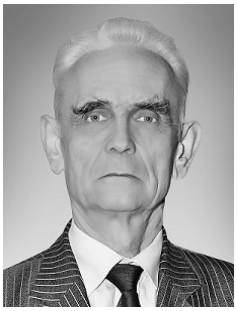
© Dudykevich V., Opirskyy I. Definition sources of error prediction for unauthorized access to information networks of the state // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 1, p. 7-11.

ВИЗНАЧЕННЯ ДЖЕРЕЛ ПОМИЛОК ПРОГНОЗУВАННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ В ІНФОРМАЦІЙНИХ МЕРЕЖАХ ДЕРЖАВИ

Валерій Дудикевич, Іван Опірський

Національний університет «Львівська Політехніка», Україна



ДУДИКЕВИЧ Валерій Богданович, д.т.н.

Рік та місце народження: 1941 рік, м. Білоскелюватe, Україна.
Освіта: Львівський політехнічний інститут (з 2000 року – Національний університет «Львівська Політехніка»), 1963 рік.
Посада: завідувач кафедри захисту інформації з 2006 року.
Наукові інтереси: вимірювальні перетворювачі частотних сигналів, число-імпульсні перетворювачі кодів для засобів вимірювання та керування, медичне приладобудування, вимірювальні випробувальні комплекси, методи і засоби технічного захисту інформації.
Публікації: понад 500 наукових публікацій, серед яких монографії, словники, підручники, навчальні посібники, наукові статті та авторські патенти на винаходи.
E-mail: vdudykev@gmail.com

ОПІРСЬКИЙ Іван Романович, к.т.н.

Рік та місце народження: 1987 рік, м. Сімферополь, АР Крим, Україна.
Освіта: Національний університет «Львівська Політехніка», 2008 рік.
Посада: старший викладач кафедри захисту інформації з 2015 року.
Наукові інтереси: методи і засоби технічного захисту інформації, охорона державної таємниці, проектування комплексних систем захисту інформації, лазерні системи акустичної розвідки, математичні методи та моделі захисту інформації, технічні канали витоку інформації, спецвимірювання.
Публікації: більше 50 наукових публікацій, серед яких наукові статті, монографія, навчальний посібник, тези та матеріали доповідей на конференціях.
E-mail: iopirsky@gmail.com

Анотація. *У даній статті досліджено та визначено джерела помилок прогнозування несанкціонованого доступу в інформаційних мережах держави. Доведено, що одним з джерел помилок контрольованих параметрів є похибки зміни значень проміжку реалізації, що спостерігається, випадкового процесу змін стану контрольованої в часі мережі. Це джерело помилок можна визначати в тому випадку, якщо знайдено вирішення задачі прогнозу в цілому. Якщо припустити, що відрізок реалізації відомий цілком точно і екстраполяція його проведена без помилок, то єдиним джерелом похибки залишається методика вирішення рівняння. Джерела похибок, що виникають на першому етапі (на етапі екстраполяції), в свою чергу можна розбити на дві групи. Перша пов'язана з деяким значенням функціоналу, тобто з недосконалістю використаної моделі об'єкта, неповнотою або неточністю кількісних характеристик, що описують об'єктивно існуючі залежності в досліджуваному процесі. Друга група похибок, виникає на етапі екстраполяції, і має місце навіть в тих випадках, коли екстраполяційний функціонал відомий цілком точно, а вихідний відрізок реалізації спостерігається без помилок. Причиною цих похибок є сам стохастичний характер задачі, що вирішується. Проведений аналіз дозволив виділити основні можливі проблеми, які потрібно вирішити для забезпечення високої достовірності прогнозу, що в свою чергу може бути використано для підвищення ефективності прогнозування несанкціонованого доступу в інформаційних мережах держави.*

Ключові слова: *несанкціонований доступ, інформаційні мережі держави, прогнозування, джерела похибок, помилка, час життя, випадковий процес, екстраполяція.*

Вступ

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

Прогнозування несанкціонованого доступу (НСД) на інформаційні мережі держави (ІМД) без сумніву повинно 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 ІМД, повинні бути зміни значень саме цих параметрів. Таким чином, прогнозування НСД в ІМД 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 ІМД під впливом НСД [1]. Кінцевою метою досліджень в цьому напрямку є створення певного алгоритму прогнозу.

Виконання будь-якої форми контролю стану ІМД базується на використанні загальної моделі мережі контролю [2]. Така модель повинна дозволяти виділяти достатню сукупність контрольованих параметрів для отримання на даному рівні відповідного рішення з заданим рівнем достовірності і для контролю функціонування, і для допускового контролю, і для діагностичного контролю, і для прогнозованого контролю.

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

Вплив поступових змін параметрів мережі може передбачити можливе несанкціоноване підключення до мережі. Цей висновок, здалось би, повинний означати, що проведення прогнозуючого контролю є доцільним в всіх без виключеннях випадках та застосовується до всіх видів підключення. Однак, такий висновок був би надмірно поспішним. Наявна статистика в жодній мірі не стосується питання про те, наскільки передчасним змінам ІМД, 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 ІМД не може бути віднесена в даний час 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. Конкретно відповісти поки що важко. 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.

В той же час прогнозування роботи засобів обчислювальної техніки, яка являється основним елементом ІМД, здійснюється своїми методами [3]. Слід очікувати, що прогнозування НСД може бути ефективним для вузлів ІМД з яскраво вираженим безперервними властивостями, що містять значне число компонентів, процеси в яких відрізняються сильною взаємообумовленістю. Але це відношення залежить не тільки від принципової можливості здійснення прогнозу. При складанні загальних алгоритмів контролю реального стану ІМД 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, припадаючи на одну прогнозовану атаку, для якої ще призначається доцільним проведення прогнозованого контролю. Якщо інтенсивність атак, які можуть контролюватись кожним прогнозним параметром, виявляється нижче цього порогу, то прогноз стає недоцільним.

Тому, коло найбільш важливих проблем, пов'язаних з проблемою прогнозу НСД в ІМД є достатньо широким. Вичерпне дослідження цих питань навряд чи можна розглянути в одній статті. Тому в межах нашої статті ми зупинимось на дослідженні тих змін характеристик та параметрів ІМД, передбачити які, навіть при повному контролі параметрів, дуже важко, адже вони виникають внаслідок помилок прогнозу в незалежності від того, чи є наявним НСД, чи ні.

Аналіз існуючих досліджень

Деякі питання, пов'язані з послідовною перевіркою прогнозів і їх оцінюванням, наведені у [4]. Для моделювання процесів НСД до інформації в ІМД широкого використання набули теоретичні моделі безпеки, які досить докладно описані в [5-7]. Сама проблема достовірності інформації, що передається, поглиблено досліджувалась, зокрема, в ряді робіт Вольтера, Гуткнехта, Вейкерта та інших [8-10]. Проте дослідження та аналіз проблематики прогнозування НСД в ІМД можна зустріти в наших попередніх наукових роботах [11-14].

Отже, ***метою*** даної роботи є визначення фізичних причин виникнення помилок (джерел похибок при прогнозуванні) прогнозування НСД в ІМД, які необхідно вирішити для забезпечення високої достовірності прогнозу.

Основна частина роботи

Для значення вектора $X^{(n)}$ задана допустима область $S_p^{(n)}$ можливих атак на ІМД і, таким чином, визначено поняття впливу (атаки). Це, в свою чергу, дозволяє визначити апріорну ймовірність захищеності мережі, проте необхідно дослідити цей процес.

Впровадження засобів обчислювальної техніки для прогнозування НСД вимагає попереднього накопичення статистичних даних про характер змін стану ІМД під час впливу НСД і за його відсутності, що є можливим лише за умови

періодичного кількісного контролю. Таким чином, на початковому етапі експлуатації мережі єдиною можливою формою прогнозу НСД є контроль стану ІМД, звідки випливає, що засоби обчислювальної техніки (ЗОТ), а саме персональний комп'ютер (ПК), завжди впроваджуються в уже складену систему, що базується на достатньо високій якості контролю. У цих умовах природно розглянути ПК як деякий додатковий засіб, що дозволяє, не маючи сформованої системи обслуговування мережі в цілому, покращити її показники і підвищити достовірність передбачення за рахунок впливу на апріорну надійність і захищеність мережі. У цих умовах ймовірність передбачення і відбиття НСД визначається виходячи з [15], з чого слідує, що контроль ІМД впливає на ймовірність захищеності контрольованих і обслуговуваних елементів мережі тільки через умовну ймовірність помилки II роду β. Використовуючи введене припущення про достатньо високу якість інформації про стан мережі, можна припустити, що $\beta = 0$ і описує ймовірність атаки, що поступає на об'єкти введеною в [15] умовною функцією передбачення $F_0(t)$. Це припущення не є принциповим, однак воно суттєво спрощує наступні роздуми.

Таким чином, при зроблених припущеннях мережа є дієздатною. При цьому з врахуванням [15] для нормального функціонування ІМД залишаємо вираз в вигляді:

$$P_{nk}(t) = \frac{1}{K_{\Pi\tau} + (1 - K_{\Pi\tau})F_0(\tau)}, \quad (1)$$

$$\begin{cases} K_{\Pi\tau}F_0(t) + (I - K_{\Pi\tau})F_0(\tau), t \le \tau, \\ F_0(t), t > \tau. \end{cases}$$

де $P_{nk}(t)$ – ймовірність проведення НСД, $F_0(t)$ – умовна функція передбачення, $K_{\Pi\tau}$ – ймовірність помилки прогнозу. Додатково припустимо, що робота мережі під дією НСД є ідеальною і зводиться до повного відновлення або відбиття атаки.

При цих умовах для апостеріорної ймовірності (вірогідності) передбачення НСД і обслуговування мережі, очевидно справедливо

$$P_{\Pi к+ВП}(\tau) = \begin{cases} 1 - \beta_{\Pi\tau}[1 - F_0(t)], t \le \tau, \\ 1 - \beta_{\Pi\tau}[1 - F_0(t)]F_0(t) / F_0(\tau), t \ge \tau. \end{cases} \quad (2)$$

З використанням (2) основна вимога до якості контролю (оскільки обслуговування ідеальне і вже не може бути покращено) формулюється у вигляді:

$$P_{\Pi к+ВП}(\tau) = 1 - \beta_{\Pi\tau}[1 - F_0(t)] \ge P_g. \quad (3)$$

Єдиний параметр, який можна варіювати в останньому виразі – це умовна ймовірність помилки прогнозу II роду $\beta_{\Pi\tau}$. Таким чином, вимоги (3) в кінцевому випадку можна звести до нерівності

$$\beta_{\Pi\tau} \le \beta_0 = (1 - P_g) / (1 - P_0(\theta)), \quad (4)$$

яка і буде прийнята в подальшому в якості основної.

Інакше кажучи, задача зводиться до знаходження умов, при яких значення умовної ймовірності помилки прогнозу II роду задовольняється умовно (4) при мінімумі деякої функції втрат. Для того, щоб ця задача могла бути розв'язаною, необхідно проаналізувати джерела і фізичну природу помилок, що виникають.

Як показано в [15], вирішальне правило, що використовується при контролі, загалом має вигляд

$$\Delta T^*_{ж} > \tau, \quad (5)$$

де $\Delta T^*_{ж}$ – оцінка залишку часу життя $T_{ж}$ контрольованого елемента мережі, що зберігся до моменту t_k. З (5) безпосередньо витікає, що помилкове рішення, прийняті за результатами контролю, пояснюються, в кінцевому підсумку, єдиною причиною – похибкою виміру випадкового залишку часу життя $\Delta T_{ж}$. Як було показано в [15], величина $\Delta T_{ж}$ безпосередньо при контролі спостерігатися не може, у зв'язку з чим її справжнє значення можна оцінити тільки шляхом непрямого вимірювання, тобто визначити на основі відомої залежності між цією величиною і величинами, що піддаються прямим змінам.

Звідси слідує, що одним з джерел помилок контрольованих параметрів (КП) є похибка зміни значень проміжку реалізації $X_{\omega}(t), 0 \le t \le t_k,$, що спостерігається, випадкового процесу зміни стану контрольованої в часі мережі. Вплив цієї похибки на результативну похибку можна оцінити, якщо відомий функціонал

$$T_{ж\omega} = \Phi_T[X_{\omega}(t)], 0 \le t \le t_k, \quad (6)$$

що зв'язує відрізок спостереження реалізації з шуканим часом існування мережі.

Інакше кажучи, це джерело помилок можна вивчати в тому випадку, якщо знайдено вирішення задачі прогнозу в цілому.

Як показано в [15], найбільш універсальний метод визначення залишку часу життя складається з двох етапів. На першому – реалізація, що спостерігається, екстраполюється в області $S > t_k$:

$$\hat{x}(s) = \Phi_X\left[X_{\omega}(t)\right], 0 \le t \le t_k, \quad (7)$$

а на другому – визначається момент першого перетину границі області $S_p^{(n)}$ продовження реалізації, що відповідає першому за часом кореню рівняння

$$\hat{X}_{\omega}(S) - S_p^{(n)} = 0, \quad (8)$$

вирішеного відносно S.

Таким чином, функціонал (6) на практиці реалізується в два етапи, кожний з яких може супроводжуватись помилками.

Найбільш зрозумілий фізичний сенс помилок, що виникають на другому етапі. Якщо припустити, що відрізок реалізації $x_{\omega}(t), 0 \le t \le t_k$, відомий цілком точно і екстраполяція його в область $S > t_k$ проведена без помилок, то єдиним джерелом похибки залишається методика вирішення рівняння (8). В принципі це рівняння також може бути вирішено цілком точно. Однак, методи екстраполяції, що розвинуто в літературі продовжують застосовуватись електронно-обчислювальними машинами (ЕОМ), що пов'язано з квантуванням процесу за часом. В результаті цього, шуканий час життя $T_{ж}$ можна знайти лише з точністю до кроку квантування, який і обмежує при прийнятих припущеннях мінімально досяжне значення похибки. Облік помилок дискретності і

регулювання їх величини не викликають принципових складностей. Тому, при подальших дослідженнях помилками дискретності можна знехтувати і вважати, що на цьому етапі похибки відсутні.

Джерела похибок, що виникають на першому етапі (на етапі екстраполяції), в свою чергу можна розбити на дві групи. Перша зв'язана з деяким значенням функціоналу $\Phi_T[\cdot]$, тобто з недосконалістю використаної моделі об'єкта, неповнотою або неточністю кількісних характеристик, що описують об'єктивно існуючі залежності в досліджуваному процесі. При детермінованому підході ці помилки зазвичай обумовлені неадекватністю вибраного аналітичного опису досліджуваної залежності, а при стохастичному – похибками визначення ймовірних характеристик апріорного випадкового процесу і неточностями перетворення апріорного процесу в апостеріорний.

Очевидно, що вплив похибок визначення ймовірних характеристик досліджуваного випадкового процесу може бути досить суттєвим, однак він буде монотонно зменшуватись по мірі накопичення і обробки статистичних даних, стаючи в границях безкінечно малих. Оскільки, методи використання статистичних даних про процес для зменшення даної складової помилки розроблені достатньо добре, подальший її розгляд не представляє інтересу.

Дещо інша ситуація складається з похибками, що викликані не відповідністю екстраполяційного функціоналу $\Phi_T[\cdot]$. Тут накопичення і обробка первинних статистичних даних про процес, як правило, не дозволяє безпосередньо судити про якість екстраполяції. Тому, необхідно розробити методи оцінки якості екстраполяційного функціоналу можливо на більш ранніх стадіях вирішення задачі прогнозу. Одночасно з цим виникає задача розробки методів покращення екстраполяційного функціоналу з тим, щоб завжди забезпечити близьке до потенційно можливої якості прогнозу. Таким чином, даний вид похибки і методи їх зменшення потребує детального аналізу.

Друга група похибок, виникає на етапі екстраполяції і має місце навіть в тих випадках, коли екстраполяційний функціонал (6) відомий цілком точно, а вихідний відрізок реалізації $x_\omega(t), 0 \le t \le t_k$, спостерігається без помилок. Причиною цих похибок є сам стохастичний характер задачі, що вирішується. Наявність в задачі «випадкових факторів» [16], принципова можливість прогнозу. Помилка, викликана ними, принципово невиправна, що робить надзвичайно важливим вивчення причин її виникнення і можливих методів управління її величиною. Раніше вказувалось, що функціонал (6) при досліджуванні цих помилок, відомий цілком точно. Це означає, що він в принципі дозволяє врахувати і використовувати всі зв'язки і залежності, що об'єктивно існують між випадковою величиною $T_{ж}$ і випадковим процесом $X(t)$, що спостерігається. Проте для того, щоб вказані можливості дали ефект при практичній реалізації, необхідно, щоб ці зв'язки дійсно існували. Звідси виникає висновок, що для забезпечення ефективного прогнозу важливе (найбільш визначальне) значення має вибір параметрів мережі, за допомогою яких здійснюється цей прогноз. При інших рівних умовах чим сильніший зв'язок часу життя $T_{ж}$ з процесом $X(t)$, що спостерігається, тим менше розглянута помилка. В границях вона стає рівною нулю, коли зв'язок детермінований і набуває максимального значення, і, коли $T_{ж}$ і $X(t)$ не залежить один від одного.

Крім того, можна вказати ще одне джерело похибок стохастичного характеру, виникає навіть в тому випадку, коли зв'язок між $T_{ж}$ і $X(t)$ достатньо високий. Ці похибки залежать від точності екстраполяції реалізації $x_\omega(t), 0 \le t \le t_k$, що спостерігається, в область $S > t_k$. Як і в попередньому випадку, точність екстраполяції при відомому функціоналі $\Phi_X[\cdot]$ обумовлена наявністю суттєвих зв'язків між різноманітними часовими перетинами процесу $X(t)$. Чим сильніші ці зв'язки і більші їх протяжності в часі, тим з більшою точністю і на більшому часовому інтервалі може здійснюватись прогноз.

Таким чином, наявність суттєвих зв'язків між відрізками реалізації $x_\omega(t)$, що спостерігаються, і часом існування мережі $T_{ж\omega}$ є необхідною, але є не достатньою умовою ефективного прогнозу. Крім того, необхідно, щоб вихідний випадковий процес $X^{(n)}(t)$, що описує зміни стану мережі в часі, володів суттєвим наслідком.

Висновки

Резюмуючи зроблений аналіз фізичних причин виникнення помилок прогнозу, можна виділити основні можливі проблеми, які потрібно вирішити для забезпечення високої достовірності прогнозу. У порядку значимості до них відносяться: розробка методики вибору прогнозованих параметрів, що задовольняють вказані потреби; дослідження можливостей побудови прогнозних і екстра полярних функціоналів $\Phi_T[\cdot]$ і $\Phi_X[\cdot]$, що дозволяють в необхідній мірі врахувати стохастичні залежності в досліджуваних процесах; дослідження впливу похибки вимірювань значень контрольованої реалізації процесу на результати прогнозу.

Література

[1] Опірський І.Р. Прогнозування несанкціонованого доступу в інформаційних системах держави з використанням перетворення Карунена-Лоєва / І.Р. Опірський // Інформатика та математичні методи в моделюванні. – Том 5, №3. – 2015. – С. 234-249.

[2] Путінцев Н.Д. Апаратний контроль цифрових обчислювальних машин / Н.Д. Путінцев // М.: Сов. Радио, 1966. – 236 с.

[3] Смирнов Н.В. Курс теории вероятностей и математической статистики / Смирнов Н.В., Дунин-Барковский И.В. – М.: Наука, 1968. – 576 с.

[4] Тартановский А.Г. Адаптивные алгоритмы последовательной проверки гипотез и оценивания

параметров / А.Г. Тартановский // Тр. МФТИ : Радиотехника и электроника, 1979. – С. 29-31.

[5] Мельников В.В. Безопасность информации в автоматизированных системах / В.В. Мельников // М: Финансы и статистики, 2003. – 368 с.

[6] Браїловський М.М. Технічний захист інформації на об'єктах інформаційної діяльності / М.М. Браїловський, С.М. Головань , В.В. Домарєв // К: Вид. ДУІКТ, 2007. – 178 с.

[7] Девянин П.Н. Теоретические основы компьютерной безопастности / П.Н. Девянин, О.О. Махальський, Д.І. Правиков, А.Ю. Щербаков // М. : Радио и связь, 2000. – 193 с.

[8] Gutknecht W., Die Sicherheit einer Nachricht als Funktion der Bandbreiten und der Stцrungen in Nachrichtenkandlen und den Analogrechnern zur Nachrichtenentzerrung. Staatsexamensarbeit–Arb.,Univ. Marburg(Lahn). –1983. – 308 z.

[9] Kran B.M. Beitrag zur Theoric der Optimierung gestцrter linearer Unertragungskandle unter Berrьcksichtigung der optimalen Information-sьbertradung. Diss. TH Karl-Marx-Stadt, 1987. – 204 z.

[10] Lцhn K., Weinerth H., Wolter H., Zur Frage der Fehlerfortpflozung und Sicherheil bei der Ubermittlung von elektronischen analogrechnern zur Rьckrechnung, AEы, 15,1981. – 455-466 z.

[11] Опірський І.Р. Технології попередження та прогнозування НСД на основі математичного апарату Баєсовських не усічених процесів прийняття рішень / І.Р. Опірський // Інформаційна безпека. – №3(15). –2014. – С. 52-60.

[12] Опірський І.Р. Оптимізація послідовних процесів прийняття рішень при умовно екстремальній постановці задачі / І.Р. Опірський // Інформаційна безпека. – №4 (16). – 2014. – С. 120-127.

[13] Опірський І.Р. Особливості процедури прогнозування несанкціонованого доступу / І.Р. Опірський // Захист інформації, спецвипуск, 2014. – С. 74-80.

[14] Опірський І.Р. Проблематика основного постулату прогнозування НСД/ І.Р. Опірський // ДНДІ МВС України: Сучасна спеціальна техніка. – №2(41). – 2015. – С. 3-9.

[15] Кудрицкий В.Д. Автоматизация контроля радиоэлектронной аппаратуры / Кудрицкий В.Д., Синица М.А., Чинаев П.И //М: Сов.радио, 1977. – 256 с.

[16] Ивахненко А.Г. Предсказание случайных процессов / А.Г. Ивахненко , В.Г. Лапа //К: Наукова думка. –1969. – 288 с.

УДК 004.056.53:061.68; 004.3.75:061.68 (045)

Дудыкевич В.Б., Опирский И.Р., Определение источников ошибок прогнозирования несанкционированного доступа в информационных сетях государства

Аннотация. *В данной статье исследовано и определено источники ошибок прогнозирования несанкционированного доступа в информационных сетях государства. Доказано, что одним из источников ошибок контролируемых параметров являются погрешности изменения значений промежутка реализации наблюдаемого случайного процесса, изменения состояния контролируемой во времени сети. Этот источник ошибок можно определить в том случае, если найдено решение задачи прогноза в целом. Если предположить, что отрезок реализации известный вполне точно и экстраполяция его проведена без ошибок, то единственным источником погрешности остается методика решения уравнения. Источники погрешностей, возникающих на первом этапе (на этапе экстраполяции), в свою очередь можно разбить на две группы. Первая связана с некоторым значением функционала, тоесть с несовершенством используемой модели объекта, неполнотой или неточностью количественных характеристик, описывающих объективно существующие зависимости в исследуемом процессе. Вторая группа ошибок возникает на этапе экстраполяции и имеет место даже в тех случаях, когда экстраполяционный функционал известный вполне точно, а выходной отрезок реализации наблюдается без ошибок. Причиной этих ошибок является сам стохастический характер решаемой задачи. Проведенный анализ позволил выделить основные возможные проблемы, которые нужно решить для обеспечения высокой достоверности прогноза, что в свою очередь, может быть использовано для повышения эффективности прогнозирования несанкционированного доступа в информационных сетях государства.*

Ключевые слова: *несанкционированный доступ, информационные сети государства, прогнозирование, источники погрешностей, ошибка, время жизни, случайный процесс, экстраполяция.*

Dudykevich V., Opirskyy I. Definition sources of error prediction for unauthorized access to information networks of the state

Abstract. *This article examines and identifies the sources of error prediction of unauthorized access to the information networks of the state. It is proved that one of the sources of errors in terms of monitored parameters is the error's value change interval of the observed realization of a random process along with the changes in the state within network time. This source of error can be determined if a solution to prediction problem is found in general. Assuming that the length of the implementation is quite accurate and its extrapolation is carried out without errors, the method of solving the equation is considered as the only source of error. Sources of errors arising in the first stage (the extrapolation step), in turn, can be divided into two groups. The first group is connected with the functional value, namely the imperfection of the object model, the incompleteness or inaccuracy of the quantitative characteristics describing the objective relations within the researched process. The second group of errors arises at the extrapolation step, and occurs even when the functional extrapolation is quite accurate as well as the output section of realization is observed without errors. Thus, a stochastic nature of the problem is the cause of these errors. The analysis identifies the key potential problems that should be solved in order to ensure the high reliability of the forecast that in turn, can be used to enhance prediction of unauthorized access to the information networks of the state.*

Key words: *unauthorized access, information network of the state, error sources prediction, error, lifetime, stochastic process, extrapolation.*

Отримано *3 лютого 2016 року*, затверджено редколегією *4 березня 2016 року*