УДК 004.7.052:004.414.2

Моденов С. Ю., аспірант (Тел.: +380 (93)600 85 39. E-mail: modenovs@mail.ru)
(Національний авіаційний університет, м. Київ)

РОЗПІЗНАВАННЯ ЗАГРОЗ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИМ МЕРЕЖАМ ЯК ОБ'ЄКТАМ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ

Моденов С. Ю. Розпізнавання загроз інформаційно-комунікаційним мережам як об'єктам несанкціонованого втручання. У статті розглянуті методи розпізнавання фізичних та інформаційних загроз інформаційно-комунікаційним системам. Проаналізовано класифікації основних видів загроз та наслідків здійснення тих чи інших загроз. Розглянуті умови, при виконанні яких можна вважати ознаки різних класів загроз некорельованими. Запропоновано відповідні методи перетворення сигналів як носіїв інформації про ознаки загроз та показано, що після таких перетворень має місце декореляція ознак. Завдяки декореляції ознак загроз спрощується структура пристроїв виявлення та розпізнавання загроз.

Ключові слова: інформаційно-комунікаційна мережа, несанкціоноване втручання, ознаки загроз, кореляція ознак, декореляція ознак

Модэнов С. Ю. Распознавание угроз информационно-коммуникационным сетям как объектам несанкционированного вмешательства. В статье рассмотрены методы распознавания физических и информационных угроз информационно-коммуникационным системам. Проанализированы классификации основных видов угроз и последствий осуществления тех или других угроз. Рассмотрены условия, при выполнении которых можно считать признаки разных классов угроз некоррелируемыми. Предложены соответствующие методы преобразования сигналов как носителей информации о признаках угроз и показано, что после таких преобразований имеет место декорреляция признаков угроз. Благодаря декорреляции признаков угроз упрощается структура устройств обнаружения и распознавания угроз.

Ключевые слова: информационно коммуникационная сеть, несанкционированное вмешательство, признаки угроз, корреляция признаков, декорреляция признаков

I. Вступ

Спроби несанкціонованого втручання у роботу системи обміну даними можна розділити на дві великих групи:

• фізичні загрози – таємне або явне проникнення зловмисника (зловмисників) на територію об'єкта зв'язку, наприклад, з метою крадіжки матеріальних цінностей;

• інформаційні загрози – несанкціонований доступ зловмисників у роботу транспортної мережі, по якій доставляється комп'ютерний трафік, та/або обслуговуючих інформаційно-управляючих систем (ІУС), наприклад, ІУС сигналізації, синхронізації тощо.

Мережне обладнання комунікаційних систем є вельми дорогим. Проте збитки операторів та провайдерів мережі при невиконанні зобов'язань з подання послуг через відмову, пошкодження або знищення об'єкту мережі, порушення нормального функціонування програмного забезпечення, знищення, модифікацію інформації, що передається, або службової інформації можуть бути взагалі несумірні з вартістю відновлення цього обладнання. Тому актуальність проблеми захисту об'єктів мережі важко переоцінити.

Конвергенція мереж і послуг зв'язку, впровадження у комутаційні вузли і станції, вже функціонуючі в складі мереж загального користування (МЗК), нових технологій і послуг, створення на базі вузлів МЗК віртуальних приватних мереж (*VPN*), відкритість взаємодії інформаційних систем, доступ через вузли МЗК у глобальну мережу Інтернет – усі ці елементи науково-технічного прогресу в телекомунікаціях мають і зворотний бік. Таким зворотним боком є збільшення загроз інформаційній безпеці мереж [1, 2].

Розроблені засоби захисту в основному розраховані на збереження власне інформаційного контенту мереж передачі даних, у той час як практично відсутні подібні рішення, орієнтовані на інфраструктуру МЗК та взагалі транспортних мереж зв'язку [3]. Невід'ємною складовою систем захисту є пристрої виявлення та розпізнавання загроз, селекції їх характерних ознак. Стаття присвячена аналізу статистичних характеристик ознак загроз та пошуку методів спрощення пристроїв розпізнавання загроз.

II. Постановка завдання

На Рис. 1 наведено класифікацію основних видів загроз, а на Рис. 2 – класифікацію наслідків здійснення тих чи інших загроз відповідно.

Рис. 1. Класифікація основних видів загроз

Рис. 2. Класифікація наслідків здійснення тих чи інших загроз

Класифікаційні ознаки повинні дозволити здійснити побудову імовірнісних сценаріїв атак як базу кількісного співвіднесення можливого збитку від нападу з витратами на його запобігання.

Таким чином, класифікаційні ознаки загроз є складовою частиною реалізації системного підходу до забезпечення безпеки мережі. У зв'язку з цим вибір сукупності класифікаційних ознак виробляється на основі наступних принципів:

– категорії класифікаційних ознак повинні корелюватися з класифікацією доступних статистичних даних по можливих типах загроз;

– між окремими категоріями класифікаційних ознак бажано виявити взаємну кореляцію, що могло б дозволити поєднувати різні категорії в одній – класифікаційній;

– об'єкти нападу повинні бути представлені в рамках, можливо, більш простої структури, що допускає незалежний розгляд інформаційної безпеки окремих елементів мережі на основі сценаріїв загроз у виді прогностичних середніх частот типових нападів на кожен елемент;

– ступінь деталізації способів нападу визначається рівнем детальності доступної статистики по цих способах і даними по засобах (методам) захисту від них.

Ефективне впровадження інтегрованих рішень захисту від існуючих та можливих загроз вимагає системного підходу до реалізації проекту. Велика частина проектів фрагменту мережі, окремого вузла або автономного об'єкту починається з етапу уточнення потреб, постановки задачі і пророблення варіантів рішення на системному рівні. Після того, як один з варіантів пройде необхідну експертизу, у тому числі і на економічну спроможність, відбувається перехід до фази реалізації проекту, що складає з робочого проектування, постачання і запуску рішення.

За даними Всесвітнього агентства інформаційної безпеки, на підприємствах промисловості, будівництва, транспорту, зв'язку витрати на безпеку складають від 15% до 30% прибутку (залежно від ступеня ризику бізнесу в даній галузі, стану нормативно-правової бази країни, криміногенної обстановки, рівня життя населення і т.д.). На жаль, ці цифри практично скрізь мають стійку тенденцію до зростання. Якщо 20 років тому було закуплено зарубіжними підприємствами і фірмами технічних засобів безпеки (ТЗБ) на суму приблизно 11,4 млрд. доларів США, то в 2011 році ці закупівлі зросли до 30 млрд. доларів. За даними спеціалізованих друкарських видань, в 2014 році об'єм ринку ТЗБ і охорони в розвинених зарубіжних країнах досягав більше 160 млрд. доларів.

На Рис. 3 представлений приблизний розподіл видів ТЗБ за функціональним призначенням.

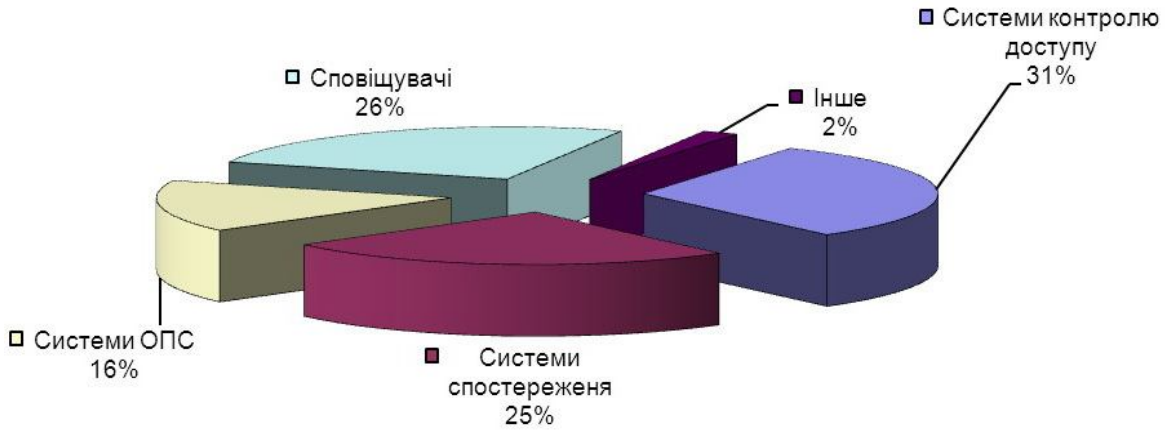

Рис. 3 Приблизний розподіл технічних засобів безпеки

Для досягнення гарантованого рівня безпеки об'єктів, що охороняються, площею до 1..2 км^2, в першу чергу, необхідно забезпечити практично миттєве з необхідною достовірністю сповіщення служби фізичної охорони. Це задача розв'язується за допомогою датчиків охоронно-пожежної сигналізації (ОПС), зовнішніх (периметрових) систем виявлення, зовнішніх і внутрішніх систем телеспостереження. Здійснюючи при цьому раціональний вибір числа і місць розстановки постів (пунктів) фізичної охорони, можна забезпечити

адекватні дії служби охорони за гарантований час і запобігти нанесенню збитку зловмисниками [4].

Якщо об'єкт розташований на відкритій території, на достатньо великому видаленні від центрального офісу, в рішенні проблеми захисту розподілених об'єктів чільну роль виконують як повнота і достовірність інформації про характер подій, так і рівень активного і пасивного захисту. Під активним захистом розуміють фізичну і, якоюсь мірою, психологічну дію на зловмисника: засліплюючі джерела світла, приголомшуючі джерела звуку, пристрої розбризкування незмивної фарби (для полегшення подальшого розшуку зловмисника), пристрої розпилювання штучних туманних утворень, сльозоточивих або погано пахнучих речовин, імітатори вибухових пристроїв (петарди, хлопавки) і т.д. Обов'язковою умовою застосування засобів активного захисту є мінімальна шкода здоров'ю і гарантія відсутності загрози життя зловмиснику.

Досвід роботи охоронних фірм свідчить, що навіть такі прості запобіжні засоби, як написи типу «Об'єкт під охороною», «Небезпечно: сльозоточивий газ», «Небезпечно: висока напруга» і ін. або усне попередження, відтворне при фіксації спроби несанкціонованого проникнення, відлякує до 60%…70% потенційних зловмисників.

Проте, залишаються більше 30% порушників, на яких не діє описані вище заходи. Тоді черговий бар'єр на їх шляху – система пасивного захисту. Це, в першу чергу, посилення конструкції самих об'єктів: міцний суцільнозварний металевий корпус з внутрішніми ребрами жорсткості, бронедвері, обладнані замками підвищеної секретності, замками системи «краб» тощо. Ступінь технічної укріпленості об'єкту повинен бути таким, щоб час, який потрібно для злому зловмиснику з кваліфікацією вище за середню і з напівпрофесійним набором інструментів, був в 2-3 рази більше часу, необхідного для прибуття групи швидкого реагування.

Не менш важливою є вимога оперативності надходження і повноти інформації про стан об'єкту. Виконання цієї умови необхідне для мінімізації як рівня хибних тривог, так і рівня пропусків загроз. Об'єкт повинен бути обладнаний відповідною системою датчиків і пов'язаний з центром прийому і обробки інформації високонадійною системою передачі.

Вважаючи, що ці умови задоволено, розглянемо завдання розпізнавання ознак штатного або екстремального стану роботи мережі.

III. Метод розпізнавання ознак загрози

За наявністю класу об'єктів загрози, що складається з одного елементу, та множини завадових об'єктів задачу розпізнавання можна розглядати як перевірку простої гіпотези проти складної альтернативи. Однак треба враховувати, що об'єкт загрози при своїй активізації може створювати різні корисні сигнали з відповідними ознаками. Деякі сигнали завадових об'єктів також можуть мати декілька ознак, але, як правило, їх кількість значно менше, ніж для об'єкту загрози. До того ж у процесі складання словника ознак доцільно вибирати по одній найбільш характерній (якщо це можливо – унікальній) ознаці для кожного завадового об'єкту.

Для узагальнення методів розпізнавання стану мережі накладемо на ознаки, що формуються, такі обмеження.

1. Ознаки об'єктів різних класів є взаємно некорельованими:

$$\iint_{X_i X_j} x_i\left(t, s_{jk}\right) x_l\left(t, s_{mn}\right) d\, x_i\, dx_j = \begin{cases} \sigma_x^2, \ i = l, \ j = m, k = n, \\ 0, \quad i \neq l. \end{cases} \tag{1}$$

2. Ознаки різних об'єктів одного класу є взаємно некорельованими:

$$\int_{X_i} x_i\left(t, s_{jk}\right) x_i\left(t, s_{mn}\right) dx_i = \begin{cases} \sigma_x^2, \ j = m, k = n, \\ 0, \quad j \neq m \ \text{ and/or } k \neq n\ . \end{cases} \tag{2}$$

3. Різні ознаки одного і того ж об'єкту є взаємно некорельованими:

$$\int_{X_i} x_i\left(t, s_{jk}\right) x_i\left(t, s_{mk}\right) dx_i = \begin{cases} \sigma_x^2, & j = m, \\ 0, & j \neq m. \end{cases} \tag{3}$$

Тут X_i, X_j – гіперпростори i-го та j-го класів відповідно; $x_i\left(t, s_{jk}\right)$ – сигнал i-го класу, що належить k-му об'єкту з j-ю ознакою; σ_x^2 – дисперсія сигналу.

Умови 1 та 2 виконуються за визначенням. Очевидно, що для сигналів різних об'єктів, характеристики яких суттєво відрізняються одна від одної, виділені ознаки будуть взаємно незалежними і, відповідно, некорельованими.

Стосовно ж умови 3, рівняння (3), не можна стверджувати, що вона виконується завжди автоматично. Розглянемо це питання детальніше.

Один і той же об'єкт може проявляти свою активність у різних формах. При цьому створюються сигнали з деяким набором характеристик. Щоб виконати умову (3), необхідно вибирати ознаки з урахуванням цих характеристик.

Наприклад, якщо різні сигнали мають щільності спектрів потужності, які не перекриваються, доцільно вибирати частотні критерії формування ознак. Якщо різні сигнали представляють собою взаємно корельовані випадкові процеси, можна формувати ознаку одного сигналу безпосередньо, а ознаку іншого сигналу формувати з його похідної чи інтегралу. Відомо [5], що випадкова функція та її похідна у співпадаючі моменти часу є взаємно незалежними. Це ствердження можна розповсюдити і на функцію та її інтеграл. Якщо розглядати інтеграл як первинну функцію, то його першообразна буде грати роль похідної. Таким чином, при відповідних перетвореннях сигналів можна задовольнити умові (3).

Якщо умови (1…3) виконуються, кореляційна матриця сформованих ознак прийме діагональний вигляд:

$$E\left[\vec{V}\left(s_i\right)\vec{V}^{T}\left(s_i\right)\right] = \begin{vmatrix} s_1^2 & & & & \\ & s_2^2 & & 0 & \\ & & \cdot & & \\ & & & \cdot & \\ & 0 & & \cdot & \\ & & & & s_M^2 \end{vmatrix}, \tag{4}$$

де

$$\vec{V}\left(s_i\right) = \left\{s_{11}, s_{12}, \ldots, s_{1i}, \ldots, s_{1M1}, s_{01}, s_{02}, \ldots, s_{0j}, \ldots, s_{0M2}\right\}, \quad i = \overline{1, M_1},\ j = \overline{1, M_0},\ M_1 + M_0 = N \tag{5}$$

– вектор еталонних ознак усіх об'єктів – тих, що створюють загрози, і нейтральних (безпечних) об'єктів, які створюють лише завади розпізнаванню.

Тоді оптимальним пристроєм розпізнавання буде просто векторний корелятор, модифікований порівняльно з класичним варіантом [5]. У цьому кореляторі обчислюється кореляційний інтеграл виду

$$q_M = \max_M \int_{t_0}^{t_0+T_H} x\left(t, s\right)\vec{V}\left(s_i\right) dt. \tag{6}$$

Цей векторний корелятор представляє собою набір кореляційних приймачів. На один вхід, загальний для всіх приймачів, подається вхідний сигнал. На другі входи кожного приймача подаються еталонні сигнали, кожен з яких відповідає ознаці (або одній з ознак) окремого об'єкту. Загальне число приймачів відповідно з (5) дорівнює $M_1 + M_0 = N$. Після обчислення усіх кореляційних інтегралів виду (6) кожен вихідний сигнал

кореляційного приймача порівнюється зі своїм пороговим рівнем. З усіх сигналів, які перевищили поріг, робиться вибір вихідного сигналу з максимальним значенням q_M. Приймається рішення про наявність відповідного об'єкту, такого, що представляє загрозу, чи є просто завадою [6, 7].

Якщо ні один з прийнятих сигналів не перевищив свого порогу, приймається рішення про відсутність загроз в зоні дії системи захисту (при використанні критерію прийняття рішення з фіксованим часом спостереження).

Якщо ж застосований метод послідовного аналізу, вихідний сигнал кореляційного приймача порівнюється з двома порогами – нижнім та верхнім, і приймаються відповідні рішення [8].

IV. Висновки

Метод декореляції ознак загрози є універсальним методом, який базується на статистичних властивостях класів ознак суб'єктів. Враховуючи ці властивості та застосовуючи лінійні або нелінійні перетворення сигналів – носіїв інформації про ознаки загрози, можна спростити побудову оптимальних пристроїв розпізнавання суб'єктів загроз інформаційно-комунікаційним мережам.

У подальшому необхідно вирішити наступні задачі:

– обгрунтування технічних і експлуатаційних характеристик пристроїв збору інформації;

– аналіз вимог до систем передачі інформації з урахуванням реальних можливостей комп'ютерних мереж;

– розробка алгоритму аналізу інформації про стан об'єкту і прийняття рішень;

– розробка алгоритмів і програм збору, обробки і реєстрації інформації про всі об'єкти, що знаходяться під контролем.

Література

1. Гольдштейн Б. С. Системный подход к реализации информационной безопасности узлов коммутации / Б. С. Гольдштейн, М. Х. Гончарок, Ю. С. Крюков // Электросвязь. – 2003. – № 4. – С. 11-16.

2. Гольдштейн Б. С. Мониторинг и предотвращение атак сетей ОКС-7 / Б. С. Гольдштейн, И. М. Ехриель, Р. Д. Рерле // Документальная электросвязь. – 2003. – № 11. – С. 23-28.

3. Віноградов М. А. Особливості охорони об'єктів зв'язку категорії Б – лінійне обладнання / М. А. Віноградов, В. В. Коробко, О. П. Скоропаденко, Г. М. Задоя, В. М. Вовк, Т. З. Матвіїв, В. А. Слюсар // Зв'язок. – 2004. – № 4. – С. 38-41.

4. Виноградов Н. А. Методика выбора технических средств безопасности / Н. А. Виноградов, С. С. Родионов // Охранные системы. – 1999. – № 4. – С. 22-24.

5. Ван Трис Г. Теория обнаружения, оценок и модуляции. Т. 1. Теория обнаружения, оценок и линейной модуляции ; пер. с англ. под ред. проф. В. И. Тихонова / Ван Трис Г. – Москва : Советское радио, 1972. – 744 с.

6. Миленький А. В. Классификация сигналов в условиях неопределенности / А. В. Миленький. – Москва : Советское радио, 1975. – 328 с.

7. Леман Э. Проверка статистических гипотез / Э. Леман. – Москва : Наука, 1979. – 408 с.

8. Вальд А. Последовательный анализ / А. Вальд. – Москва : Физматгиз, 1960. – 606 с.

Дата надходження в редакцію: 17.01.2015 р. Рецензент: д.т.н., проф. М. А. Віноградов