

**Іван Опірський**

Національний університет «Львівська політехніка»

УДК 004.056:061.68; 004.3.75:061.68

## **ЗАГАЛЬНІ ПРОБЛЕМИ ПРОГНОЗУВАННЯ НСД В ІНФОРМАЦІЙНИХ МЕРЕЖАХ ДЕРЖАВИ**

*Анотація:* Представлено аналіз загальних проблем несанкціонованого доступу в інформаційних системах держави. Проведено аналіз та вирішення задачі екстраполяції випадкового процесу  $X(t)$  з врахуванням даних контролю різними методами. Представлено етапи вирішення задачі прогнозування в автоматизованих системах контролю та приведено методіку рішення проблематики прогнозу.

*Summary:* This paper analyzes common problems unauthorized access to information systems of the state. The analysis and problem solving extrapolation random process  $X(t)$  taking into account the various data control methods. Presented stages of solving the problem of forecasting in automated control systems and methodology given solution perspective projection.

*Ключові слова:* Несанкціонований доступ, інформаційні системи держави, Марківський процес, випадковий процес, прогнозування.

### **I Вступ**

Проблема прогнозування включає в себе низку труднощів, одні з яких власне зв'язані з прогнозуванням, інші характерні для всіх напрямків автоматичного контролю, треті визначають загальні можливості прогнозування і його місце серед інших видів контролю.

Розглянемо дані проблеми.

Прогнозування НСД до інформаційних систем держави (ІСД) без сумніву має ґрунтуватись на вивченні тенденцій, що спостерігаються в зміні її поточного стану під дією НСД. В теорії автоматичного контролю передбачається, що цей стан може бути представлено сукупністю значень деяких контрольних параметрів. Тоді, очевидно, причиною, що викликає зміни стану ІСД, мають бути зміни значень саме цих параметрів. Таким чином прогнозування НСД в ІСД повинно базуватись на прогнозуванні значень складових контрольних параметрів. Це може здійснюватись на базі математичного апарату екстраполяції процесів, що описує закономірності змін в параметрах. В свою чергу використання апарату екстраполяції потребує певної формалізації процесів змін контрольних параметрів, тобто потребує створення певної математичної моделі процесів вимірювання параметрів ІСД під впливом НСД. Кінцевою метою дослідів в цьому напрямку є створення певного алгоритму прогнозу.

Виконання будь-якої форми контролю стану ІСД базується на використанні загальної моделі мережі контролю. Дана модель має дозволити виділяти достатню сукупність контрольованих параметрів для отримання на даному рівні достовірності і для контролю функціонування, і для фокусного контролю, і для діагностичного контролю, і для прогнозованого контролю.

Звичайно, що визначення сукупностей контрольних параметрів для кожного виду контролю буде володіти своєю специфікою, яка залежить від конкретної форми алгоритму відповідного контролю. Так, для контролю функціонування як контрольні параметри як правило не використовують вихідні параметри мережі. Прогнозний контроль потребує визначення спеціальних прогнозних параметрів. Такі параметри мають відрізнятися рядом особливостей [1].

По-перше, вони повинні з відповідною точністю представляти стан контрольованого об'єкту ІСД.

По-друге, вони повинні відображати основні тенденції в змінах мережі.

По-третє, як і всі контрольні параметри, вони повинні допускати зміни з необхідною точністю.

Всі перелічені особливості, як це легко побачити, в той же час є особливостями параметрів якості.

Отже, задача виділення сукупності параметрів, що прогнозуються, може практично збігатися з задачею виділення параметрів якості, і в зв'язку з цим належати до однієї з загальних задач теорії контролю.

### **II Основна частина**

Важливою проблемою щодо підвищення ефективності використання системи контролю НСД є визначення дійсного місця прогнозуючого контролю серед усіх форм контролю. Рішенням цієї проблеми в чималому степені залежить від самої можливості здійснення прогнозу в тих чи інших конкретних умовах застосування в системах та мережах.

Поступові зміни параметрів мережі можуть передбачати можливе несанкціоноване підключення до мережі. Цей висновок, здалось б, повинний означати, що проведення прогнозуючого контролю є доцільним у всіх без винятку випадках, та застосовувати до всіх видів підключення. Однак такий висновок був би надмірно поспішним. Наявна статистика в жодній мірі не стосується питання про те, наскільки передчасні зміни ІСД, що призводять до НСД, могли б бути представлені значеннями тих чи інших контрольних параметрів. Так, наприклад, підключення з компіляцією визначити дуже важко і воно не впливає на зміни параметрів [2].

Таким чином, деяка частина змін характеристик ІСД не може бути віднесена наразі до числа НСД, які можна було б з достатньою вірогідністю передбачити на основі контрольних змін. Кожна ж частина цих змін може бути віднесена до цієї групи. Конкретної відповіді на це питання поки що немає. Але без відповіді на це питання не можна вирішити задачу визначення загальної ефективності прогнозного контролю, яка в певній мірі залежить від відношення інтенсивності прогнозованих НСД.

Але це відношення залежить не тільки від принципової можливості здійснення прогнозу. При складанні загальних алгоритмів контролю реального стану ІСД необхідно розраховувати затрати на проведення тої чи іншої форми контролю з відповідним підвищенням ефективності експлуатації мережі. Це, зокрема, означає існування певного нижнього порогу інтенсивності передбачення НСД, що припадає на одну прогнозовану атаку, для якої ще визначається доцільним проведення прогнозованого контролю. Якщо інтенсивність атак, які можуть контролюватись кожним прогнозним параметром, виявляється нижче цього порогу, то прогноз стає недоцільним.

В той же час прогнозування роботи засобів обчислювальної техніки, яка є основним елементом ІСД, здійснюється своїми методами [3].

Слід очікувати, що прогнозування НСД може бути ефективним для вузлів ІСД з ярко вираженими безперервними властивостями, що містять значне число компонентів, процеси в яких відрізняються сильною взаємообумовленістю.

Як слідує з проведеного аналізу, коло навіть самих важливих запитань, зв'язаних з проблемою прогнозу НСД в ІСД, є достатньо широке. Вичерпне дослідження цих всіх питань навряд чи можна розглянути в одній статті. Тому не всі перелічені проблеми будуть розглянуті в рівній мірі. Більш того, деякі питання взагалі не будуть порушені в даній статті.

Як уже виявлялось, цінність того чи іншого методу прогнозу визначається тим, наскільки повне вірогідне описання випадкових величин  $\Delta T_{II}$  можна отримати з його допомогою. З цієї точки зору найкращими є ті з них, які забезпечують отримання умовного закону розподілу величини  $T_{II}$  (безпосереднє обчислення прогнозного НСД). Найбільш загальним методом в цьому плані є наступний. Нехай випадковий процес  $X(t)$  визначений в дискретних точках  $t_i, i=1, I$  інтервалу  $t_1, t_I$ . Тоді його вичерпною вірогідною характеристикою є  $I$ -мірна щільність розподілу  $f_I(x_1, x_2, \dots, x_i, \dots, x_I)$  випадкових величин  $X(t_i)$ ; при цьому відомості, необхідні для рішення задачі прогнозу, можна задати у вигляді спільної  $(I+1)$ -мірної щільності розподілу значень процесу і залишок часу до атаки  $f_{I+1}(x_1, \dots, x_i, \dots, x_I, \Delta t_n)$ . Нехай тепер в результаті контролю отримано  $k>1$  послідовних значень реалізації процесу  $x_i, i=1, k$ . Не мала умовна щільність розподілення залишку часу життя знаходиться як

$$f_k(\Delta f_n / x_i, i=1, k) = \frac{\int_{-\infty}^{\infty} \dots \int_{-\infty}^{\infty} f_{I+1}(x_1, \dots, x_I, \Delta t_n) dx_{k+1} \dots dx_I}{f_k(x_1, \dots, x_i, \dots, x_k)} \quad (1)$$

Очевидною перевагою даного методу є його універсальність, оскільки крім звичного виконання вимог дискретності опису процесу  $X(t)$  ніяких обмежень не передбачалось. Але настільки очевидним є велика практична важкість реалізації даного методу, наскільки отримання багатомірних щільностей розподілу із статистичних даних і математичні операції з ними є досить складними. Тому практичне застосування методу, яке базується на описанні апріорного процесу багаторівневої функції розподілу, знайдено в найпростіших випадках, зокрема для марковських випадкових процесів, що багатократно описані в літературі [4, 5, 6].

Марковський характер моделі є основним недоліком даного методу, оскільки реальні процеси впливу НСД мають зазвичай відчутний наслідок. Обмеження можливостей методу безпосереднього визначення умовного розподілу залишку часу до атаки приводить до необхідності знову повернутись до вирішення задачі за допомогою систем рівнянь.  $\hat{x}_w(t) - a = 0$  або  $\hat{x}(t) - b = 0$ ,

де,  $\hat{x}_w(t)$  – продовження досліджуваної реалізації в область  $t > t_k$ ; задана допустима область  $[a, b]$  така, що при виконанні перевірки  $a < x < b$ , мережа вважається дієздатною і в даному випадку набуде виду

$$X^{PS}(t) - a = 0; X^{PS}(t) - b = 0. \quad (2)$$

де,  $X^{PS}(t) = X[t/x_w(\Theta), t_1 \leq \Theta \leq t_k]$  – апостеріорний (умовний) випадковий процес, що виникає з апіорного при врахуванні результатів контролю.

Як і в детермінованому варіанті, задача вирішується в два етапи. Перший етап – екстраполяція випадкового процесу  $X(t)$  з врахуванням даних контролю (прогнозування стану ІСД), другий – визначення деяких ймовірних характеристик випадкового залишку часу до атаки  $\Delta T_{II}$  (прогнозування НСД). Тут очевидна визначальна роль першого етапу, етапу екстраполяції, від можливостей якого залежить розв'язок задачі в цілому. При вирішенні задачі екстраполяції можна розглядати дві основні постановки [7,8], що відрізняються по виду передбачуваної характеристики процесу  $X(t)$ .

1. Отримання в певному сенсі оптимальної оцінки майбутнього значення даної реалізації процесу  $\hat{x}(t_k + \tau) = Hx_w(t)$ ,  $t \leq t_k$ ,  $0 \leq \tau \leq \infty$  за її відомим минулим  $x_w(t)$ ,  $t \leq t_k$ . Тут  $H$  – оператор екстраполяції, вибраний виходячи із заданих вимог оптимальності. Цей підхід до задачі екстраполяції випадкового процесу отримав найбільше розповсюдження в задачах автоматичного управління та зв'язку, і в даний час таке визначення операції екстраполяції є загально прийнятим [9].

Не важко помітити, що стосовно задачі контролю після рішення власної задачі екстраполяції цей підхід формально перестає відрізнятися від детермінованого. Його очевидним недоліком в даному випадку є те, що в кінцевому підсумку він дозволяє отримати порівняно обмежену інформаційну прогнозу характеристику – точкову оцінку випадкової величини  $\Delta T_{II}$ .

2. Визначення умовного (апостеріорного) випадкового процесу  $X^{PS}(t) = X[t/x_w(\Theta), t_1 \leq \Theta \leq t_k] = \Gamma[X(t), x_w(\Theta)]$ , де  $\Gamma$  – оператор перетворення апіорного процесу в апостеріорний, що не використовує інформацію контролю. Цей метод рішення задачі є більш загальним, чим методи першої групи, які витікають з нього як випадковість. При його використанні система рівнянь (2) зберігає свій стохастичний характер, її рішення дозволяє знайти всі необхідні ймовірності характеристики  $\Delta T_{II}$ .

Однак, одночасно виникають і суттєві труднощі, оскільки, загальних методів рішення цієї системи при відсутності обмежень на характер випадкового процесу не існує. Таким чином, кожен із варіантів рішення задачі екстраполяції має свої переваги і недоліки. Це призводить до необхідності більш детального аналізу. Таким чином, жоден з розглянутих методів не є достатньо універсальним для застосування його в системах автоматизованого контролю.

Крім цього розглянуті методи дозволяють дати лиш точкову оцінку процесу (НСД), як вказувалось раніше, не є вичерпним рішенням задачі. В зв'язку з цим значного розвитку отримали різні інженерні методи, що дозволяють вирішити задачу прогнозу в цілому шляхом моделювання відповідного випадкового процесу з використанням принципу статистичних дослідів. Оскільки автоматична система контролю (АСК) має в своєму складі засоби обчислювальної техніки, то ці методи є особливо прийнятними при автоматизації контролю. Ідея їх полягає в тому, що тим чи іншим методом моделюється безліч реалізацій випадкового процесу  $X^{PS}(t)$ , які використовуються для рішення системи рівнянь (2) і визначення будь-яких необхідних апостеріорних характеристик статистики цим методом. В даному випадку рішення задачі прогнозу складається з наступних етапів:

1 етап. Отримання з статистичних даних елементів опису досліджуваного випадкового процесу  $X(t)$ , придатного для відтворення його шляхом моделювання. Від універсальності такого опису в більшій мірі залежить і універсальність методу в цілому.

2 етап. Розробка алгоритму, що дозволяє враховувати значення конкретної реалізації процесу  $X(t)$ , що вимірювались при контролі, і отримування на цій основі опису апостеріорного випадкового процесу  $X^{PS}(t)$ . Наявність такого опису дозволяє шляхом моделювання визначити характеристики даного процесу і, таким чином, повністю вирішити задачу прогнозування.

3 етап. Розробка алгоритму рішення системи стохастичних рівнянь (2). Виконання даного етапу дозволяє повністю вирішити задачу прогнозування НСД.

Наведений перелік показує, що основною передумовою до рішення задачі є наявність достатньо зручного опису процесу  $X(t)$ . При цьому пропонується апроксимувати реальний випадковий процес  $X(t)$  лінійною функцією часу  $X(t)=A+Bt$ , де  $A$  і  $B$  – випадкові коефіцієнти ймовірні, характеристики яких визначаються за допомогою методу найменших квадратів на основі з умови  $M \int_T [X(t) - (A + Bt)]^2 dt = \min$ , при чому  $T$  – інтервал спостереження випадкового процесу  $X(t)$ .

### III Висновки

Проблема прогнозування включає в себе низку труднощів, одні з яких власне зв'язані з прогнозуванням, інші характерні для всіх напрямків автоматичного контролю, треті визначають загальні можливості прогнозування і його місце серед інших видів контролю.

Таким чином в статті досліджено та приведено деякі загальні проблеми прогнозування несанкціонованого доступу в інформаційних системах, досліджено загальні методи прогнозування та представлено етапи вирішення задачі прогнозування в автоматизованих системах контролю, що в свою чергу дозволило отримати подальший розвиток вирішенню проблеми прогнозування НСД.

*Список використаної літератури:* 1. Силин В. Б., Заковряшин А. И. *Автоматическое прогнозирование состояния аппаратуры управления и наблюдения*. Москва. Энергия 1973г. – 336 с. 2. Путінцев Н. Д. *Апаратний контроль цифрових обчислювальних машин*. – М. Сов. радио, 1966. – 236 с. 3. Смирнов Н. В., Душин-Барковский И. В. *Курс теории вероятностей и математической статистики* – М.: Наука, 1968. – 576 с. 4. Тихонов В. И., *Достижение границ марковских процессов // изв. Вузов радиотехника, т. 15, № 4, 1972. – С. 253.* 5. Згуровський М. З., Панкратова Н. Д., *Техническое предвидение* -К.: Политехника, 2005. – 165 с. 6. Демидович Б. П., Марон Н. А., Шувалова Д. З. *Численные методы анализа* –М.: Наука, 1967. – 242 с. 7. Клямко Э. И. *Схемный и тестовый контроль автоматических цифровых вычислительных машин* – М.: Сов. Радио., 1983. – 320 с. 8. Сидоров А. М. *Методы контроля электронных цифровых машин*. – М.: Сов. Радио., 1986. – 342 с. 9. Згуровський М. З. *Основи системного аналізу/ Згуровський М. З., Панкратова Н. Д.* – К:ВНУ, 2007–544 с.

**Олексій Мервінський**

*Національний технічний університет України «Київський політехнічний інститут»*

УДК 35.078.3+340.68

## ЄВРОПЕЙСЬКІ ВИМОГИ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

*Анотація:* Розглядаються нормативно-правові акти Європейського Союзу, пов'язані із захистом і обробкою персональних даних у сфері електронної комерції і спрямовані на захист основоположних прав і свобод людини і громадянина, проведено їх аналіз.

*Summary:* The article reviews normative acts, regulations, constitutive or other documents European Union involving protection and processing of personal data in the field of e-commerce and aim to protect the fundamental rights and freedoms of natural persons, particularly the right to privacy in relation to the processing of personal data and includes statistical analysis.

*Ключові слова:* Електронна комерція, персональні дані, захист персональних даних, захист прав суб'єкта персональних даних.

### I Вступ

Розвиток новітніх технологій та сучасних засобів комунікацій призвів до появи в другій половині ХХ століття нового виду діяльності – електронної комерції («*electronic commerce*» або «*e-commerce*»), яка за своєю сутністю є сферою економіки, що функціонує в електронній формі в електронному середовищі з використанням комп'ютерних мереж, зокрема глобальної мережі Інтернет. Проте створення та забезпечення функціонування таких сфер діяльності супроводжується можливістю виникнення певних ризиків, насамперед для фізичних осіб, які вступають у правові відношення в результаті створення попиту на товари та послуги, укладання договорів в електронній формі, здійсненні електронних платежів, а також обслуговуванні споживачів. Масовий характер використання персональних даних в сфері електронної