УДК 004.056,5.621.396

Юрій Іванович Хлапонін *(канд. техн. наук, с.н.с., доцент кафедри)*

Національний авіаційний університет, Київ, Україна

ЗАСТОСУВАННЯ МЕТОДУ СПЛАЙН-АПРОКСИМАЦІЇ ДЛЯ ДОСЛІДЖЕННЯ ПРОБЛЕМНИХ ЗАДАЧ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ

В статті розглядається застосування методу сплайн-апроксимації для дослідження проблемних задач інформаційної безпеки. Для оцінки захищеності інформації необхідно враховувати та дослідити всі можливі технічні канали витоку інформації. Універсальним методом аналізу таких процесів є метод статистичного моделювання. Суттєвою проблемою є також захист програмного забезпечення мережевих серверів, де виявлення інформаційної загрози носить чітко виражений статистичний характер і розв'язується методами теорії ймовірності і теорії статистичних рішень. Процес захисту інформації розглядається як процес обслуговування потоку вимог до систем захисту інформації, викликаного необхідністю реагування на загрози інформації з метою їх недопущення або знешкодження. Постає необхідність розрахунку імовірності правильного виявлення загроз для інформації. В даному випадку ефективним виявляється метод сплайн-апроксимації емпіричних залежностей, який дозволяє розрахувати дані імовірності.

Ключові слова: *захист інформації; сплайн; сплайн- апроксимація; загроза; нейромережа*.

Вступ

Постановка проблеми та її звязок з важливими науковими завданнями. Процеси проектування, випробування та експлуатації складних радіоелектронних систем пов’язані з обробкою великих масивів інформації про параметри як системи в цілому, так і її вузлів та компонентів. Протягом всього життєвого циклу систем захисту інформації [1] необхідно вирішувати велику кількість оптимізаційних задач. На етапі проектування необхідно оптимально визначити вимоги до системи, обрати елементну базу, забезпечити резервування тощо. На етапі виготовлення необхідно забезпечити умови протікання технологічного процесу з метою максимальної надійності реалізації підсистем, комплектуючих елементів тощо. На етапі випробувань вирішується задача забезпечення якості та надійності шляхом видалення ненадійних вузлів, часткової зміни інформаційних потоків. І нарешті, на етапі експлуатації систем захисту інформації необхідно вирішувати задачі адаптивної оптимізації процесу функціонування і технічного обслуговування з урахуванням післядії, тобто накопиченої статистики попередньої експлуатації системи.

Методологія якісного оцінювання рівня захищеності інформації ґрунтується на результатах вимірювань та експертних оцінках, яким притаманні принципові недоліки, що призводять до низького рівня захищеності інформації.

Більшість цих задач в перекладі на мову математичних моделей зводиться до знаходження умовних і безумовних екстремумів тих чи інших функцій і функціоналів.

Як теоретичні дослідження, так і практика рішення розрахункових задач, переконливо показали ефективність використання в якості універсального обчислювального апарата для рішення цих задач методів сплайн-апроксимації [2].

Аналіз останніх досліджень та публікацій. Для оцінки захищеності інформації експерту необхідно враховувати всі можливі технічні канали витоку інформації, стан відповідного каналу буде відповідати стану захищеності інформації від певного виду загроз.

Мовна інформація з обмеженим доступом (ІзОД), що циркулює на об’єкті інформаційної діяльності (ОІД), вважається захищеною, якщо для кожного з каналів витоку інформації фактичні значення відношень сигнал/завада в октавних смугах частот, отримані за результатами вимірювань в контрольних точках (КТ) не перевищують нормованих показників.

Технічному захисту підлягає інформація з обмеженим доступом, носіями якої є поля і сигнали, що утворюються в результаті роботи технічних засобів пересилання, оброблення, зберігання, відображення інформації (ТЗПІ), а також допоміжних технічних засобів і систем (ДТЗС). Технічний канал витоку вважається захищеним, якщо сигнал не перевищує встановленого нормативною документацією відношення "інформативний сигнал/шум".

Виконавцям таких вимірювань доводиться робити сотні вимірювань, робити математичні обчислення та обробляти статистичні дані. Зважаючи на складнощі математичних моделей, які адекватно відображають встановлення взаємозв'язку процесів і параметрів

електромагнітного випромінювання та акустичних коливань з процесами і параметрами обробки інформації в інформаційно-телекомунікаційних мережах, можливості аналітичного дослідження таких процесів обмежені. Єдиним універсальним методом аналізу таких процесів є метод статистичного моделювання.

Поняття "інформаційна загроза" розглядається як потенційна можливість певним чином порушити інформаційну безпеку, чи ступінь імовірності виникнення такого явища (події), наслідком якого можуть бути небажані впливи на інформацію. Намагання реалізувати загрозу розглядається як атака, а той, хто починає таку спробу, – як зловмисник. Потенційні зловмисники називаються джерелами загрози. Успішність атаки може приводити до втрати інформацією однієї з критичних особливостей (конфіденційності, цілісності чи доступності інформації).

Зазвичай загроза є наслідком наявності вразливих місць у захисті інформаційних систем (таких, наприклад, як можливість доступу сторонніх осіб до критично важливого устаткування або помилки у програмному забезпеченні). Загроза інформації, що циркулює в інформаційній системі, залежить від її структури та конфігурації, технології оброблення інформації в ній, стану навколишнього фізичного середовища, а також дій персоналу.

Суттєвою проблемою є захист програмного забезпечення мережевих серверів, яка тісно пов'язана з завданням забезпечення безпеки інформації в розподілених мережах. Для вдосконалення системи захисту необхідно врахувати механізми реалізації можливих атак. В [3] визначена структура можливих атак в мережі Internet. Щодо Internet-серверу представляють інтерес атаки типу: відмова в обслуговуванні, підміна довіреного об'єкту (суб'єкту) інформаційно-телекомунікаційної системи (ІТС), а також впровадження в ІТС помилкового об'єкту з метою порушення конфіденційності або цілісності інформації, розміщеної на Internet-сервері.

Крім того, значна кількість успішних атак на ресурси ІТС реалізована за допомогою троянських програм та вірусів, створених за допомогою сучасних технологій. Завдання їх виявлення ускладнюється тим, що для кожної операційної системи та ІТС потрібно використовувати власну методику розпізнавання даних шкідливих програм.

В процесі аналізу потоку інформації повинно бути ухвалено рішення про наявність або відсутність загрози в кожному сегменті мережі, що перевіряється. Як сам факт наявності загрози в сегменті мережі, так і її параметри є випадковими. Отже, виявлена загроза носить випадковий характер, і рішення, що приймається при її наявності або відсутності, є статистичним.

Формулювання цілей статті. Проблема виявлення інформаційної загрози, таким чином, носить чітко виражений *статистичний характер* і розв'язується методами теорії ймовірності і теорії статистичних рішень.

Особливо характерне статистичне моделювання в випадках, коли ІТС та її підсистеми описуються моделями теорії масового обслуговування. Так, процес захисту інформації розглядається як процес обслуговування потоку вимог до систем захисту інформації, викликаного необхідністю реагування на загрози інформації з метою їх недопущення або знешкодження. Постає необхідність розрахунку імовірності правильного виявлення загроз для інформації з загального трафіку. В даному випадку ефективним виявляється метод сплайн-апроксимації емпіричних залежностей, який дозволяє розрахувати дані імовірності.

Виклад основного матеріалу дослідження

Яка ж роль сплайнів в статистичному моделюванні?

Це, перш за все, формування вибіркових сукупностей. Базуючись на відомих алгоритмах реалізації випадкових чисел з заданим розподілом, покажемо один зі способів застосування сплайнів до цих алгоритмів.

1. Нехай ω_k - незалежні випадкові числа, рівномірно розподілені в інтервалі (0, 1). Позначимо $F(t)$ будь-яку функцію розподілу випадкової величини, $F^{-1}(x)$ – обернену до неї функцію. Тоді випадкові числа

$$\xi_k = F^{-1}(\omega_k) \qquad (1)$$

незалежні і мають функцію $F(t)$ в якості функції розподілу. Відмітимо, що тут можна замість (1) взяти також відношення

$$\xi_k = F^{-1}(1-\omega_k)\,. \qquad (2)$$

Ми бачимо, що для реалізації даного методу необхідно мати алгоритм обчислення $F^{-1}(t)$, а це часто вкрай складна процедура.

Пропонована нами сплайн-апроксимація працює наступним чином. Розіб'ємо інтервал (0, 1) на n рівних інтервалів

$$D_1 = \left(0, \frac{1}{n}\right),\ D_2 = \left(\frac{1}{n}, \frac{2}{n}\right), \ldots, \quad D_n = \left(\frac{n-1}{n}, 1\right) \qquad (3)$$

і побудуємо сплайн

$$G(x) \approx F^{-1}(x), 0 < x < 1, \qquad (4)$$

з вузлами в точках $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}$. Для обчислення вводимо значення конфіденційності полінома $P_j(x)$, до якого зводиться сплайн в інтервалі $\left(\frac{j-1}{n}, \frac{j}{n}\right)$. Тепер реалізуємо випадкове число ω_k . Якщо ω_k потрапляє в

інтервал D_j, звертаємося до процедури обчислення $P(x)$ і знаходимо

$$\xi = P(\omega). \quad (5)$$

2. У випадку аналітичних складностей з обчисленням зворотоньої функції можна використати сплайн-апроксимацію до щільності

$$f(t) = F(t). \quad (6)$$

Побудований алгоритм сплайн-апроксимації представимо наступною схемою аналітичних перетворень і обчислювальних процедур. Припустимо, що $f(t) = 0$ поза інтервалом $[a, b]$. Розіб'ємо цей інтервал на n частин точками $t, t, \ldots, t$, причому так, щоб всі інтервали $(a, t), (t, t), \ldots, (t, t), (t, b)$ мали імовірність $\frac{1}{n}$.

Далі побудуємо сплайн

$$Q(t) \approx f(t), a \le t \le b. \quad (7)$$

В інтервалі (t, t), де приймається $t = a$, $t = b$, сплайн зводиться до полиному $Q(t)$, коефіцієнти котрого фіксуються як результати обчислень. Позначимо також

$$b = \max_{t \le t \le t} Q(t).$$

Спочатку "кидаємо жереб" з n рівноймовірними наслідками. При j-му випаданні випадкове число ξ (індекс опускаємо) приймає значення в інтервалі (t, t). Для його побудови візьмемо пару незалежних рівномірних в інтервалі (0, 1) випадкових чисел ω і ω.

Якщо

$$\omega < \frac{1}{b} Q\left[t + \omega(t - t)\right], \quad (8)$$

припускаємо

$$\xi = t + \omega(t - t). \quad (9)$$

При протилежній нерівності процедура повторюється з новими значеннями випадкових чисел ω і ω і так далі, поки на якомусь кроці не отримаємо потрібну рівність, тобто реалізацію випадкового числа ξ з щільністю $f(t)$.

Висновки з даного дослідження

За допомогою сплайн-апроксимації можна моделювати уточнені можливі значення результатів вимірювання на ОІД для кожної контрольної точки, в якій проведено визначення октавних рівнів акустичного (вібраційного) сигналів в кожній *i*-й октавній смузі частот та визначити оптимальні значення отриманих рівнів. Зважаючи на те, що виконавцям таких вимірювань доводиться робити сотні вимірювань на ОІД, використання сплайнів може бути корисним для інтерпретації даних моделювання. Так як сплайни враховують гладкість кривої, то, в принципі, можна зекономити на кількості точок параметричного простору, в якому проводиться моделювання, в порівнянні зі звичайною кусочно-лінійною апроксимацією.

Задачі забезпечення доступності інформації в ІТС вирішуються за допомогою систем аналізу захищеності та систем виявлення та запобігання вторгненням (атакам). Системи аналізу захищеності проводять всебічне дослідження контрольованих ресурсів ІТС з метою виявлення "слабких ділянок". Отримані результати є миттєвим знімком стану захищеності в даний момент часу. Очевидно, що сигналом про потенційну можливість атаки є досягнення контрольованими параметрами деяких граничних величин. Одним з основних недоліків таких систем є те, що контроль програмного забезпечення, який проводиться даними системами, часто носить запізнілий характер.

За допомогою сплайн-апроксимації можна моделювати та прогнозувати можливі атаки на ресурси мережевих серверів на основі статистики попередніх спостережень та аналізу трафіку. Оскільки, задачу виявлення атак можна розглядати як задачу розпізнавання образів, то для її рішення застосовуються також нейронні мережі [4, 5]. Для цього функціонування системи, що потребує захисту і взаємодіючих з нею зовнішніх об'єктів представляється в вигляді траєкторій в деякому числовому просторі ознак. В якості методу виявлення зловживань, нейронні мережі навчаються на прикладах атак кожного класу і, в подальшому, застосовуються для розпізнавання приналежності поведінки одному з класів атак. Основна складність в застосуванні нейронних мереж полягає в коректній побудові такого простору ознак, який дозволив би розділити класи атак між собою та відділити їх від нормальної поведінки. Крім того, для класичних нейронних мереж характерне довге навчання, при цьому час навчання залежить від розміру навчальної вибірки.

Суттєво скоротити час навчання нейронної мережі допоможе застосування сплайн-апроксимації простору ознак, що вказують на відхилення від нормальної поведінки системи (наявність атаки чи іншої загрози). Це є темою подальших наукових досліджень автора та буде публікуватися по мірі отримання результатів.

Практичне значення отриманих результатів

Запропоновано новий підхід оцінки рівня захищеності інформації.

Відмінність її від існуючих систем оцінки рівня захищеності заключається в тому, що застосування сплайнів дозволяє скоротити час проведення вимірювань, якщо мова йде про аналіз стану захищеності інформації, яка озвучується або обробляється на об'єкті інформаційної діяльності. За допомогою сплайн-апроксимації можна моделювати та прогнозувати можливі атаки на

ресурси мережевих серверів на основі статистики попередніх спостережень та аналізу трафіку з метою їх недопущення або знешкодження.

Новизна результату

Науковою новизною результату дослідження є:

вперше запропоновано застосування сплайн-апроксимації для моделювання системи оцінки рівня захищеності інформації.

введено поняття імовірності правильного виявлення загроз для інформації.

запропоновано застосування сплайн-апроксимації простору ознак перед обробкою в нейромережній системі.

Література

1. Богуш В. М. Проектування захищених комп'ютерних систем та мереж / В. М. Богуш, О. А. Довидьков // ДУІКТ, – 2006. – С. 5. **2. Корнейчук Н. П.** Сплайны в теории приближения. – М. : Наука, 1984. – 352 с. **3. Лукацкий А. В.** Обнаружение атак. – СПб. : БХВ-Петербург, 2003. – 624 с. **4. Борисов В. В.** Нечеткие модели и сети мережі / В. В. Борисов, В. В. Круглов , А. С. Федулов. – 2 изд. М. : Горячая линия – Телеком, 2012. – 284 с. : ил. **5. Хлапонин Ю. І.** Устройство для обучения распознаванию образов, Авторское свидетельство на изобретение от 16.05.91 № 4944920/24.

ПРИМЕНЕНИЕ МЕТОДА СПЛАЙН-АППРОКСИМАЦИИ ДЛЯ ИССЛЕДОВАНИЯ ПРОБЛЕМНЫХ ЗАДАЧ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

Юрий Иванович Хлапонин ***(канд. техн. наук, с.н.с., доцент кафедры)***

Национальный авиационный университет, Киев, Украина

В статье рассматривается применение метода сплайн-аппроксимации для исследования проблемных задач информационной безопасности. Для оценки защищенности информации необходимо учитывать и исследовать все возможные технические каналы утечки информации. Универсальным методом анализа таких процессов является метод статистического моделирования. Существенной проблемой является также защита программного обеспечения сетевых серверов, где выявление информационной угрозы носит четко выраженный статистический характер и решается методами теории вероятности и теории статистических решений. Процесс защиты информации рассматривается как процесс обслуживания потока требований к системам защиты информации, вызванного необходимостью реагирования на угрозы информации с целью их недопущения или обезвреживания. Возникает необходимость расчета вероятности правильного обнаружения угрозы для информации. В данном случае эффективным оказывается метод сплайн-аппроксимации эмпирических зависимостей, который позволяет рассчитать данные вероятности.

Ключевые слова: *защита информации; сплайн; сплайн-аппроксимация; угроза; нейросеть.*

APPLICATION OF SPLINE APPROXIMATION METHOD FOR STUDYING PROBLEM TASKS OF ASSESSING INFORMATION SECURITY

Yurii I. Khlaponin ***(Candidate of Military Sciences, Senior Research Fellow, Associate Professor of a Department)***

National Aviation University, Kyiv, Ukraine

The use of spline approximation method for studying the information security problem tasks is considered in the article. The all possible technical channels of information leakage must be considered and researched for assessing information security. The universal analysis method of such processes is the method of statistical modeling. The critical problem is also software protection of network servers, where information threat detection is clearly statistical defined and it is solved by methods of probability theory and statistical decision theory. The information security process is considered as a service process of requirements flow for information security systems, caused by necessity of respond to information threats for the purpose of their prevention or neutralization. The necessity of calculating the correct threat detection probability for information is becoming. The method of spline approximation of empirical relationships is effective in this case. This method allows calculating probabilities data.

Keywords: *information security; spline; spline approximation; threat; neural network.*

References

1. Bohush V. M., Dovydykov O. A., (2006), Planning secure computer systems and networks, [*Proektuvannia zakhyshchenykh kompiuternykh system ta merezh*], DUIKT, p. 5. **2. Korneichuk N. P.** (1984), Splines in approximation theory, [*Splaynyi v teorii priblizheniya*], M. : Nauka,. p. 352. **3. Lukatskyi A. V.**, (2003), Attack detection, [*Obnaruzhenie atak*], SPb. BHV-Peterburg, p. 624. **4. Borisov V. V.**, Kruglov V. V., Fedulov A. S., (2012), Indistinct models and networks, [*Nechetkie modeli i seti*], 2 izd. M. : Goryachaya liniya – Telekom, p. 284. **5. Hlaponin Yu. I.**, Device for Pattern Recognition Learning, [*Ustroystvo dlya obucheniya raspoznavaniyu obrazov*] Inventor's certificate of 16.05.91 № 4944920/24.

Отримано: 8.10.2014 р.