УДК 004.056.53:005.004.7
DOI: 10.25140/2411-5363-2021-1(23)-96-102

Володимир Хорошко, Михайло Шелест, Юлія Ткач

ВИЯВЛЕННЯ ТА ОЦІНЮВАННЯ КІБЕРАТАК В ІНФОРМАЦІЙНИХ МЕРЕЖАХ ІЗ ВИПАДКОВИМ МОМЕНТОМ ПОЯВИ

На основі ймовірнісної оцінки в роботі розкриті оптимальні, послідовні або близькі до них процедури, що дозволяють підвищити кібербезпеку інформації. Розв'язана задача, яка полягала в побудові оптимальної N-усіченої послідовної процедури спільного виявлення кібератак (КА) та оцінки моменту її появи при функції втрат. Проаналізована статистика, пов'язана з усередненим обсягом прогнозу (УОП). Запропоновано загальний вигляд оптимальної процедури послідовного виявлення-оцінювання КА з невідомим моментом появи при зазначених втратах.

Ключові слова: *кібератака, інформаційні мережі, кібервплив, кібербезпека.*
Бібл.: 11.

Актуальність теми дослідження. При розгляді проблеми кібербезпеки інформації необхідно враховувати можливі види несанкціонованих дій (кібератак), які ведуть до втрати або модифікації даних. Виявлення, запобігання або істотне ускладнення дії кібератак (КА) - один із центральних напрямів галузі кібербезпеки в інформаційних мережах. Визначення узагальнених вимог із кіберзахисту інформаційних мереж від кібератак на інформацію та оцінка ступеня їх захищеності є досить складними задачами. Досвід практичної експлуатації інформаційних мереж у різних сферах діяльності держави показує, що існують реальні загрози КА, що призводять до негативного впливу на складові кібербезпеки.

Постановка проблеми. Існують реальні можливості виникнення непередбачених ситуацій внаслідок впливу КА, що ведуть до втрати інформації або до втрати працездатності інформаційної мережі. У концепції кібербезпеки інформаційної мережі на основі загроз від КА повинні визначатися необхідні кошти, методи та процедури виявлення і оцінювання КА в мережах.

Має місце процес розмежування різних видів загроз. При цьому необхідність розуміння ролі КА і кібербезпеки пов'язана в першу чергу з активізацією міжнародних терористичних, екстремістських організацій і злочинних угруповань, а також окремих держав, які здійснюють кібератаки і кібервпливи на громадян, суспільство й держави з метою реалізації своїх інтересів.

При цьому в умовах ведення гібридних війн в останні роки систематично здійснюються різні КА, кібервпливи і несанкціоновані дії в інформаційних мережах, що підриває економічну, військову, технічну та інші сфери держави.

Тому, для ефективного функціонування інформаційних мереж у сучасних умовах і засобів їх захисту, а також для надійного виявлення і оцінювання КА необхідно розвивати нові підходи і методи, їх реалізації.

Аналіз останніх досліджень та публікацій. У сучасних дослідженнях значне місце посідають дослідження, присвячені виявленню та оцінюванню кібератак в інформаційних мережах. Так, у статті [12] розглядаються особливості застосування випадкової нейронної мережі для виявлення легких атак в IoT. Виявлення аномалій у великомасштабних кібератаках за допомогою нечітких нейронних мереж досліджувались у [13]. Деякі результати, пов'язані зі спільним послідовним виявленням і оцінюванням, отримані в [3]. З результатів роботи [3] можна зробити висновок, що в загальному випадку знайти конструктивне рішення не вдається навіть у двохальтернативній задачі. Тому спробуємо вирішити цю задачу багатоальтернативного послідовного виявлення і оцінювання кібератаки з випадковим моментом її появи. Втрати в процесі розпізнання (виявлення) та оцінювання кібератаки залежать як від помилок в її виявленні, так і від неточності оцінювання, що не дозволить забезпечити адекватну протидію, і при цьому виникає задача спільного розвитку й оцінювання [1; 2].

Виділення недосліджених частин загальної проблеми. При виявленні й розпізнаванні кібератак зазвичай цікавляться не тільки фактом появи тієї чи іншої атаки, але й її інформативними параметрами. Результат дій, що виконуються при вирішенні задачі про наявність кібератаки, залежить від ступеня близькості оцінки до істинного значення параметрів. Причому на практиці момент прийняття рішення зазвичай не байдужий, оскільки зі збільшенням часу спостереження, витрати зростають і бажано якнайшвидше прийняття рішень. При цьому послідовні процедури виявлення-оцінювання, взагалі кажучи, мають більшу ефективність у порівнянні з непослідовними. Тому важливим та нагальним є пошук оптимальних, послідовних або близьких до них процедур, що дозволить підвищити кібербезпеку інформації.

Мета статті полягає у знаходженні оптимальних, послідовних або близьких до них процедур, що дозволить підвищити кібербезпеку інформації.

Виклад основного матеріалу. Нехай подія $\{\theta = 1\}$ означає наявність кібератаки (КА), яка може з'явитись в момент $\infty > \lambda_n = \lambda_0 > 0$, n ≥ 1, причому $\pi_{01} = P(\theta = 1) = P(\lambda_0 < \infty) < 1$ $(\pi_{00} = P(\theta = 0) = P(\lambda_0 = \infty) = 1 - \pi_{01})$. Припустимо, що $x_n,\ n \geq 1$, незалежні як і до так і після появи КА, так що справедлива модель [2]:

$$P_0(x_1^n) = p(x_1^n|\theta = 0) = \prod_{i=1}^{n} p_{oi}(x_i) = p(x_1^n|\theta = 1, \lambda_0 > n\Delta);$$

$$p_{11}(x_1^n|\lambda) = p(x_1^n|\theta = 1, \lambda_0 = \lambda) = \prod_{i=1}^{n} x_{oi}(x_i) P_{\lambda j+1}(x_{j+1}) \prod_{i=j+2}^{n} P_{1i}(x_i),$$

$j\Delta \leq \lambda \leq (j+1)\Delta, j \leq n-1, n = 1, N$, де $P_{\lambda n}(x_n)$ – щільність, що залежить від λ причому

$$P_{\lambda n}(x_n) = \begin{cases} P_{0n}(x_n) \text{ при } \lambda = n\Delta, \\ P_{1n}(x_n) \text{ при } \lambda = (n-1)\Delta; \end{cases}$$

Прийнята при розгляді у [4] задача виявлення збою послідовності без оцінки його моменту.

Задача полягає в побудові оптимальної N-усіченої послідовної процедури спільного виявлення КА та оцінки моменту її появи при функції втрат:

$$g(\theta, \lambda, u_n, n) = \begin{cases} g_{01}(n), \theta = 0,\ u_n = (1, \lambda_n), \\ \widetilde{g_{11}}(n)\ \theta = 1, \lambda \geq n\Delta, u_n = \left(1, \hat{\lambda}_n\right), \\ g_{11}(n) + c(n - [\lambda]) + F_n\left(\lambda - \hat{\lambda}_n\right)^2, \theta = 1, \\ \lambda < n\Delta, u_n = \left(1, \hat{\lambda}_n\right), n = \overline{1, N} \end{cases} \quad (1)$$

де c – вартість затримки в обчисленні розв'язку про наявність КА та її появи за один крок; $[\lambda] = i$ при $(i-1)\Delta < \lambda \leq i\Delta$ (i – інтервал між відліками).

Розв'язок $u_n = 0$ на кроках n=1, N-1 еквівалентно за розв'язком u_n про продовження спостережень [4]. На N-му кроці цей розв'язок є остаточним, оскільки процес $\{x_n\}$ спостереженню більше недоступний і втрати $g(\theta, \lambda, u_n = 0, N)$ пов'язані та мають вигляд:

$$g(\theta, \lambda, u_n, N) = \begin{cases} g_{00}(N), \theta = 0,\ u_n = 0, \\ g_{10}(N) + c(N - [\lambda]), \theta = 1, \lambda < N\Delta, u_n = 0, \\ \tilde{g}_{10}(N)\ \theta = 1, \lambda \geq N\Delta, u_n = 0. \end{cases} \quad (2)$$

Функція втрат (1), (2) відрізняється від [4]

$$g_{ij}\left(\lambda_n^{(i)}, \hat{\lambda}_n^{(j)} n\right) = \begin{cases} g_{ii}(n) + w_n\left(\lambda_n^{(i)} - \lambda_n^{(j)}\right) \text{ при } i,j \neq 0, \\ g_{j0}(n) \text{при } i = 0, j = \overline{0, m-1}, \\ g_{i0}(n) \text{ при } j = 0, i = \overline{0, m-1}, \end{cases} \quad (3)$$

де w_n – неспадна невід'ємна функція, що визначає залежність втрат від неточності оцінювання інформаційного параметру, яка не залежить від номерів гіпотез, що приймаються, та істинної гіпотези. Відрізняється тим, що від значень інформаційного параметру залежить не тільки втрати за рахунок неточності їх оцінювання, але і сама величина $g_{ij}(n, \lambda)$.

Наприклад,

$$g_{11}(n, \lambda) = g_{11}(n) + c(n - [\lambda]) \quad (4)$$

при $\lambda \leq n\Delta$, $g_{11}(n, \lambda) = \widetilde{g_{01}}(n)$ при $\lambda > n\Delta$.

У частинному випадку, коли $C = 0, g_{11}(n) = \widetilde{g_{11}}(n), g_{10}(N) = \tilde{g}_{10}(N)$ (4) втрати (1), (2), (3) співпадають та можна скористатись результатами, що отримуються в [5]. Використовуючи (1), неважко показати, що оптимальна оцінка відрізняється від результатів, отриманих в [5]. Вона являє собою середній апостеріорний розподіл $P(\lambda_0 \leq \lambda | x_1^n, \theta = 1, \lambda \leq n\Delta)$ з щільністю $\widetilde{p_{01}}(\lambda) = p_1(x_1^n|\lambda)p(\lambda)/[\int_0^{-n\Delta} p_1(x_1^n|\lambda)p(\lambda)d\lambda], \lambda \leq n\Delta$, $p(\lambda)$-щільність апріорного розподілу $\prod(\lambda) = P_0(\lambda_0 \leq \lambda | \theta = 1)$, тобто $\widetilde{\lambda_n^0} = \int_0^{n\Delta} \lambda \widetilde{p_{01}}(\lambda)d\lambda$ оскільки

$$w_n\left(\lambda - \widehat{\lambda_n}\right) = \begin{cases} F_n\left(\lambda - \widehat{\lambda_n}\right)^2, \lambda < n\Delta \\ 0, \lambda \geq n\Delta \end{cases} \quad (5)$$

Введемо позначення: $m_n^{(i)}(x_1^n) = M\left[\lambda_0^i \middle| x_1^n, \theta = 1, \lambda_0 \leq n\Delta\right], i \geq 1;$

$D_n(x_1^n) = M[\left(\lambda_0 - m_n^{(i)}\right)^2 | x_1^n, \theta = 1, \lambda_0 \leq n\Delta]$ – і-й нецентральний момент та дисперсія апостеріорного розподілу (5); $L_n(x_1^n)$ – статистика, пов'язана з усередненим обсягом прогнозу (УОП)

$$(x_1^n) = \int_0^{\infty} [p_1(n_1^n|\lambda)/p_0(x_1^n)]\, p(\lambda)d\lambda \quad (6)$$

Використовуючи (2), можна показати [6], що для $\{m_n^{(i)}\}$ справджуються рекурентні рівності.

$$m_{n+1}^{(i)} = L_n L_{n+1}^{-1}\left\{\gamma_{n+1}(x_{n+1})m_n^{(i)} + \frac{\nu_{n+1}^{(i)}}{L_n}\right], n \geq 0, m_0^{(i)} = 0, i \geq 1 \quad (7)$$

Тут $\gamma_n(x_n) = \frac{p_{1n}(x_n)}{p_{0n}(x_n)}$ статистика L_n задовольняє рекурентне співвідношення [3]:

$$L_{n+1} = \beta_{n+1}(x_{n+1}) + \gamma_{n+1}(x_{n+1})L_n, n \geq 0, L_0 = 0$$

Отже, $\nu_n^{(i)}(x_n) = \int_{(n-1)\Delta}^{n\Delta} \lambda^i \frac{p_{\lambda n}(x_n)}{p_{0n}(x_n)} p(\lambda)d\lambda, i \geq 0$ причому $\nu_n^0(x_n) = \beta_n(x_n)$.

При i = 1 співвідношення (7) задає алгоритм формування оптимальної оцінки моменту виявлення КА (6), при i = 2 – другого апостеріорного моменту. Також згідно з рівністю:

$$D_n(x_1^n) = m_n^{(2)}(x_1^n) - [m_n^{(1)}(x_1^n)] \quad (8)$$

та за допомогою (7) і рекомендацій [3] визначається апостеріорна дисперсія, а отже

$$\varphi^0(x_1^n, n) = F_n D_n(x_1^n) \quad (9)$$

Якщо збій послідовності при виявленні КА відбувається, то

$$P_{\lambda n}(x_n) = p_{1n}(x_n) \text{ для всіх } \lambda \in [(n-1)\Delta, n\Delta], \quad (10)$$

або КА може з'явитись лише в дискретні моменти $n\Delta, n = 0,1,2 \ldots$

$p(\lambda) = p_n\delta(\lambda - n\Delta)$, $(\sum_{n\geq 0} p_n = 1)$, то $\nu_{n+1}^{(i)} = \alpha_{n+1}^{(i)}\gamma_{n+1}(x_{n+1})$ та з [3], (7) слідує, що

$$m_{n+1}^{(i)} = L_n(\alpha_{n+1}^0 + L_n)^{-1}\left(m_n^{(i)} + \frac{\alpha_{n+1}^{(i)}}{L_n}\right), n \geq 0, m_0^{(i)} = 0, i \geq 1 \quad (12)$$

де $\alpha_{n+1}^{(i)} = \int_{n\Delta}^{(n+1)} \lambda^i\, p(\lambda)d\lambda;\ \alpha_{n+1}^{(0)} = \alpha_{n+1}$.

З (12) слідує, що значення будь-якого моменту апостеріорного розподілу (5) на $(n+1)$-му кроці при виконанні (10) або (11) залежить лише від n спостережень, причому $(L_n, m_n^{(i)})$:

$$m_n^{(i)}(x_1^{n+1}) = m_{n+1}^{(i)}(x_{n+1}) = m_{n+1}^{(i)}(L_n, m_n^{(i)}) \quad (13)$$

У більш загальному випадку вирази (7), (8) [3] можемо записати:

$$m_n^{(i)}(x_1^{n+1}) = m_{n+1}^{(i)}\left(x_{n+1}, m_n^{(i)}, L_n\right), i \geq 1 \quad (14)$$

$$D_{n+1}(x_1^{n+1}) = D_{n+1}(S_{n+1}) = D_{n11}(x_n, x_{n+1}), \quad (15)$$

де $S_n = \left(m_n^{(1)}, m_n^{(2)}\right)$; $Z_n = (L_n, S_n)$,

де Z_n–транзитивна статистика

$$Z_{n+1}(x_1^{n+1}) = Z_{n+1}(x_{n+1}, Z_n), n \geq 0 \quad (16)$$

Статистика π_n пов'язана з L_n рівністю

$$\pi_n = \frac{\nu(L_n + A_n)}{[1+\nu(L_n+A_n)]}, \quad (17)$$

$A_n = P(\lambda_0 \geq n\Delta|\theta = 1)$, $\nu = \frac{\pi_{01}}{1-\pi_{01}}$. З (14), (16), (17) слідує, що умови, які прийняті в [7] виконані, причому $T_n = Z_n = (L_n, S_n)$, $S_n = (m_n^{(1)}, m_n^{(2)})$, $S_{n+1} = S_{n+1}(x_{n+1}, Z_n)$.

Таким чином, можна скористатись твердженням, що послідовність $\{Z_n, n = 1, n\}$ є достатньою, а оптимальна процедура послідовного виявлення-оцінювання має вигляд наведений у [9], де T=Z_n – трьохмірна статистика відповідно (9), (15), причому у відповідності с висновками у [8] $V_{n0}^N = V_{nn}^N, n = 1,\ N = 1$.

У тому випадку, коли (4) не виконано, безпосередньо застосувати теорему 2 з [8] неможливо та задача дещо ускладнюється, однак трьохмірна статистика $Z_n = (L_n, m_n^{(1)}, m_n^{(2)})$ залишається достовірною і в цьому випадку. Дійсно, використовуючи (1) та (17), неважко показати, що

$$R_{n1}\left(x_1^n, \widehat{\lambda_n^0}\right) = \Gamma_{n1}(Z_n) = \mathrm{c}\sum_{i=1}^n \widetilde{\pi_{in}}, \quad (18)$$

де $\Gamma_{n1}(Z_n) = (1 + \nu \wedge_n)^{-1}\{\nu L_n[g_{11}(n) + + F_n D_n(S_n)] + g_{01}(n) + \nu \mathrm{A}_n\widetilde{g_{11}}(n)\}$; (19)

$\pi_{in} = P(\lambda_0 < i\Delta|x_1^n)$ – апостеріорна ймовірність наявності КА та моменту $i\Delta$.

Апостеріорний ризик $R_{No}(x_1^N)$ визначається рівністю з [10]. За допомогою (18), (19) та рекомендацій [10] отримуємо, що оптимальна процедура на N-му кроці має вигляд:

$$u_N^0(Z_n) = \begin{cases} 1, m_N^{(i)}, L_n \geq L_N^0(D_N) \\ 0, L_n \geq L_N^0(D_N) \end{cases}$$

де L_n, $m_N^{(i)}$, D_N – находяться у відповідності з (8) та (9), а $L_N^0(D_N)$ - поріг, що залежить від апостеріорної точності оцінювання моменту появи КА λ_0:

$$L_N^0(D_N) = \frac{\nu \mathrm{A}_n[\widetilde{g_{11}}(N) - \widetilde{g_{10}}(N) + g_{01}(N) - g_{00}(N)]}{\nu[g_{10}(N) - g_{11}(N) - F_N D_N(S_N)]} \quad (20)$$

Наступні результати отримуємо для випадку стрибкоподібного збою послідовності при появі КА, коли виконується умова (10), або для випадку дискретного розподілу моментуλ_0 (11). При цьому, як слідує з (13)

$$D_{n+1}(x_0^{n+1}) = D_{n+1}[Z_n(x_1^n)], n \geq 0, \quad (21)$$

де Z_n – транзитна статистика.

Використовуючи (19) – (21), (16), (18), аналогічно [4], можна показати, що найменший апостеріорний ризик (НАР) в області продовження спостережень $V_{n0}^N = V_{n1}^N = [R_{n0}^N(x_1^n) \le R_{n0}(x_1^n)]$ має вигляд:

$$R_{n0}^N(x_1^n) = \tilde{\Gamma}_{n0}^N(Z_n) + \sum_{i=1}^n \tilde{\pi}_{in}, \tag{22}$$

де $\tilde{\Gamma}_{n0}^N(Z_n) = \Gamma_{n0}^N(Z_n) + \sum_{V=1}^{N-n} \frac{D_n^{(V)}(Z_n,N)}{1+v\wedge_n}$, (23)

Величини $D_n^{(V)}$ визначаються рекурентно у відповідності з рівняннями

$$D_n^{(V)}(Z_n,N) = \int D_{n+1}^{(V)-1}[Z_{n+1}(x_{n+1}Z_n),N]\ p_{0n+1}(x_n+1)dx_{n+1}, v \ge 2, \tag{24}$$

$$D_n^{(1)}(Z_n,N) = F_{n+1}D_{n+1}(Z_n,n,N)v(L_n+\alpha_{n+1}). \tag{25}$$

Функція Γ_{n0}^N визначається за допомогою [11], в яких L_n заміняється Z_n, так як області

$$X_{n+1}^0(Z_n,N) = [x_{n+1}: \tilde{\Gamma}_{n+10}^N(Z_{n+1}) \le \tilde{\Gamma}_{n+11}^N(Z_{n+1})]; \tag{26}$$
$$X_{n+1}^1(Z_n,N) = [x_{n+1}: \tilde{\Gamma}_{n+10}^N(Z_{n+1}) > \tilde{\Gamma}_{n+11}^N(Z_{n+1})]$$

залежать не тільки від L_n, але і від $m_n^{(1)}, m_n^{(2)}$ з виразів (18) та (22) слідує, що оптимальна процедура послідовного виявлення-оцінювання КА з невідомим моментом появи при втратах (1) у загальному випадку при невиконанні умов (4) має вигляд:

$$u_N^0(Z_n) = \begin{cases} 1, m_N^{(i)}, Z_n \in V_{n1}^N \\ 0, Z_n \notin V_{n1}^N, n = 1,N \end{cases} \tag{27}$$

де V_{n1}^N - область зупинки спостережень:

$$V_{n1}^N = [Z_n: \Gamma_{n1}(Z_n) \le F_{n0}^N(Z_n)] \tag{28}$$

Причому на N-му кроці процедура визначається співвідношенням (19) та (20).

Висновки. Таким чином, якщо в задачі виявлення без оцінювання моменту появи КА або при вирішенні задачі виявлення і оцінювання окремо оптимальна процедура заснована на порівнянні одновимірної статистики L_n с з детермінованим порогом, то при спільному вирішенні цих завдань оптимальні області зупинки і продовження спостережень визначаються в тривимірному просторі (за допомогою рівностей (23) - (26) і (28)).

Користуючись співвідношенням (23) – (26), можна показати, що $F_{n0}^N(\pi_n, S_n)$ є неперервною функцією π_n при кожному фіксованому значенні S_n. Це свідчить про можливості представлення правила (27) у вигляді

$$u_N^0(Z_n) = \begin{cases} \left(1, m_N^{(i)}\right), L_n \ge L_n^0(S_n,N) \\ 0, \quad L_n < L_n^0(S_n,N), n = 1,N \end{cases} \tag{29}$$

де $L_n^0(S_n,N)$, - поріг, який знаходиться з рівності: $\tilde{\Gamma}_{n0}^N(y,S_n) = \Gamma_{n1}(y,S_n), n = 1,N-1$.

Причому при n = N поріг визначається рівністю (20). Описання виразом (29) може виявитись більш зручним з практичного погляду, ніж (27) та (28).

Структура процедур виявлення виду (27) та (29) залишається оптимальною і при невиконанні умов (10) та (11). Однак співвідношення (23) – (25) при цьому вже не справджуються.

Список використаних джерел

1. Левин Б. Р. Теоретические основы статистической радиотехники. Москва : Радио и связь, 1989. 656 с.

2. Сосулин Ю. Г. Теория обнаружения и оценивание стохастических сигналов. Изд. 2-е. Москва : Сов. радио, 2001. 323 с.

3. Ширяев А. Н. Статистический, последовательный анализ. Оптимальные правила постановки. Изд. 3-е, доп. Москва : Наука, 2002. 282 с.

4. Огірський 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.

5. Леман Э. Проверка статистических гипотез. Изд. 2-е. Москва : Наука, 2000. 418 с.

6. Кокс Д., Лбюис П. Статистический анализ последовательностей событий. Изд-е 2-е доп. Москва : Наука, 2001. 315 с.

7. Суслин Ю. Г., Фишман М. М. Теория последовательных решений и ее применение. Изд. 2-е доп. Москва : Радио и связь, 2005. 292 с.

8. Де Гроот М. Оптимальные статистические решения. Изд. 3-е доп. Москва : Мир, 2004. 506 с.

9. Иоффе А. Д., Тихомиров В. М. Теория экстремальных задач. Изд. 3-е. Москва : Наука, 1999. 558 с.

10. Ковалевский В.Н. Методы оптимальных решений в распознавании изображений. Изд. 2-е доп. Москва : Наука, 1996. 348 с.

11. Закс Ш. Теория статистических выводов. Изд. 2-е доп. Москва : Мир, 1995. 775 с.

12. Filus K., Domańska J., Gelenbe E. (2021) Random Neural Network for Lightweight Attack Detection in the IoT. In: Calzarossa M.C., Gelenbe E., Grochla K., Lent R., Czachórski T. (eds) Modelling, Analysis, and Simulation of Computer and Telecommunication Systems. MASCOTS 2020. Lecture Notes in Computer Science, vol 12527. Springer, Cham. URL: https://doi.org/10.1007/978-3-030-68110-4_5.

13. Paulo Vitor de Campos Souza, Augusto Junio Guimarães, Thiago Silva Rezende, Vinicius Jonathan Silva Araujo, Vanessa Souza Araujo (2020). Detection of Anomalies in Large-Scale Cyberattacks Using Fuzzy Neural Networks, AI 2020, 1(1), 92-116. URL: https://doi.org/10.3390/ai1010005-07.

References

1. Levyn, B. R. (1989). *Teoreticheskie osnovy statisticheskoi radiotekhniki [Theoretical Foundations of Statistical Radio Engineering].* Radyo y sviaz.

2. Sosulyn, Yu. H. (2001). *Teoriia obnaruzheniia i otsenivanie stokhasticheskikh signalov [Detection theory and estimation of stochastic signals].* Sovetskoe radio.

3. Shyriaev, A. N. (2002). *Statystycheskyi, posledovatelnыi analyz. Optymalnыe pravyla postanovky [Statistical, sequential analysis. Optimal staging rules].* Nauka.

4. Ohirskyi, I. R. (2015) Zahalni problemy prohnozuvannia NSD v informatsiinykh systemakh derzhavy [General problems of NSD forecasting in state information systems]. *Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsikh v Ukraini – Legal, regulatory and metrological support of the information protection system in Ukraine*, 2(30), pp. 31-34.

5. Leman, E. (2000). *Proverka statystycheskykh hypotez [Testing statistical hypotheses].* Nauka.

6. Koks, D. (2001). *Statisticheskii analiz posledovatelnostei sobytii [Statistical analysis of sequences of events].* Nauka.

7. Suslyn, Yu. H. (2005). *Teoryia posledovatelnыkh reshenyi y ee prymenenye [The theory of successive decisions and its application].* Radio i sviaz.

8. De Hroot, M. (2004). *Optimalnye statisticheskie resheniia [Optimal statistical solutions].* Nauka.

9. Ioffe, A.D. (1999). *Teoriia ekstremalnykh zadach [Theory of extreme problems].* Nauka.

10. Kovalevskii, V.N. (1996). *Metody optimalnykh reshenii v raspoznavanii izobrazhenii [Methods of optimization in image recognition].* Nauka.

11. Zaks, Sh. (1995). *Teoriia statisticheskikh vyvodov [Statistical inference theory].* Mir.

12. Filus K., Domańska J., Gelenbe E. (2021). Random Neural Network for Lightweight Attack Detection in the IoT. In: Calzarossa M.C., Gelenbe E., Grochla K., Lent R., Czachórski T. (Eds.) *Modelling, Analysis, and Simulation of Computer and Telecommunication Systems. MASCOTS 2020. Lecture Notes in Computer Science,* 12527. https://doi.org/10.1007/978-3-030-68110-4_5.

13. Paulo Vitor de Campos Souza, Augusto Junio Guimarães, Thiago Silva Rezende, Vinicius Jonathan Silva Araujo, Vanessa Souza Araujo (2020). Detection of Anomalies in Large-Scale Cyberattacks Using Fuzzy Neural Networks, AI 2020, 1(1), 92-116. https://doi.org/10.3390/ai1010005-07.

UDC 004.056.53:005.004.7

Volodymyr Khoroshko, Mykhailo Shelest, Yuliia Tkach

DETECTION AND EVALUATION OF CYBERATACS IN INFORMATION NETWORKS WITH RANDOM MOMENT OF OCCURRENCE

Detection, prevention or significant impediment to cyberattacks (CA) is one of the central areas of cybersecurity in information networks. Determining the generalized requirements for cyber protection of information networks from cyberattacks on information and assessing the degree of their security are quite difficult tasks.

There are real possibilities for unforeseen situations as a result of cyberattacks, leading to the loss of information or to its loss and loss of information network. The concept of cybersecurity of the information network on the basis of threats from cyberattacks should determine the necessary tools, methods and procedures for detection and evaluation of cyberattacks in networks. Therefore, for the effective functioning of information networks in modern conditions and means of their protection, as well as for the reliable detection and evaluation of cyberattacks, it is necessary to develop new approaches and methods, their implementation.

Some results related to joint sequential detection and evaluation were obtained in [3]. As follows from [3], in the general case, is not possible to find a constructive solution even in the two-alternative problem. Losses in the process of recognition (detection) and evaluation of a cyberattack depend on both errors in its detection and inaccuracy of evaluation, which will not provide adequate response, and there is a problem of joint development and evaluation [1, 2]. Therefore, we will try to solve this problem of multi-alternative sequential detection and evaluation of a cyberattack with a random moment of its occurrence.

Consistent detection and evaluation procedures are generally more efficient than inconsistent ones. Therefore, it is important and urgent to find optimal, consistent or close to them procedures that will increase the cybersecurity of information.

The purpose of the article is to find optimal, consistent or close to them procedures that will increase the cybersecurity of information.

Based on the probabilistic assessment, the optimal, sequential or close to them procedures are revealed in the work, which allow to increase the cybersecurity of information. The problem to build the optimal N-truncated sequential procedure for joint detection of cyberattacks (CA) and to estimate the moment of its occurrence in the loss function was solved. Statistics related to the average volume of the forecast (UOP) are analyzed. A general view of the optimal procedure for sequential detection-evaluation of a cyberattacks with an unknown moment of occurrence during these losses is proposed.

Thus, if the optimal procedure is based on comparing one-dimensional statistics Ln c with a deterministic threshold for solving the problem of detection without estimating the moment of cyberattacks or for solving the problem of detection and evaluation separately, then the optimal areas for stopping and continuation of observations are determined in three-dimensional space for solving these problems.

Keywords: *cyberattack, information networks, cyber impact, cybersecurity.*

References: 11.

Хорошко Володимир Олексійович – доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій, Національний авіаційний університет (просп. Любомира Гузара, 1, м. Київ, 03058, Україна).
Khoroshko Volodymyr – Doctor of Technical Sciences, Professor, Professor of the Department of Information Technology Security, National Aviation University (1 Lubomir Guzara Av., 03058 Kyiv, Ukraine).
E-mail: professor_va@ukr.net
ORCID*:* http:/orcid.org/0000-0001-6213-7086

Шелест Михайло Євгенович – доктор технічних наук, професор, професор кафедри кібербезпеки та математичного моделювання, Національний університет «Чернігівська політехніка» (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Shelest Mykhailo – Doctor of Technical Science, Professor, Professor of Department of Cybersecurity and Mathematical Simulation, Chernihiv Polytechnic National University (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: mishel3141@gmail.com
ORCID: https:// orcid.org/ 0000-0003-1090-0371
SCOPUS Author ID: 57211429755

Ткач Юлія Миколаївна – доктор педагогічних наук, професор, завкафедри кібербезпеки та математичного моделювання, Національний університет «Чернігівська політехніка» (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Tkach Yuliia – Doctor of Pedagogical Science, Professor, Head of Department of Cybersecurity and Mathematical Simulation, Chernihiv Polytechnic National University (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: tkachym79@gmail.com
ORCID: https://orcid.org/0000-0002-8565-0525
SCOPUS Author ID: 57193026076

Хорошко В., Шелест М., Ткач Ю. Виявлення та оцінювання кібератак в інформаційних мережах з випадковим моментом появи. *Технічні науки та технології.* 2021. № 1(23). С. 96-102.