. ін.) Склад цих засобів, їхніх компонентів, механізмів, функцій та їхні необхідні характеристики (внесені затухання в робочому діапазоні частот — коефіцієнти ослаблення сигналів витоку) визначаються або їхніми паспортними даними, або на підставі обстеження відповідних джерел витоку інформації з урахуванням вимог Плану ТЗІ та політики безпеки організації, як складової Плану ТЗІ.

Методики визначення умовної імовірності подолання порушником засобів захисту від електричних витоків $q_{ев}$, $q_{пв}$, $q_{мк}$ та відповідних вихідних даних не відрізняється від вище наведеної методики щодо визначення умовної імовірності подолання порушником засобів захисту від електромагнітних витоків

Шукана ймовірність подолання порушником засобів захисту від порушення конфіденційності інформації за рахунок приймання витоків інформації технічними каналами визначається як:

$$q_{зв} = P_{емв} \cdot q_{емв} + P_{ев} \cdot q_{ев} + P_{пв} \cdot q_{пв} + P_{мк} \cdot q_{мк}.$$

Приклад. 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 $h^2 = (0{,}54;\ 1{,}41;\ 3{,}24;\ 22)$.

h^2	$h^2/2$	$\Phi_0^{-1} = \alpha = \sqrt{h^2/2}$	Φ_0	$P_{сп}$	$q_{зв}$
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

В останньому рядку таблиці наведено результати з використанням виразу (3).

Приклад. Нехай на підставі обстеження приміщення та засобів ТКМ, яка розташована в даному приміщенні установлено, що максимальне значення напруженості електромагнітного поля витоків елементами ПЕОМ у діапазоні частот 40–1000 МГц складає близько 950 мкВ/м, а значення напруженості електромагнітного поля генератора шуму є таким, що відношення енергетик шум/сигнал $h^2 = 25$. Тоді, на підставі виразу (3), отримаємо: $q_{емв} = 0{,}5\exp(-6{,}25) = 9{,}6\cdot10^{-4}$.

Значення співвідношення сигнал/шум на виході відповідних засобів захисту дорівнює практично коефіцієнту ослаблення сигналів витоку даного засобу.

Приклад. З урахуванням наведених вище прикладів і виразу

$$q_{зв} = P_{емв} \cdot q_{емв} + P_{ев} \cdot q_{ев} + P_{пв} \cdot q_{пв} + P_{мк} \cdot q_{мк}$$

отримаємо, що

$$q_{зв} = 9{,}6\cdot10^{-4}.$$

Визначення ймовірності подолання засобів фільтрації зовнішніх (віддалених) загроз конфіденційності із телекомунікаційних мереж

Імовірності подолання порушником (відповідною віддаленою загрозою) засобів фільтрації зовнішніх (віддалених) загроз конфіденційності з телекомунікаційних мереж $q_{кткм}$ визначаються характеристиками засобів і протоколів внутрішньо- та зовнішньомережного обмінів на транспортному, мережному та канальному рівнях семирівневої моделі взаємодії відкритих систем OSI. Для відокремлених ТКМ підприємства величину цієї ймовірності слід прийняти $q_{кткм} = 0$.

Визначення ймовірності подолання засобів антивірусного захисту

Імовірності подолання порушником (відповідною загрозою) засобів антивірусного захисту $q_{ав}$ можна визначити, знаючи, приміром, співвідношення між кількістю вірусів, занесених у базу засобів антивірусного захисту, та загальною кількістю існуючих, точніше відомих на час оцінки, вірусів. Наприклад, якщо кількість вірусів, які занесені до бази засобів антивірусного захисту, дорівнює $N_{вз}$, а загальна кількість відомих вірусів — $N_{вв}$, то величину $q_{ав}$ можна визначити з виразу:

$$q_{ав} = 1 - N_{вз}/ N_{вв}.$$

Приклад. Якщо кількість вірусів, які занесені до бази Norton Antivirus, складає 68 092 вірусів, а в базі даних Антивірус Касперського їх 98 987, то можна вважати, що при використанні першого із цих засобів $q_{ав} \approx 1{,}5\cdot10^{-5}$, а другого — 10^{-5}.

Приклад. Визначимо ймовірність порушення конфіденційності $q_{пк}$:

$$q_{пк} = q_{кзі}\cdot[1 - (1 - q_1)\cdot(1 - q_{зв})\cdot(1- q_{ав1})].$$

Для даних, які визначено у вищенаведених прикладах:

$$q_{кзі} = \{0;\ 2^{-256} = 10^{-77}\},$$

$$q_1 = 10^{-22},\ q_{зв} = 9{,}6\cdot10^{-4},\ q_{ав1} = 10^{-5}.$$

Тоді, у разі відсутності засобів криптографічного перетворення ($q_{кзі} = 1$) або використанні авторизованими користувачами режимів читання чи модифікації відносно інформаційних об'єктів

$$q_{пк} = (q_1 + q_{зв} + q_{ав}) \approx 10^{-5},$$

а при використанні засобів криптографічного перетворення ($q_{кзі} = 10^{-77}$) і використанні відносно інформаційних об'єктів режимів зберігання чи передачі лініями зв'язку:

$$q_{пк} = 10^{-77} \cdot (q_1 + q_{зв} + q_{ав}) \approx 10^{-82}.$$

Висновок

Для оцінки ступені забезпечення конфіденційності інформаційних об'єктів телекомунікаційних мереж при використанні відповідних систем захисту інформації у роботі запропоновано підходи та математичні моделі щодо оцінок і визначення ймовірностей подолання порушниками складових застосованих систем захисту конфіденційності.

1. Типове положення про службу захисту інформації в автоматизованій системі (НД ТЗІ 1.4-001-2000).

2. Василенко В.С., Матов О.Я. Методика оцінки загроз ресурсам інформаційних систем. *Інформаційні технології та спеціальна безпека*. 2015. № 1. С. 35–50.

3. Василенко В.С., Матов О.Я. Алгоритми кодування інформаційних об'єктів в коді умовних лишків. *Реєстрація, зберігання і оброб. даних*. 2015. Т. 17. № 1. С. 99–107.

4. Матов А.Я., Василенко В.С., Дубчак О.В. Целостность и доступность информационных объектов. ISBN 1561-6886. Современный научный вестник «Руснаучкнига». Белгород: *Научно-теоретический и практический журнал*. 2013. № 50(189). С. 69−74.

5. Бунин С.Г., Войтер А.П. Вычислительные сети с пакетной радиосвязью. Київ: Техніка, 1989. 223 с.

6. Бронштейн И.Н., Семендяев К.А. Справочник по математике для инженеров и учащихся ВТУЗов. Москва: Наука, 1981.

7. Абенгауз Г.Г. и др. Справочник по вероятностным расчетам. Москва: Воениздат МО, 1970.

Надійшла до редакції 06.11.2017