УДК 004.9

д.т.н., проф. Дудикевич В.Б., Стеренчук В.М.,
к.т.н. Ракобовчук Л.М., (НУ «ЛП», Україна)

СИНТЕЗ МАТЕМАТИЧНОЇ МОДЕЛІ ПРОГНОЗУВАННЯ ДЛЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Вступ

В сучасних умовах управління ризиками в системах захисту інформації (СЗІ) пов`язане з обробкою і аналізом великих обсягів даних. Для ефективної підтримки прийняття рішень можуть використовуватись інструментальні програмні засоби аналізу,моделювання та прогнозування.

В цілому, область застосування таких засобів може бути різною, в залежності від задач, які ставляться – від простих недовготривалих прогнозів, побудованих на основних показниках, до складних систем моніторингу та аналізу, які охоплюють тисячі документів за різними напрямками діяльності.

Оцінка параметрів СЗІ в умовах високої невизначеності умов її функціонування повинна будуватись з використання не однієї математичної моделі, а цілих груп, які побудовані ієрархічно, що дає змогу їм вдосконалюватись на основі оптимального набору вихідних даних.

При синтезі оптимальних математичних моделей для СЗІ вихідними повинні бути наступні два етапи:

- вибір математично продуктивного критерію оптимальності у відповідності з архітектурою системи захисту і технології обробки інформації в інформаційних системах (ІС);
- чітке формулювання математичної задачі, яка б враховувала всі апріорні дані, а також могла б знайти рішення у відповідності з заданими критеріями.

Складність дослідження питань захисту інформації в СЗІ полягає у великій невизначеності умов функціонування ІС. Постановка задач захисту інформації у ІС не в кожному випадку є ефективною,оскільки формується в умовах непередбачуваної поведінки СЗІ,а часто і у екстремальних умовах.

Відомі математичні моделі, використані для опису структури та поведінки СЗІ, при некоректно поставленій задачі не дають бажаного результату. Саме тому існує необхідність розробки нових, орієнтованих на специфіку роботи СЗІ методів та процесів моделювання, які б вирішували задачу нормального функціонування системи, не доводячи її до аварійного стану.

Для отримання інформації про стан СЗІ необхідно виділити певні групи параметрів і визначити інтервали перевірки їх значень. При цьому,слід звернути увагу на особливо важливі аспекти з точки зору реалізації нормального функціонування СЗІ.

В роботі [1] висловлена думка, що особливості аналізу СЗІ роблять неможливим застосування традиційних математичних підходів, в тому числі методів математичної статистики і теорії імовірності, однак, це не зовсім так.

Сьогодні у зв'язку з розвитком теорії стохастичних фракталів стає популярною така характеристика тимчасових рядів, як показник Херста (Н) [2, 3]. Існують різні способи визначення фрактальних розмірностей, до числа яких відноситься R/S-спосіб, на підставі якого визначається показник Херста. Цей показник має широке застосування в аналізі тимчасових рядів завдяки своїй стійкості. Тобто, при його розрахунку використовуються мінімальні припущення про досліджувану систему, класифікуються тимчасові ряди, завдяки чому, з`являється можливість відрізнити випадковий ряд від невипадкового, навіть якщо випадковий ряд не гаусовський (тобто не нормально розподілений).

Метою дослідження було доказати доцільність використання показника Херста, який включає в себе елементарні математичні операції для синтезу прогнозу поведінки СЗІ.

Прогнозно-аналітичні дослідження

Для дослідження взята вибірка спам-повідомлень за період з 01.12.2008 по 18.06.2009 (поштова скринька на сайті інтернет - провайдера litech.net). Подобова кількість вхідних повідомлень наведена на рис. 1.

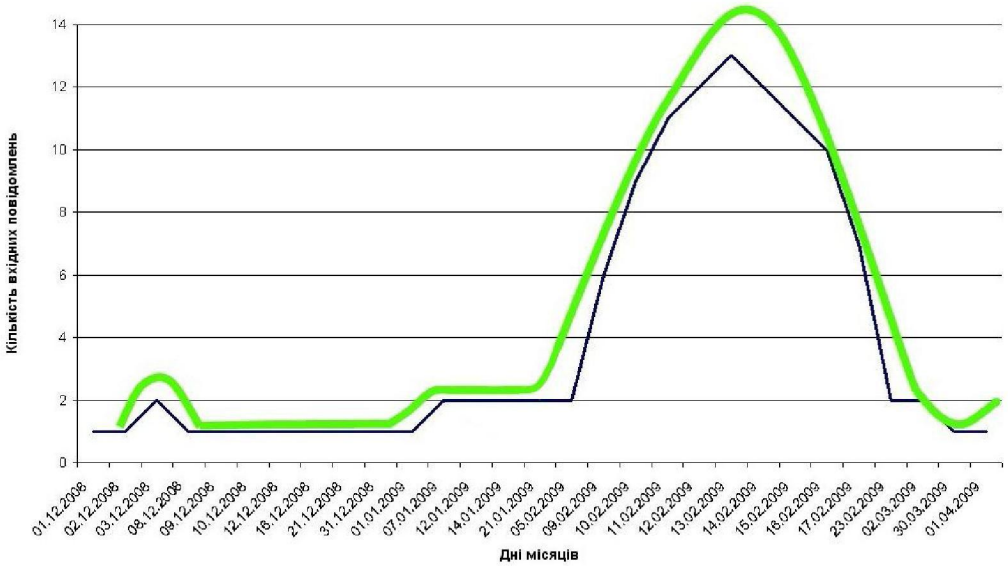

Рис. 1. Графік залежності кількості вхідних повідомлень

Стрибок припадає на період з 05.02.2009 по 23.02.2009 , який і був розглянутий детальніше.

Для наочності складу спам – повідомлень на рис.2 приведений їх розподіл, відповідно до параметрів (мова,тип,розмір).

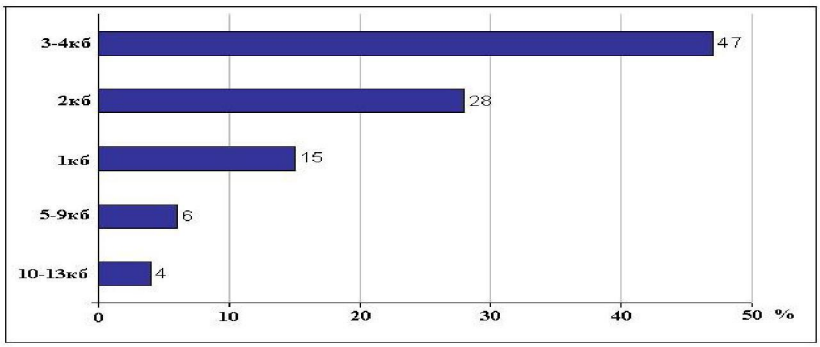

Рис. 2. Розмір спам-повідомлень

Показник Херста розраховували за методикою [3], після чого була визначена динаміку зміни процесу.

Показник Херста (H) для тимчасових рядів:

$$R/S = (N/2)^H \qquad (1)$$

де R/S - коефіцієнт нормованого розмаху; R – «розмах» тимчасового ряду; S - стандартне відхилення.

Середньоарифметичне значення ряду N:

$$< \xi >_{сер} = \frac{1}{N}\sum_{t=1}^{N}\xi_t = 3,68 пов. \qquad (2)$$

Відхилення ряду від середнього значення:

$$X(t,N)=\sum_{u=1}^{t}(\xi_u - M_N)=\sum_{u=1}^{t}\xi_u - t\cdot M_N \qquad (3)$$

де N період, який змінюється від 2 до довжини ряду; t – змінна, яка змінюється від 1 до N-1; M_N - середнє арифметичне значення N елементів ряду; u – конкретний елемент ряду.

Прорахована динаміка накопичення відхилення ряду X(t,N) за виразом:

$$R=\max X(t,N)-\min X(t,N)=12.16 \qquad (4)$$

При чому, середньоквадратичне відхилення складало:

$$S=\sqrt{\frac{1}{N}\sum_{t=1}^{N}(\xi(t)-<\xi>_{\text{ñåð}})^2}=4{,}37 \qquad (5)$$

Відповідно,показник Херста H для даної вибірки склав: H=0.43.

Значення $H > 0{,}5$ означає, що, спрямована в певний бік динаміка процесу у минулому, найімовірніше, спричинить продовження руху в тому ж напрямі. Якщо $H < 0{,}5$,то прогнозується, що процес змінить спрямованість. $H = 0{,}5$ означає невизначеність [3]. В даному випадку $H < 0{,}5$, тобто динаміка процесу повинна змінити напрям. Прогноз виявився вірним. В період з 7 березня по 18 червня 2009р. спостерігалося різке зниження надходження спаму на дану поштову скриньку. Досліджуючи надходження спаму на e-mail було виявлено, що його інтенсивність і тематика часто залежить від подій які відбулися в конкретній країні і в світі.

Висновки

В результаті дослідження, можна сказати, що застосування такої характеристики як показник Херста дозволяє синтезувати математичні моделі прогнозу поведінки певних СЗІ та визначити динаміку інформаційних потоків, повідомлення з яких відображають процеси, що відбуваються в теперішньому часі.

Розробки систем прогнозування і нових екстраполяційних методів, як показано на прикладі показника Херста, дають можливість моделювати сценарії подій з потрібними тенденціями розвитку. Отже, цей напрямок в галузі інформаційної безпеки є актуальним і перспективним.

Список літератури

1. Домарев В.В. Безопасность информационных технологий. Системный подход: - К.: ООО «ТИД «ДС», 2004. -992 с.

2. Матвієнко А.В. Фрактальні властивості мікрогеометрії оброблених поверхонь. (http://masters.donntu.edu.ua/2007/mech/majeed/library/st%20ua.html)

3. Ландэ Д.В. Элементы фрактального анализа информационных потоков. (http://download.yandex.ru/class/lande/frakt-lecture.pdf)

В даній роботі описано проблематику побудови моделей аналізу та прогнозування поведінки систем захисту інформації, а також запропоновано та приведено приклад використання показника Херста для вирішення цієї задачі. Перевагою даного показника є його обчислення з використанням простих математичних підходів.

Ключові слова: системи захисту інформації, математична модель прогнозування.

В предоставленной работе описана проблематика построения моделей анализа и прогнозирования поведения систем защиты информации, а также предложен и приведен пример использования показателя Херста для решения этой задачи.

Ключевые слова: системы защиты информации, математическая модель прогнозирования.

This work describes problems of construction of analysis models and prognostication of conduct of the informational security systems and also the example of the use of Kherstas index is offered and resulted for the decision to this task. Advantage of this index is his calculation with the use of simple mathematical approaches.

Key words: data security system, mathematical prediction model.

Надійшла 22.12.2009