УДК 007.52

А.О. Петров

СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ ЗАГАЛЬНОГО КОРИСТУВАННЯ

Розглянуто питання розробки системи захисту інформації в мережах загального користування.

Ключові слова: *захист інформації, система, мережі загального користування, конфіденційні дані.*

Рассмотрены вопросы разработки системы защиты информации в сетях общего пользования.

Ключевые слова: *защита информации, система, сети общего пользования.*

Questions of the development of information security system in public networks are considered.

Keywords: *information security, system, public networks.*

В епоху глобалізації процесів життєдіяльності сучасного суспільства, коли інформаційні канали стали невід'ємною системоутворюючою частиною діяльності людства, усе більшої актуальності набуває завдання передачі величезних інформаційних потоків та забезпечення конфіденційності передаваної інформації, а також розмежування прав доступу до неї. В якості основних інформаційних каналів використовуються мережі загального користування, підключитися до яких теоретично може кожний.

На суспільному та державному рівнях все більш значимим і суттєвим фактором, що безпосередньо впливає на розвиток науки, економіки, внутрішньої та зовнішньої діяльності держави, стає інформаційний ресурс, властивостями якого є розподіленість та динамічність.

Високий темп зростання структур інформаційних зв'язків забезпечив стрімке зростання швидкості обігу інформації і спроектував життєдіяльність людства на мережеву інфраструктуру. Величезний потенціал розвитку цих технологій породив загрозу для безпеки інформації – складну науково-практичну проблему, яка призводить до складних соціальних наслідків. У цій ситуації найважливішим завданням стає ор-ганізація швидкого, надійного та захищеного зв'язку в мережах загального користування (МЗК).

Розвиток засобів зняття інформації, технічних засобів розвідки в тому числі, обумовлює зростання погроз несанкціонованого доступу, порушення цілісності, доступності інформаційних ресурсів. У зв'язку з високою ресурсомісткістю захищених каналів зв'язку і неухильно зростаючою потребою в передачі інформації з обмеженим доступом відкритими каналами, усе гостріше постає проблема передачі конфіденційних даних по МЗК. Отже, набуває актуальності моделювання та розробка методів захисту інформації в МЗК [1].

Стратегія технічного захисту інформації в захищених інформаційно-телекомунікаційних системах повинна бути комплексною. Її головною метою має стати виключення можливості або зменшення ефективності просочування інформації з обмеженим доступом і забезпечення її цілісності.

Основу стратегії при реалізації циклу регулярних робіт із захисту інформації в телекомунікаційній системі (ТС) складають наступні базові принципи:

– безперервний збір інформації про функціонування систем і засобів захисту і про роботи, що проводяться. Для цього необхідно здійснювати постійний моніторинг і спостереження за захистом;

– систематичний аналіз стану захищеності інформації з обмеженим доступом;

– систематичне уточнення вимог до захисту інформації;

– проведення базового циклу робіт із захисту в разі незадовільного стану захищеності або зміни вимог до захисту.

Як базові компоненти стратегії ЗІ в МЗК рекомендується розглядати: об'єкти ТЗІ, погрози безпеці, моделі порушника, політику безпеки, моделі ТЗІ, використовувані засоби ТЗІ і стійкість (гарантії ТЗІ).

Як свідчить статистика, найбільші втрати завдаються легальними користувачами, проти яких усі попередні заходи є неефективними.

Невід'ємним компонетом, який завершує опис предметної області ЗІ у МЗК, є вимоги до побудови та комплектування механізмів захисту в єдину систему:

– індуктивна модель безпеки – система, одного разу встановлена в безпечний стан, не повинна змінювати свого стану в процесі функціонування;

– вимоги до експлуатації каналу, що захищається, зв'язки, виконання яких забезпечує неможливість зміни умов застосування системи захисту;

– формалізовані вимоги і параметри оцінки якості проведення тестування засобу захисту;

– коректно визначені умови застосування системи захисту (погрози, як такі, тут не враховуються), на підставі яких формулюються й обґрунтовуються вимоги до необхідного набору механізмів захисту.

Для оптимального вибору варіанту комплексної системи захисту інформації (КСЗІ) в МЗК необхідно ввести критерії оцінки ефективності системи захисту інформації (СЗІ). З-поміж різноманітних оцінок основними представляються наступні:

– вірогідність реалізації загрози;

– оцінка можливих втрат (у вартісному вираженні);

– оцінка вартості можливих заходів щодо недопущення реалізації погроз.

Методика синтезу повинна спиратися на стабільні показники. Тому за основу можна прийняти укрупнені структурні й мережеві моделі інформаційної системи, погроз і захистів, які не залежать від конкретної реалізації системи (рис. 1).

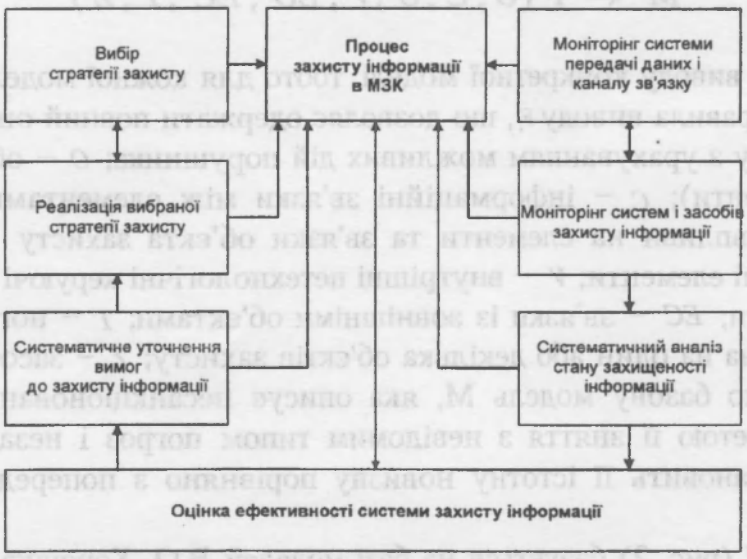

Рис.1. Системно-концептуальна схема захисту інформації в МЗК

У процесі створення підсистеми інформаційної безпеки та її експлуатації вимоги корегуються й конкретизуються так, що завдання не втрачає актуальності в наступні періоди життєвого циклу, як системи в цілому, так і її частини – підсистеми інформаційної безпеки.

Комплексна узагальнена математична модель захисту інформації в мережах загального користування

Комплексна узагальнена математична модель захисту інформації в мережах загального користування ґрунтується на основі об'єкта захисту інформації, багаторівневої моделі засобів нападу, багаторівневої системи засобів захисту [2].

Розглянемо формальне представлення комплексної моделі захисту інформації в мережах загального користування.

Завдання створення моделі комплексної системи захисту інформації має наступні специфічні особливості:

– невизначені й неповні відомості про склад інформаційної системи й характерні погрози;

– багатокритеріальність завдання, пов'язана з необхідністю обліку великої кількості приватних показників СЗІ.

Така модель інформаційної безпеки повинна мати наступні властивості: компактність; універсальність; комплексність; адаптивність.

Також структура моделі повинна дозволяти:

– можливість установлювати рівні захисту;

– здійснювати контроль над станом СЗІ;

– оперативно реагувати на зміни умов функціонування.

У якості загальної моделі формального опису системи захисту запропоновано модель системи безпеки з повним перекриттям.

Модель системи захисту M складається з безлічі "реалізованих" погроз – небезпек $\{m\}$, які повинні виводитися з опису складу системи захисту:

$$M \leftarrow F(O, C, U, V, EO, EC, T, Z) \qquad (1),$$

де F – правила виводу конкретної моделі, тобто для кожної моделі M_i повинні існувати свої правила виводу F_i, що дозволяє одержати повний опис конкретної системи захисту з урахуванням можливих дій порушника; O – об'єкти захисту (та його елементи); C – інформаційні зв'язки між елементами об'єкта; U – можливі різні впливи на елементи та зв'язки об'єкта захисту (вразливості), неконтрольовані елементи; V – внутрішні нетехнологічні керуючі впливи; EO – зовнішні об'єкти; EC – зв'язки із зовнішніми об'єктами; T – погрози, кожна з яких спрямована на один або декілька об'єктів захисту; Z – засоби захисту.

Розроблено базову модель М, яка описує несанкціонований доступ до інформації з метою її зняття з невідомим типом погроз і незаданим рівнем захисту, що становить її істотну новизну порівняно з попередніми моделями [3].

Модель М (рис. 2) базується на базі моделей В.О. Хорошка.

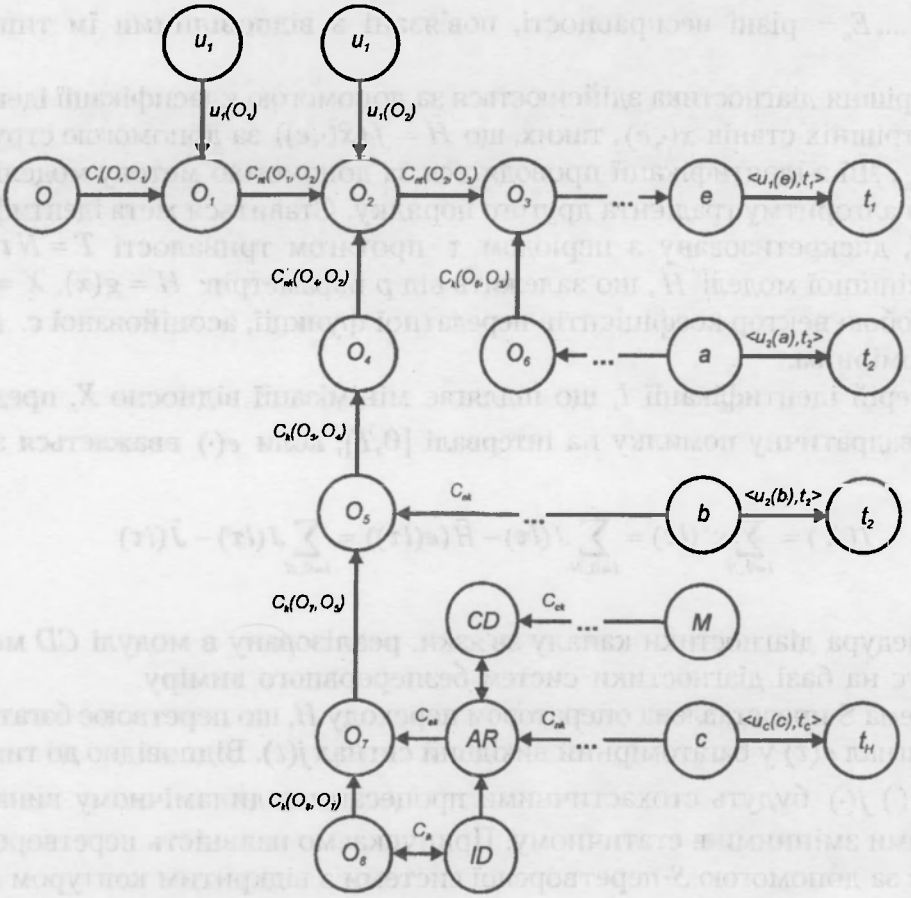

Рис. 2. Структура моделі М. Підвищена ефективність захисту забезпечується компонентами внутрішньої діагностики та діагностики каналу зв'язку

Позначення на рис. 2: $\{O_j\}$ – об'єкти захисту; $\{t_j\}$ – набір погроз; $\{C_{ij}\}$ – набір інформаційних зв'язків; $\{U_{ij}\}$ – набір вразливостей об'єктів і зв'язків; $\{C_k\}$ – набір керуючих зв'язків; a, b, e – незахищені об'єкти; t_n – погрози невідомих типів; AR – контур адаптивного керування захистом; C_{ak} – адаптивний керуючий зв'язок, ID – модуль внутрішньої діагностики; CD – модуль діагностики каналу зв'язку, C_{ik} – діагностичний зв'язок між ID і СЗІ, $C_{ск}$ – зв'язок, що надає інформацію про стан каналу зв'язку для СЗІ за допомогою модуля *CD*, М – СПД.

Однак у структуру моделі М вводяться: спеціальний модуль внутрішньої діагностики, що здійснює діагностику всієї системи захисту, ухвалюючи розв'язку про корегування алгоритму поведінки СЗІ, що дозволить досягти стійкості до відмов СЗІ; спеціальний модуль, що діагностує канал зв'язку з наступною зміною рівня захищеності, що дозволить досягти адаптивності СЗІ.

Внаслідок введення в модель двох компонент виникають нові технологічні зв'язки: C_{ik} – діагностичний зв'язок між *ID* та СЗІ, C_{ck} – зв'язок, який передає інформацію про канал зв'язку для СЗІ за допомогою модуля *CD*.

Алгоритм модуля внутрішньої діагностики СЗІ (*ID*) функціонує наступним чином.

1. Залежно від зовнішніх факторов система буде приймати стани: E_0 – справна робота системи *S*;

2. $E_1,..,E_n$ – різні несправності, пов'язані з відповідними їм типами погроз.

Внутрішня діагностика здійснюється за допомогою класифікації ідентифікованих внутрішніх станів $x(\cdot,e)$, таких, що $\hat{H} = f(\hat{x}(\cdot,e))$ за допомогою структурної відстані d_x. Дії з ідентифікації проводяться за допомогою методу моделі з використанням алгоритму градієнта другого порядку. Ставиться мета ідентифікувати систему S, дискретизовану з періодом τ протягом тривалості $T = N\tau$, за допомогою лінійної моделі H, що залежить від p параметрів: $H = g(x)$, $X = [x_1...x_p]$; X являє собою вектор коефіцієнтів передатної функції, асоційованої с. $\hat{H}$ Вихід $J(\cdot)$ є одномірним.

Критерій ідентифікації I, що підлягає мінімізації відносно X, представляє середньоквадратичну помилку на інтервалі $[0,T]$, коли $e(\cdot)$ вважається заданим:

$$I(X) = \sum_{l=0,N} \varepsilon^2(l\tau) = \sum_{l=0,N} J(l\tau) - \hat{H}(e(l\tau)) = \sum_{l=0,N} J(l\tau) - \hat{J}(l\tau) \qquad (2).$$

Процедура діагностики каналу зв'язки, реалізовану в модулі *CD* моделі M, функціонує на базі діагностики систем безперервного виміру.

Система S представлена оператором переходу H, що перетвоює багатомірний вхідний сигнал $e(t)$ у багатомірний вихідний сигнал $j(t)$. Відповідно до тимчасової функції, $e(\cdot)$ $j(\cdot)$ будуть стохастичними процесами в динамічному випадку або випадковими змінними в статичному. Припускаємо наявність перетворення, що дає її опис за допомогою S-перетвореної системи з відкритим контуром (рис. 3).

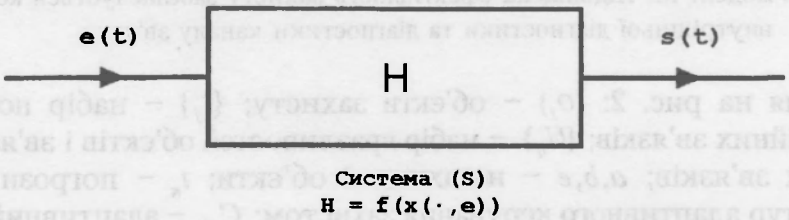

Рис. 3. Система з відкритим контуром

Важливою умовою є те, що вхідний сигнал $e(t)$ і вихідний сигнал $j(t)$ доступні для спостереження та вимірів у будь-який момент години за допомогою відповідних датчиків.

Система S буде характеризуватися погіршенням працездатності $E_C, c = 0,...,(c-1)$, якщо (і тільки якщо) її вхід $e(\cdot)$ і відповідний вихід $j(\cdot)$ одночасно задовольняють: $d_e(e,e_c) = 0$ і $d_j(j,j_c) = 0$.

Стан E_0 представляється сигнатурою $(e_O(), j_O())$.

Система S буде вважатися несправною, (зниження рівня захищеності каналу), якщо:

$$d_x(x(\cdot,e),x(\cdot,e_c)) = 0.$$

Внутрішня діагностика використовує $(e(\cdot), j(\cdot))$ для спостереження, вимірювання або оцінки параметрів, що характеризують внутрішній стан системи:

$$S(\cdot) = H(e(\cdot)),\ H = f(x(\cdot, e)) \qquad (3).$$

Адаптивна діагностика: діагностика головним чином може здійснюватися на будь-який момент часу $t > 0$ в тому розумінні, що головною турботою є детектування різких змін внутрішнього стану системи S або погіршення працездатності, що перевищують установлені пороги; дані яких необхідно зареєструвати для класифікації несправностей у момент часу $t \geq 0, \in \{(e(\tau), j(\tau)), \tau \in [0,T]\}$.

Таким чином, логічним є введення до складу СЗІ в МЗК двох компонент: самодіагностики й контролю стану середовища каналу передачі даних. На підставі отриманих діагностичних даних система передачі скорегує параметри захисту (шифрування, зашумлення та ін.), внаслідок чого виникає безперервний процес самодіагностики з наступною зміною характеристик працюючої системи, без її зупинки.

Були отримані наступні наукові результати:

1. Проведений аналіз побудови систем захисту інформації в мережах загального користування засвідчив незадовільний рівень існуючих засобів захисту в цій області, а також виявив низку проблем у їх проектуванні. Виявлено ряд факторів, що негативно впливають на ступінь захищеності МЗК у результаті об'єднання телекомунікаційних систем за допомогою мереж загального користування, що складаються із сегментів різних фізичних стандартів:

– велика кількість використовуваних стандартів і протоколів при обміні інформацією всередині мереж загального користування;

– складності при організації керування розподіленими телекомунікаційними мережами при використанні віртуальних приватних мереж;

– незастосовність існуючих методів захисту інформації до деяких окремих випадків (у цьому контексті окремим випадком є мережа загального користування).

2. Сформульовано стратегію захисту інформації в МЗК. Основною метою реалізації стратегії ТЗІ в МЗК є збереження властивостей інформації, що захищається, у такому стані, який забезпечує найбільш успішну реалізацію політики безпеки та прозору передачу даних за допомогою МЗК.

3. Розроблено модель ймовірних погроз і захисту інформації в МЗК, що містить у собі модель ймовірного порушника, модель об'єкта захисту, засобу захисту, а також можливі активні та пасивні канали витоку інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Петров А.А.* Оценка эффективности комплексной системы защиты информации в сетях общего пользования / А.А. Петров, В.А. Хорошко // Збірник наукових праць Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2009. – Вип. № 21. – С. 128–131.

2. *Петров А.А.* Методы защиты информации в сетях общего пользования / А.А. Петров // Вісник СНУ ім. В. Даля. – 2008. – № 126. – С. 81–86.

3. *Петров А.А.* Модель вероятностных угроз и защиты информации в сетях общего пользования / А.А. Петров // Безпека та захист інформації в інформаційних і телекомунікаційних системах: міжнар. наук.-практ. конф., 28–29 травня 2008 р: тези допов. – Харків: 2008. – С. 19–20.

Отримано 12.04.2011