DOI 10.15276/imms.v10.no 3-4.177
УДК 004.056.53:005.004.7

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 3-4, pp. 177-189

ВИЯВЛЕННЯ КІБЕРАТАК В ІНФОРМАЦІЙНИХ МЕРЕЖАХ

І.Р. Опірський[1], Ю.М. Ткач[2], В.О. Хорошко[3]

[1]Національний університет «Львівська політехніка», м. Львів, 79013, вул. С. Бандери, 12, Україна;
e-mail: iopirsky@gmail.com
[2]Національний університет «Чернігівська політехніка», м. Чернігів, 14035, вул. .Шевченка, 95, Україна;
e-mail: tkach_ym@ukr.net
[3]Національний авіаційний університет, 03058, м. Київ, просп. Любомира Гузара,1, Україна;
e-mail: professor_va@ukr.net

Усе більшого значення в забезпеченні національної безпеки різних держав світу набуває кібернетична безпека. Кібернетичні атаки та кібернетичні впливи все частіше стають одними з головних дій для досягнення мети контролю над різними об'єктами, такими як людина, організація, регіон, держава тощо в сучасному світі. Таким чином, у світі з'явилось нове явище у міжнародній політиці, а саме можливість досягненню власних політичних цілей, економічного та духовного підпорядкування народів інших держав без застосування військової сили, а лише з допомогою інформаційного впливу. Тому в світі доволі активно розвиваються кібернетичні атаки та кібернетичні впливи. В наслідок цього для ефективної роботи сучасних інформаційно-телекомунікаційних мереж та засобів їх захисту, а також для надійного виявлення та передбачення кібернетичних атак та несанкціонованих дій необхідно розвивати нові підходи та методи кібернетичної безпеки. Метою статті є виявлення кібернетичних атак в інформаційно-телекомунікаційних мережах. Зокрема, розглянуто задачу виявлення кібернетичної атаки на фоні білого гаусівського шуму за умови неперервного часу спостереження. Наведено теоретичне обґрунтування усередненого об'єкту прогнозування. При послідовному аналізі усередненого об'єкту прогнозування в загальному випадку з'ясовано, що він не дає достатню статистику в задачі послідовного виявлення кібератак. З вищесказаного слідує, що одним з головних питань при синтезі оптимальних послідовних і непослідовних кібератак з випадковими моментами появи є розробка алгоритмів формування усередненого об'єкту прогнозування. У результаті проведених досліджень запропоновано методику виявлення несанкціонованого доступу з невідомим моментом виникнення в дискретному часі спостереження.

Ключові слова: інформаційні системи, кібератака, усереднений об'єкт прогнозу.

Вступ

Поступовий перехід в розвитку людства від «інформаційного суспільства» та «високотехнічного» обумовлено еволюційним підходом до забезпечення безпеки в нових умовах на різних рівнях. Відбувається поступова трансформація концепції інформаційної громадянина, суспільства та держави до необхідності її поповнення новою концепцією кібернетичної безпекою. При цьому має місце процес розмежування різних видів безпеки за геополітичними рівнями та розумінням ролі кібернетичної безпеки на кожному з них. Необхідність розуміння ролі кібернетичної безпеки пов'язана в першу чергу з активізацією міжнародних терористичних, екстремістських організацій та злочинних угрупувань, а також окремих держав, котрі здійснюють кібератаки та кібервплив на громадян, суспільство, державу з метою реалізації власних інтересів [1, 2, 3].

Все більшого значення в забезпеченні національної безпеки різних держав набуває кіберпезпека. Кібератаки та кібервпливи все частіше стають одними з головних дій для досягнення мети контролю над різними об'єктами (людиною, організацією, регіоном, державою тощо) в сучасному світі [4]. Фактично виникло нове явище у

міжнародній політиці – можливість досягненню власних політичних цілей, економічного та духовного підпорядкування народів інших держав без застосування військової сили. Тому в світі доволі активно розвиваються кібератаки та кібервпливи.

При цьому, в умовах введення гібридних війн, протягом останніх років систематично відбуваються успішні кібератаки, кібердії та несанкціоновані дії терористів й зловмисників в інформаційно-комунікаційних мережах, що підриває оборону, економіку, військову та науково-технічну сфери не тільки держава, але й окремих галузей та підприємств.

Тому для ефективної роботи сучасних інформаційно-телекомунікаційних мереж та засобів їх захисту, а також для надійного виявлення та передбачення кібератак та несанкціонованих дій необхідно розвивати нові підходи та методи кібербезпеки. Слід відмітити, що математичний апарат, який застосовується, а також відомі методи та засоби захисту інформації в кібернетичному просторі та інформаційно-телекомунікаційних мережах з точки зору протидії зловмисникам, не забезпечують можливості прогнозуванню та виявленню кібератак для відповідного реагування на загрози інформації, але підхід в ранньому виявленні кібератаки в будь-який момент часу є досить актуальним.

Мета статті

Метою статті є виявлення кібератак в інформаційних мережах.

Основна частина

У [5,6,7] питання виявлення НСД з невідомим моментом виникнення розглядались в дискретному часі спостереження, проте ми розглядаємо задачу виявлення кібератаки $A(t)$ на фоні білого гаусівського шуму $V(t)$ інтенсивністю $N\left[MV(t)\right]=0$, $MV(t)V(a)=N\theta(1-a)$ за умови неперервного часу спостереження. Більш точно, припускаємо, що спостереженню притаманний випадковий процес виду:

$$X(t)=\theta I(t-\lambda_0)A(t)+V(t),\ t\geq 0, \tag{1}$$

де $\theta-$ параметр, який приймає значення 0 та 1 з ймовірностями $\pi_0=P(\theta=0)$ та $1-\pi_0=P(\theta=1)$; λ_0 – випадковий момент появи кібератаки $A(t)$, що являє собою в загальному випадку випадковий процес; $I(y)$ – індикаторна функція, яка дорівнює 1 при $y\geq 0$ та 0 в протилежному випадку. Будемо також вважати, що відомий апріорний розподіл $\Pi(\lambda)=P(\lambda_0\leq\lambda|\theta=1)$ величини λ_0.

У подальшому для коректного використання математичного апарату перейдемо до моделі, яка еквівалентна (1) з інформаційної точки зору, припускаючи, що спостерігається процес $y(t)$ зі стохастичним диференціалом [8].

$$dy(t)=\theta I(t-\lambda_0)A(t)dt+\sqrt{N}dw(t),t\geq 0, \tag{2}$$

при $w(t)$ – стандартний вінеровський процес.

Нехай P_0 та $P_{1\lambda}$ - ймовірнісні міри, які виникли внаслідок $y(t)$ при $\theta=0$ та $\theta=1$, $\lambda_0=\lambda$ відповідно; $\gamma_\lambda(t)=\frac{dP1\lambda}{dP0}(y^t)$ – область прогнозу (ОП) гіпотези $H_{1\lambda}$; $\theta=1,\lambda_0=\lambda$ і H_0, $\theta=0$; $\Lambda(t)=\int_0^\infty \gamma_\lambda(t)d\Pi(\lambda)$ - усереднений об'єкт прогнозу (УОП) $\left(y^t=\{y(u),u\le t\}\right)$.

Якщо процес (2) спостерігається на інтервалі [0,T] фіксованої тривалості T, а функція втрат має вигляд відповідно до [8,9]

$$g(\theta,\lambda,\mathrm{n},u_n)=\begin{cases} g_{01}(n),\ \theta=0,\ u_n=1, \\ g_{11}(n)+C\left(n-[\lambda]\right),\ \theta=1,\ \lambda<\mathrm{n}\Delta,u_n=1, \\ g_{11}(n),\theta=1,\lambda\ge \mathrm{n}\Delta,u_n=1,\mathrm{n}=\overline{1,N}. \end{cases}$$

де $u_n=1$ – розв'язок про наявність збою на n-му кроці;
C- вартість затримки прийняття рішення про наявність збою на один крок; $[\lambda]=\mathrm{n}-1$ *при* $(n-1)\Delta\le\lambda<n\Delta$.

Розв'язок $u_n=0$ про відсутність збою на кроках $n=1$, $N-1$ ототожнюється з рішенням u_n про продовження спостережень, оскільки при подальшому спостереженні збій може виникнути та бути виявленим. На N-му кроці спостереження призупиняються з вірогідністю 1 та поряд з втратами, наведені в попередньому виразі, виникають втрати [10], які пов'язані з прийняттям рішенням $u_N=0$:

$$g(\theta,\lambda,u_n,N)=\begin{cases} g_{00}(N),\ \theta=0,\ u_N=0; \\ g_{10}(N)+C\left(N-[\lambda]\right),\ \theta=1,\ \lambda<N\Delta,u_N=0; \\ \tilde{g}_{10}(N),\theta=1,\lambda\ge \mathrm{N}\Delta,u_N=0. \end{cases}$$

У цих виразах значення $g_{i1}(n)$, $g_{i0}(N),\tilde{g}_{1j}(n)$ не залежать від λ, причому $g_{11}(n)<\tilde{g}_{11}(n)\le g_{01}(n),g_{00}(N)\le g_{10}(N)\le g_{10}(N)$. Їх залежність від номеру етапу може бути обумовлена, наприклад, вартістю спостережень. Однак, в багатьох задачах покладають, що $\tilde{g}_{11}(n)=g_{01}(n)$ та $\tilde{g}_{10}(N)=g_{00}(N)$. При цьому $N\Delta=T,C\left(N-[\lambda]\right)=C(T-\lambda)$, то оптимальне байєсове непослідовне правило має вигляд:

$$u_t^0\Lambda(T)=\begin{cases}1,\Lambda(T)\ge H\\ 0,\Lambda(T)<H\end{cases}. \tag{3}$$

Правило (3) оптимально також в умовах екстремальній задачі, коли потрібно мінімізувати середню ймовірність пропуску при заданій ймовірності хибної тривоги α_0(*при цьому* $H=H(\alpha_0)$ є рішенням рівняння $P_0\left[\Lambda(T)\ge \mathrm{H}(\alpha_0)=\alpha_0\right]$.

При послідовному аналізі усередненого об'єкту прогнозування (УОП) в загальному випадку не являє собою достатню статистику та в задачі послідовного виявлення [11].

З вищесказаного слідує, що одним з головних питань при синтезі оптимальних послідовних і непослідовних виявлювачів кібератак з випадковими моментами появи є знаходження алгоритмів формування УОП. Для моделі (1) ця задача детально розглянута в [12], це показано, що $\Lambda(t)$ задовольняє стохастичне рівняння:

$$d\Lambda(T) = N^{-1}[\int_0^t m_\lambda(t)\gamma_\lambda(t)d\Pi(\lambda)]dy(t), \mathrm{t} > 0, \Lambda(0) = 1 \tag{4}$$

У виразі (4) $m_\lambda(t) = M_{1\lambda}[I(t-\lambda)A(t)|y^t]$ – апостеріорне математичне сподівання, що є оптимальним в середньоквадратичному змісті фільтраційної оцінки кібератаки $A(t)$ при $\mathrm{t} \geq \lambda$ у відомому $\lambda_0 = \lambda[m_\lambda(\mathrm{t}) = 0$ при $t < \lambda; M_{1\lambda}$ – сподівання, що відповідає мірі $P_{1\lambda}]$. При цьому $\gamma_\lambda(t)$ задовольняє рівняння:

$$d\gamma_\lambda(t) = N^{-1}\gamma_\lambda(t)m_\lambda(\mathrm{t})\mathrm{dy}(\mathrm{t}); t > 0, \gamma_\lambda(0) = 1 \tag{5}$$

розв'язок якого має вигляд:

$$\gamma_\lambda(t) = \exp[N^{-1}\int_0^t m_\lambda(u)dy(u) - (2N)^{-1}\int_0^t m_\lambda^2(u)du] \tag{6}$$

де $\gamma_\lambda(t) = 1$ при $\lambda > t$.

З рівнянь (4) - (6) слідує, що в загальному випадку, коли кібератака $A(t)$ довільна, алгоритм формування УОП потребує усереднення величини $m_\lambda(\mathrm{t})$ $\gamma_\lambda(t)$ за множиною значень λ, причому знаходження функціоналу $m_\lambda(\mathrm{t})$, в цілому наштовхується на великі труднощі. Якщо $A(t), t \geq 0$, - Гаусівській процес, то $m_\lambda(\mathrm{t})$ задається лінійним функціоналом виду:

$$m_\lambda(t) = \begin{cases} \int_0^1 \mathrm{H}(t,u), d\mathrm{y}(u), \lambda \leq \mathrm{t} \\ 0, \lambda > t \end{cases}.$$

де $\mathrm{H}(t,u)$ - імпульсна характеристика фільтру, знайдена з рівняння Вінера-Хопфа.

Задача суттєво спрощується, якщо кібератака $A(t)$ є детермінованою функцією. Тоді

$$m_\lambda(t) = \begin{cases} \mathrm{A}(t), \lambda \leq \mathrm{t} \\ 0, \lambda > t \end{cases},$$

і, як слідує з (4) та (6), УОП задовольняє рівняння:

$$d\Lambda(\mathrm{t}) = N^{-1}A(t)\left[\Lambda(\mathrm{t}) - S_t\right]dy(t), \quad t > 0, \Lambda(0) = 1 \tag{7}$$

де $S_t = 1 - \Pi(t)$. З (2) та (7) слідує, що процеси $\{\Lambda(\mathrm{t}), F_t^y, Pi\}$, $t \geq 0$, $\mathrm{i} = 0,1$, є неоднорідними марківськими процесами. Це дозволяє довести, що в задачі

послідовного виявлення квазідетермінованої атаки з невідомим моментом появи [13] при відомих функціях втрат оптимальне послідовне правило має такий вигляд :

$$u_t^0\left[\Lambda(\mathrm{t})\right]=\begin{cases}1,\ \Lambda(\mathrm{t})\geq B(t),\\ 0,\ \Lambda(\mathrm{t})<B(t),\mathrm{t}\geq 0\end{cases},$$

де $B(t)$ - поріг, який є детермінованою функцією часу ($u_t^0=0$ еквівалентно продовженню спостережень).

У випадку детермінованої атаки $A(t)$ вдається знайти також рівняння для оптимальної оцінки моменту появи λ_0 по відношенню до квадратичної функції втрат. Позначимо через $\mu_n(t)=M_1\left(\lambda_0^n|y^t\right)$, $n\geq 1$, n-й апостеріорний момент величини $\lambda_0(\mathrm{M}_1\left(\bullet|y^t\right)$ – сподівання за умовною мірою

$$|P_1(S\,|\,y^t=P(\lambda_0\in \mathrm{S}\,|\,\theta=1,\ y^t)).$$

Використовуємо формулу Байєса отримуємо:

$$\mu_n(t)=\frac{\varphi_n(t)}{\Lambda(\mathrm{t})},\tag{8}$$

де $\varphi_n(t)=\int_0^\infty \lambda^n\gamma_\lambda(t)\,d\Pi(\lambda)$.

Введемо нормовану статистику

$$\overline{\varphi}_n(t)=\frac{\varphi_n(t)}{\beta_n(0)},$$

де $\beta_n(t)=\int_t^\infty \lambda^n d\Pi(\lambda)$.

Статистика $\varphi_n(t)$, очевидно, що може бути записана у вигляді:

$$\overline{\varphi}_n(t)=\int_0^\infty \gamma_\lambda(t)\,dP_n(\lambda),\tag{9}$$

де $P_n(\lambda)=\frac{1}{\beta_n(0)}\int_0^\lambda y^n d\Pi(y)$ - нормована до одиниці міри.

До статистики (9) при виконанні умови:

$$\int_0^t |A(u)|^2\,du<\infty, t<\infty\tag{10}$$

застосовні всі розмірковування [12], які привели до диференційного рівняння (7) для статистичних $\Lambda(\mathrm{t})$, якщо розподіл $\Pi(\lambda)$ замінити на розподіл $P_n(\lambda)$, то для $\overline{\varphi}_n(t)$ справджується вираз:

$$d\bar{\varphi}_{\text{n}}(t) = N^{-1}A(t)\left[\bar{\varphi}_{\text{n}}(t) - \int_0^{\infty} dP_n(\lambda)\right]dy(t), \quad t>0,\ \bar{\varphi}_{\text{n}}(0)=1.$$

Звідси слідує, що при виконанні умови (10) та при $\beta_n(0)<\infty$, статистика $\varphi_{\text{n}}(t)$ задовольняє стохастичне диференціальне рівняння:

$$\begin{gathered} d\varphi_{\text{n}}(t) = N^{-1}A(t)\left[\varphi_{\text{n}}(t) - \int_0^{\infty}\lambda^n d\Pi(\lambda)\right]dy(t), \quad t>0, \\ \varphi_{\text{n}}(0) = \int_0^{\infty}\lambda^n d\Pi(\lambda) \end{gathered} \tag{11}$$

Таким чином, n-й апостеріорний момент величини λ_0 визначається за допомогою співвідношень (7), (8) та (11). В частинному випадку, при виконанні умови:

$$\int_0^{\infty}\lambda^n d\Pi(\lambda)<\infty, \int_0^{\infty}\lambda^2 d\Pi(\lambda)<\infty,$$

оптимальною оцінкою моменту появи кібератак є апостеріорне середнє $\mu_1(t)$, яке знаходиться за допомогою (8) та (11) при $n=1$.

Розглянемо тепер випадок, коли атака з'являється з ймовірністю одиниці, π_0 =0. При цьому, з одиничною ймовірністю $\theta=1$ в (1) та (2) та $\gamma_\lambda(t)=\frac{dP_\lambda}{dP_\infty}(y^t)$, де $P_\lambda(\bullet)=P(\bullet|\lambda_0=\lambda)$ – міра, що відповідає процесу (2) при $\lambda_0=\lambda(\theta=1), P_\infty=P_\lambda$ при $\lambda=\infty$ (вінеровська міра).

Задача виявлення атаки в цьому випадку відрізняється від традиційної, тієї що розглянута раніше. У байєсовській постановці її слід трактувати як задачу оцінки моменту появи кібератаки, при втратах, рівних φ_0 *при* $\lambda\le t$ та $\text{C}(\text{t}-\lambda)$ *при* $\text{t}>\lambda$, де φ_0 - втрата при хибній тривозі; С- вартість затримки в виявленні кібератаки в одиницю часу.

Якщо задано обмеження на ймовірність хибної тривоги, тобто розглядається клас правил виявлення $\Delta(\alpha)$, таких що $P\left[\tau(u)<\lambda_0\right]\le\alpha$ (де Р- міра, що відповідає $(y(t)<\lambda_0)$, $t\ge 0$; $\tau(u)$- момент зупинки, який відповідає правилу $u(x)$, то задачу виявлення кібератак з випадковим моментом появи природньо трактувати як задачу якнайшвидшого виявлення збою процесу, що спостерігається, в класі $\Delta(\alpha)$. Іншими словами, бажано знайти таке послідовне правило $u^0(x)$, яке мінімізує $\text{M}(\tau(\text{u})-\lambda_0\,|\,\tau(\text{u})\ge\lambda_0)$ в класі $\Delta(\alpha)$.

Розглянемо правило

$$u_t^0 = \left[\pi(t)\right] = \begin{cases} 1,\ \pi(t)\ge B \\ 0, \pi(t)<B, t\le 0 \end{cases} \tag{12}$$

де $\pi(t)=\text{P}(\lambda_0\le\text{t}|\text{y}^\text{t})$ – апостеріорна ймовірність появи атаки (збою) в момент t; B - деяка константа. Тривалість правила (12) визначається співвідношенням:

$$\tau_0 = inf\left\{t\ge 0 : \pi(t)=B\right\} \tag{13}$$

Відмітимо, що $P(\tau_0 < \lambda_0) = \mathrm{M}\left[1 - \pi\left(\tau_0\right)\right]$ з (13) отримуємо $\mathrm{B} = 1 - \mathrm{P}(\tau_0 < \lambda_0)$. Тому при виборі порогу за формулою:

$$B = 1 - \alpha \tag{14}$$

забезпечуємо $P(\tau_0 < \lambda_0) = \alpha$ та, відповідно, приналежність правила (12) та (14) до шляху $\Delta(\alpha)$.

Очевидно, статистика буде:

$$\pi(t) = \frac{\left(\Lambda(t) - S_t\right)}{\Lambda(t)}. \tag{15}$$

Нехай S_t, $\Pi'(t) = d\Pi(t)/dt -$ неперервна функція. Тоді, застосовуючи до функції (15) формулу Винера-Хопфа с урахуванням (7) отримуємо, що $\pi(t)$ має стохастичний диференціал

$$\mathrm{d}\pi(\mathrm{t}) = \beta(t)(1 - \pi(\mathrm{t})\mathrm{dt} + N^{-1}A(t)\pi(\mathrm{t})(1 - \pi(\mathrm{t})\left(\mathrm{dy}(\mathrm{t}) - \mathrm{A}(\mathrm{t})\pi(\mathrm{t})\mathrm{dt}\right),$$
$$\mathrm{t} > 0, \pi(0) = \Pi(0),\ \partial e \beta(t) = \frac{\Pi'(t)}{S_t}. \tag{16}$$

Рівняння (16) узагальнює рівняння (4.149) [9] на випадок довільної детермінованої функції $A(t)$ і довільного неперервного розподілу моменту виявлення кібератаки.

В частинному випадку, при постійній атаці $A(t) = A, \mathrm{t} > 0$ показовому розподілі $\lambda_0\left(\Pi(\lambda) = 1 - \exp\left(-\beta\lambda\right)\right)$, тоді $\beta(\mathrm{t}) = \beta,\ \mathrm{t} > 0,$ рівняння (16) співпадає з (4.149) з [9].

При цьому $\left\{\pi(t), t \geq 0\right\}$ задається однорідним марковським процесом та правило (12), (14) строго оптимальні в класі $\Delta(u)$[14].

У більш загальному випадку, коли $A(t)$ змінюється з часом і розподіл $\Pi(\lambda)$ не є показовим, правила (12, 14) не оптимальні в класі $\Delta(\alpha)$. Якщо асимптотично при $\beta \to 0$ вимоги показовості не грає суттєвої ролі, то вимога сталості $A(t)$ при $t > 0$ виявляється доволі обмеженою з практичної точки зору.

За аналогією з [5] побудуємо модифікацію правила (12), котра оптимальна без введення апріорного розподілу моменту збою. Нехай $\lambda \in [0,\ \infty]$ – невідомий момент збою, про властивості якого не робиться ніяких апріорних припущень. Будемо вважати, що в (2) $A(t) = 0$ при $t \geq 0,$ тобто задача полягає у виявлені зміни постійного коефіцієнту зносу винеровського процесу. Введемо наступні позначення: M_λ – математичне сподівання по мірі R_λ, яка відповідає процесу (2) при $\lambda_0 = \lambda(P_\infty -$ вінеровська міра, що відповідає (2) при відсутності збою; ΔT - клас послідовних правил $u(x)$, таких що $M_\infty \tau(u) \geq T,\ T \in [0, \infty];\ \tau_\lambda(u) = M_\lambda(\tau(\mathrm{u}) - \lambda \mid \tau(\mathrm{u}) \geq \lambda)$ - середній час запізнення у виявленні збою при умові, що збій відбувся в момент λ. Бажано забезпечити $\overline{\tau}_\lambda$ як можна менше в класі $\Delta(T)$, тобто серед правил, в яких середній час до хибної тривоги не менше заданої величини T. Оскільки правила, що

мінімізує τ_λ при всіх $\lambda \geq 0$, не існує, природньо спробуємо знайти мінімаксне правило, яке забезпечує мінімум $\mathrm{E}(\mathrm{u}) = \sup \tau_\lambda(u)$ *в класі* $\Delta(T)$. Перейдемо в (12) від статистики $\pi(t)$ до статистики $\varphi(t) = \dfrac{\pi(t)}{\left[1-\pi(t)\right]}$.

Якщо в якості апріорного розподілу виступає показникове, то нескладно переконатись:

$$\varphi(t) = \beta \int_0^t \gamma_\lambda(t) \exp(-\beta(\lambda - t) d\lambda \tag{17}$$

Позначаючи $L(t) = \dfrac{\varphi(t)}{\beta}$, при $\beta \to 0$ з (17) отримаємо:

$$L(t) = \int_0^t \gamma_\lambda(t) d\lambda = \int_0^t \exp\left\{\frac{a}{N}(y(t) - y(\lambda)\right\} - \frac{a^2}{2N}(t-\lambda) \tag{18}$$

При цьому правило (12) еквівалентно правилу:

$$u_t^0\left(L(t)\right) = \begin{Bmatrix} 1,\ L(t) \geq b \\ 0, L(t) < b, t \geq 0 \end{Bmatrix} \tag{19}$$

де $b = \lim\limits_{\beta \to 0} \dfrac{B}{(1-B)\beta}$

Таки чином , якщо $B \to 0$, $\beta \to 0$ так , що $b = const$, то (19) є границею байєсовського правила (12). В інтерпретації [5], придатної для задач контролю систем, це означає, що періодично, але дуже зрідка виникають збої, ймовірність хибної тривоги наближається до 1 (див. 14). Отже $\dfrac{(1-\alpha)}{\beta} = b < \infty$, причому після оголошення наявності збою відбувається перевірка її справжнього стану та процес відновлюється [10]. Позначимо через $\bar{E}(\alpha, \beta) = M(\tau_0 - \lambda_0 \mid \tau_0 \geq \lambda_0)$ середнє запізнення у виявленні виявлення кібератаки в правилах (12), (14) (M - сподівання за мірою P, породженою вектором $\left[y(t), \lambda_0\right]$. З наведених суджень слідує, що при $\alpha \to 1$, $\beta \to 0$ значення $\bar{E}(\alpha, \beta)$ співпадає з середнім значенням з правила (19) і, як показано в [5], при $b \to \infty$ визначається рівністю

$$\bar{E}(b) = \frac{1}{q}\left\{\ln(qb) - 1 - Э + G\left(\frac{1}{qb}\right)\right\}, \tag{20}$$

де $\mathrm{q} = a^2 / 2N; Э = 0.577$ константа Ейлера, G – коефіцієнт, що характеризує складність задачі, яка розв'язується. Будемо вважати, що b в (19) обирається виходячи із заданого допустимого часу за хибною тривогою T. При цьому процес спостереження може відновитись після прийняття рішення про наявність збою або його відсутності в залежності від конкретної розв'язуваної задачі, що розв'язується.

Оскільки $\gamma_\lambda(t)$ являться мартингалом для $t \geq \lambda$, то процес $L(t)-t,\ t \geq 0,$ також є мартингалом з нульовим середнім (відносно міри P_∞) й, зрозуміло, для будь-якого обмеженого марківського моменту $M_\infty L(\tau) = M_\infty \tau$. Так як, крім того, для моменту зупинки:

$$\tau_0 = inf\left\{t : L(t) = b\right\} \tag{21}$$

справджується рівність $L(\tau_0) = b$, $mo\, M_\infty \tau_0 = b.$ Таким чином, при виборі

$$b = T \tag{22}$$

забезпечується рівність $M_\infty \tau_0 = T$ і тому правило (19), (22) належать до класу $\Delta(T)$.

Детальний аналіз правила (19) та (22), а також його порівняння з правилом Пейджа, яке засноване на порівнянні статистики

$$\tilde{L}(t) = \frac{a}{N}\left\{y(t) - \frac{a}{2N}t - \min_{\lambda \leq t}\left[y(\lambda) - \frac{a}{2N}\lambda\right]\right\}$$

З порогом b_t, визначеним для забезпечення $M_\infty \tau = T$ (r – момент зупинки, що відповідає цьому правилу) з рівняння $\frac{1}{2}qT = \exp(b_t) - b_t - 1$, наведені в [15]. Використовуючи результати цієї роботи можна показати, що для $E(u^0) = \sup_{\lambda \geq 0} \tau_\lambda(u^0)$ правила (19) та (22) справджується рівність:

$$E(u^0) = q^{-1}\left\{\ln(qT) - Э + G\left(\frac{\ln(qT)}{qT}\right)\right\}\ T \to \infty, \tag{23}$$

Більш того, в [15] отримані асимптотичні рівності для τ_λ правила Ширяєва (19) та (22), та правила Пейджа у випадку, коли зміни коефіцієнта зсуву процесу відбувається на величину μ, ої відрізняється від a, на яку «налаштовані» ці правила. Аналіз показує, що при $\mu = a$ середнє затримки у виявленні збою у вказаних правилах практично однакові, при $\mu > a$ правило Пейджа дещо краще, а при $\mu < a$ виграє правило Ширяєва. Якщо використовувати розклад для середньої затримки виявлення для правила, заснованого на порівнянні статистики, що отримується усередненням $L(t)$ за деякою мірою на множині значень a, яке пристосоване для випадку невідомого значення a, то аналіз виявив, що останнє правило є асимптотично оптимальним за першим порядком, в той час як правила Пейджера та Ширяєва все не є актуальними при збільшенні a.

Порівняння (23) та (20) свідчить про те, що головні члени асимпотичних розкладів для середньої затримки $\bar{E}(u^o)$ та максимальної затримки $\bar{E}(u^o)$ співпадають. Це дає підстави покладати, що правило Ширяєва (19) та (22) є асимтотичномінімаксним (у сенсі першого порядку) при $T \to \infty$ в класі $\Delta(T)$, хоча і не є строго мінімаксним в цьому класі. Останнє витікає з тих же міркувань, що й для дискретного часу [13].

Можна «відредагувати» статистику $L(t)$ шляхом рандомізації в момент $t=0$ так, щоб правило (19) опинилося мінімаксним при всіх $T>0$.

Статистика (18), як нескладно показати, за допомогою формули Винера-Хопфа, має стохастичний диференціал:

$$dL(t)=dt+L(t)\frac{a}{N}dy(t),\ L(0)=0 \tag{24}$$

Введемо статистику $L^*(t)$, яка задовольняє стохастичному рівняння (24) з початковою умовою $L^*(0)=z\in[0,bt]$, де z – випадкова величина з розподілом $(y)=P(z\le y)$, зосередженим на інтервалі $[0,b_m]$, таким, що розподіл $P_\infty\left(L^*(t)\le y\middle|\tau^*\right\rangle t)$ не залежить від t. Тут $t^*=inf\left\{t: L^*(t)=b_t\right\}$ - момент зупинки, який відповідає правилу $u^*(x)$, що співпадає з правилом (19) при заміні $L(t)$ на $L^*(t)$. Тоді $\overline{\tau_\lambda^*}(y)=M_\lambda(\tau^*-\lambda)r^*>\lambda,\ L^*(\lambda)=y)$ *не* залежить від λ, так як на множині $\{\tau^*>\lambda\}$ для будь – якого $\lambda\ge 0$ умови однакові, якщо фіксується $L^*(\lambda)$. Тому середній час запізнення можна записати так: $\overline{r_\lambda}(u^*)=\int_0^{bt}r_\lambda(y)\,d\psi_m(y)=E(u^*)$ також не належить від λ і правило $u^*(x)$ являється мінімальним.

Для забезпечення приналежності правила $u^*(x)$ класу $\Delta(T)$, *більш точно*, *для виконання умови* $M_\infty\tau^*=T$, поріг b_t необхідно обирати за формулою:

$$b_t=T+M_\infty L^*(0) \tag{25}$$

Це випливає з мартингальних властивостей статистики $L^*(t)-t$, в силу яких $M_\infty\left(L^*(\tau^*)-\tau^*\right)=M_\infty L^*(0)$, і тієї обставини, що $L^*(\tau^*)=b_t$. Знаходження необхідного розподілу $\psi_m(y)$ і, відповідно, порогу b_t при довільному значенню T, не є можливим. Однак цю задачу можна розв'язати при великих значеннях T.

Дійсно, якщо $T\to\infty$, то в якості розподілу $P_\infty(L(\infty)\le y)$ марківського процесу $L(t)(t\to\infty)$, що задовольняє (24) при $y(t)=\sqrt{N}\,\omega(t)$. Можна показати, що це розподіл

$$\psi_m(y)=\exp\left(-\frac{1}{qy}\right),\ y\in(0,\infty) \tag{26}$$

Використовуючи (26), знаходимо

$$M_\infty L^*(0)=\exp\left(\frac{1}{qb_t}\right)\int_{(qbt)^{-1}}^{\infty}y^{-1}\exp(-y)\,dy=\frac{1}{q}E_1\left(\frac{1}{qb_t}\right)\exp\left(\frac{1}{qb_t}\right) \tag{27}$$

де $E_1(x)$ – інтегральна показникова функція.

При $b_t \to \infty$ з (27) маємо

$$M_\infty L^*(0) = \frac{1}{q}\left\{ lnqb_t - Э + G\left(\frac{1}{qb_t}\right)\right\} \tag{28}$$

З (25) та (28) слідує, що при великих значення Т поріг b_t є розв'язком транспортного рівняння

$$b_t = T + \frac{1}{q} lnqb_t \tag{29}$$

Оскільки в якості розподілу початкового значення $L^*(0)$ при великих Т наступає стаціонарний розподіл $\{L(t)\}$, то зрозуміло, що для $\mathrm{E}(u^*)$ справджується розклад (20) при заміні b на b_t;

$$\mathrm{E}(\mathrm{u}^*) = \frac{1}{\mathrm{q}}\left[\ln(\mathrm{qb_t}) - 1 - Э + \mathrm{G}\left(\frac{1}{\mathrm{qb_t}}\right)\right] \quad T \to \infty \tag{30}$$

Якщо покласти $b_t = T + \frac{1}{\mathrm{q}}$ lnqT, то в силу (28) та (30) маємо

$$\mathrm{M}_\infty \tau^* = \mathrm{T} + \frac{1}{\mathrm{q}}\mathrm{lngT} - \frac{1}{\mathrm{g}}\ln(\mathrm{qT} + \mathrm{lngT}) = \mathrm{T} - \mathrm{G}\left(\frac{\mathrm{lnT}}{\mathrm{T}}\right),\ T \to \infty \tag{31}$$

$$E(u^*) = \frac{1}{q}\left\{ \ln(qT) - 1 - Э + G\left(\frac{lnqT}{qT}\right)\right\},\ T \to \infty \tag{32}$$

Висновки

Таким чином з (31) та (32) слідує, що $u^*(x)$ «майже», належить класу ΔT, та головний член асимтотичного розкладу максимального за λ значення ризику дорівнює аналогічному головному члену асимптотичного розкладу ризику правилі (19). Звідси випливає, що обидва правила асимтотично мінімаксні в сенсі першого порядку.

Список літератури

1. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки. Житомир: ЖНАЕУ, 2016. 636 с.
2. Brailovskyi N., Kozura V., Kondakova S., Khoroshko V. Analysis of the Cyber security Status of the Information Space. *Scientific and Practical Cyber Security Journal*, V2, №4, 2018. P. 64-74.
3. Іванченко І.С., Хорошко В.О. Інформаційне протиборство в геополітичному просторі. *Сучасна спеціальна техніка*, 2019. №3 (58), С. 26-37.
4. Пирцхалава Л.Г., Хорошко В.А., Хохлачова Ю.Е., Шелест М.Е. Информационное противоборство в современных условиях. К.: ЦП "КОМПРИНТ", 2019. 226 с.
5. Опірський І.Р. Загальні проблеми прогнозування НСД в інформаційних системах держави. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, 2015. Вип. 2(30). С. 31-34.
6. Козюра В.Д., Ткач Ю.М., Шелест М.Є., Козюра В.Д. та ін. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах. Ніжин : ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. 144 с.
7. Козюра В.Д., Ткач Ю.М., Шелест М.Є. та ін. Захист інформації в комп'ютерних системах. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. 236 с.
8. Закс Ш. Теория статистических выводов. М: Мир, 1995. 776с.
9. Ширяев А.Н. Статистический последовательный анализ. Оптимальные правила остановки. М.: Наука, 1999. 272с.
10. Креденцер Б.П., Миночкин А.И., Могилевич Д.И. Оценка эксплуатационно-технических характеристик объектов телекоммуникаций при априорной неопределенности. К.: Феникс, 2012. 336с.
11. Кокс Д., Льюис П. Статистический анализ последовательностей событий. М.: Мир, 1999. 312 с.
12. Опірський І.Р. Оптимізація послідовних процесів прийняття рішень при умовно екстремальній постановці задачі. *Інформаційна безпека*, 2014. №4(16). С. 120-127.
13. Опірський І.Р. Проблематика основного постулату прогнозування НСД. *Сучасна спеціальна техніка*.2015. №2(41). С. 3-8.
14. Дудикевич В.Б., Опірський І.Р., Гаренюк П.І., Ваврічен О.А. Оптимальність не усеченної процедури Вальда в задачах перевірки двох простих прогнозів НСД в інформаціних мережах держави. *Інформатика та математичні моделі в моделюванні*. 2016. Т.6, №3. С. 215-226.
15. Pollak M., Siegmund D. A Diffusion Process and Its Applications to Detecting a Change in the Drift of Brownian Motion. *Biometrika.* 1995. V.72, №2. P.267-280.

CYBER ATTACKS DETECTION IN INFORMATION NETWORKS

I.R. Opirsky[1], Y.M. Tkach[2], V.O. Khoroshko[3]

[1]National University "Lvivska Politechnika",
Ukraine, Lviv, 79013, ul. S. Banderi, 12, e-mail: iopirsky@gmail.com
[2]National University "Chernigivska Politechnika",
Ukraine, Chernigiv, 14035, ul. Shevchenko, 95, e-mail: tkach_ym@ukr.net
[3]National Aviation University, 03058,
Ukraine, Kiyiv, prosp. Lyubomyr Guzara, 1, e-mail: professor_va@ukr.net

Cyber security is becoming increasingly important in ensuring the national security of various countries. Cyber attacks and cyber influences are increasingly becoming one of the main actions to achieve the goal of control over various objects (person, organization, region, state, etc.) in the modern world. Thus, a new phenomenon in international politics has emerged in the world - the ability to achieve their own political goals, economic and spiritual subordination of the peoples of other states without the use of military force. Therefore, cyber attacks and cyber influences are developing quite actively in the world. Therefore, for the effective operation of modern information and telecommunication networks and means of their protection, as well as for the reliable detection and prediction of cyber attacks and unauthorized actions, it is necessary to develop new approaches and methods of cyber security. The purpose of the article is to detect cyber attacks in information networks. The problem of detecting a cyber-attack A (t) against the background of white Gaussian noise V (t) under the condition of continuous observation time is considered. The theoretical substantiation of the averaged forecasting object (AOP) is given. A consistent analysis of UOP in the general case revealed that it is not a sufficient statistic in the problem of sequential detection of cyber attacks. From the above it follows that one of the main issues in the synthesis of optimal sequential and inconsistent detector of cyber attacks with random moments of occurrence is to find algorithms for the formation of UOP. As a result of the conducted researches the technique of detection of NSD with the unknown moment of occurrence in discrete time of supervision is offered.
Keywords: information systems, cyber-attack, averaging about forecasting.