блемы оценки качества защиты (киберзащиты) при проектировании или модификации информационной системы. В статье рассмотрены пути повышения системности подхода к самой проблеме защиты информации при комплексном использовании всех имеющихся средств защиты. При этом все средства, методы и меры, которые используются для защиты информации, объединяются в единый целостный механизм – систему защиты, которая должна обеспечивать защиту не только злоумышленников, но и некомпетентных или недостаточно подготовленных пользователей и персонала. Также рассмотрено системное решение проблемы оценки качества защиты (киберзащиты) при проектировании или модификации информационной системы.
***Ключевые слова**: информационные системы, защита информационных систем, киберзащита, защита информации, оценка киберзащиты.*

Аясрах Ахмад Расмі Алі, аспірант, Національний авіаційний університет.
Аясрах Ахмад Расми Али, аспирант, Национальный авиационный университет.
Ayasrah Ahmad Rasmi Ali, graduate student, National Aviation University.

Отримано *08 жовтня 2021 року*, затверджено редколегією *17 грудня 2021 року*

DOI: 10.18372/2225-5036.27.16001

БАГАТОАЛЬТЕРНАТИВНЕ ВИЯВЛЕННЯ КІБЕРАТАК В ІНФОРМАЦІЙНИХ МЕРЕЖАХ

Хорошко[1] В.О., Ткач[2] Ю.М., Шелест[2] М.Є.

[1]Національний авіаційний університет
[2] Чернігівський національний технологічний університет

ХОРОШКО Володимир Олексійович, д.т.н., професор.
Рік та місце народження: 1945 рік, м. Харків, Україна.
Освіта: Київський інститут інженерів цивільної авіації, 1968 рік.
Посада: професор кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, технічні системи захисту інформації, аналіз функціонування складних систем.
Публікації: більше 500 наукових публікацій, серед яких наукові статті, монографії, підручники, патенти навчально-методичні посібники.
E-mail: professor_va@ukr.net.
ORCID: 0000-0001-6213-7086.

ШЕЛЕСТ Михайло Євгенович, д.т.н., професор.
Рік та місце народження: 1954 р., м. Ромни, Україна.
Освіта:. Національний університет "Львівська Політехніка"
Посада: професор кафедри кібербезпеки та математичного моделювання.
Наукові інтереси: інформаційна безпека, оцінювання вразливостей, оптимізація інформаційних систем.
Публікації: більше 100 наукових публікацій, серед яких наукові статті, монографії, підручники, навчально-методичні посібники та деклараційні патенти.
E-mail: mishel3141@gmail.com.
ORCID: 0000-0001-7110-4876.

ТКАЧ Юлія Миколаївна, д.пед.н., професор
Рік та місце народження: 1979 рік, м. Чернігів, Україна.
Освіта: Чернігівський національний технологічний університет, 2012 рік; Чернігівський державний педагогічний університет ім. Т.Г. Шевченка, 2001.
Посада: завідувач кафедри кібербезпеки та математичного моделювання з 2010 р.
Наукові інтереси: інформаційна та кібербезпека.
Публікації: більше 80 наукових публікацій, серед яких, підручники, навчальні посібники, монографії, наукові статті та тези.
E-mail: tkachym79@gmail.com.
ORCID: 0000-0002-8565-0525.

Анотація. *Розвиток інформаційних мереж та інформаційних технологій неможливий без комплексного вирішення задач підвищення ефективності передачі інформації спільно з вирішенням задачі захисту інформація, що передається. Відомі методи і засоби захисту інформаційних мереж й інформації в них потребуються застосування програмного, програмно-апаратного і апаратного забезпечення. У статті виділено ознаки, за якими відбувається групування інформаційних мереж в класи, до них відносяться: наявність в мережах інформації різного рівня конфіденційності; рівень повноважень обслуговуючого персоналу та користувачів мережі на доступ до конфіденційної інформації; режими функціонування мереж – колективний або індивідуальний. В якості однієї із можливостей протидії сучасним кібератакам запропоновано виявлення кібератак в інформаційних мережах з випадковим моментом її появи, що дозволяє збільшити ефективність кіберзахищеності інформаційних мереж та інформації, яка циркулює в них.*

Ключові слова*: інформаційна безпека, інформаційна мережа, кібератака, виявлення кібератак, інформаційні технології.*

Вступ

Розвиток інформаційних мереж та інформаційних технологій неможливий без комплексного вирішення задач підвищення ефективності передачі інформації спільно з вирішенням задачі захисту інформація, що передається.

Відомі методи і засоби захисту інформаційних мереж й інформації в них потребуються застосування програмного, програмно-апаратного і апаратного забезпечення. Але, враховуючи сучасні вимоги захисту, а точніше кіберзахисту, вони не забезпечують виявлення і оцінку кібератак (КА). При цьому, основною формою атак слід вважати:

– на технічному рівні: кібернетичні атаки (кібератака – сукупність узгоджених за цілями, змістом і часом дій або заходів, так званих кіберакцій, спрямованих на визначений об'єкт, з метою порушення конфіденційності, цілісності, доступності, спостереженості інформації, що і ній циркулює, а також порушення роботи інформаційної мережі);

– на стратегічному та спеціальному рівнях: кібернетичні операції (за аналогією з методами звичайної війни, кібероперація - це сукупність узгоджених за часом, глибиною та задачами відносно короткочасних кібератак, що спрямовані на певну кількість об'єктів взаємодії противника з метою отримання несанкціонованого доступу до інформації і порушення роботи інформаційних мереж або взагалі повний її вивід із ладу).

Метою статті є розробка методики багатоальтернативного виявлення кібератак інформаційних систем.

Основна частина

Слід зазначити, що оборонними засобами є засоби, призначені для виявлення та попередження атакуючих дій противника. Вони можуть ділитися на наступні основні групи: розвідувальні засоби інформаційного забезпечення і засоби забезпечення інформаційної безпеки й кібербезпеки.

При цьому, необхідно враховувати, що до ознак, за якими відбувається групування інформаційних мереж в класи, відносяться:

– наявність в мережах інформації різного рівня конфіденційності;

– рівень повноважень обслуговуючого персоналу та користувачів мережі на доступ до конфіденційної інформації;

– режими функціонування мереж – колективний або індивідуальний.

В якості однієї із можливостей протидії сучасним кібератакам пропонується їх виявлення, що дозволяє збільшити ефективність кіберзахищеності інформаційних мереж та інформації, яка циркулює в них. Використовуємо результати, отримані в [1], для багатоальтернативного випадку, враховуючи, що в випадковий момент λ_0 може з'явитись одна з $M-1$ $(M \geq 3)$ кібератак з ймовірностями $\pi_{oi}=P(\theta=i)$, $i=\overline{1,M-1}$, і з ймовірністю $1-\mu=P(\theta=0)$ не з'явитись ні одна з кібератак ($\mu=\sum_{i=1}^{M-1}\pi_{oi}<1$). Величини x_n, $n\geq 1$, які спостерігаються, є незалежними як при відсутності, так і при наявності кібератак, до того ж для спрощення припустимо, що збій послідовності після появи кібератаки відбувається стрибком. У результаті:

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

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

$$j\leq n-1, n\geq 1, i=\overline{1,M-1}, j\Delta\leq\lambda<(j+1)\Delta.$$

Припустимо, що функція втрат має вигляд:

$$g(\theta,\lambda,n,u_n)= \begin{cases} g_{0j}(n),\theta=0,u_n=(j,\hat{\lambda}_n^{(i)}), \\ \tilde{g}_{ij}(n),\theta=i,\lambda>n\Delta,u_n=(j,\hat{\lambda}_n^{(j)}), \\ g_{ij}(n)+(\lambda-\hat{\lambda}_n^{(j)})^2+c(n-[\lambda]),\theta=i, \\ \lambda\leq n\Delta,u_n=(j,\hat{\lambda}_n^{(j)}),n=\overline{1,N},i,j=\overline{1,M-1}; \end{cases} \quad (3)$$

$$g(\theta,\lambda,u_n,N)=\begin{cases} g_{00}(N),\theta=0,u_N=0, \\ g_{i0}(N),\theta=i,\lambda>N\Delta,u_N=0, \\ g_{i0}(N)+c(N-[\lambda]),\theta=i,\lambda\leq N\Delta, \\ u_N=0,i=\overline{1,M-1}; \end{cases} \quad (4)$$

де $\hat{\lambda}_n^{(j)}$- оцінка моменту появи j-ї КА.

Введемо наступні позначення:

$\pi_{ni}=P(\theta=i|x_1^n)$ – апостеріорна ймовірність наявності i-ї КА;

$\Lambda_{ni}=\tilde{p}_i(x_1^n)/p_0(x_1^n)$ – усереднений об'єм прогнозу (УОП);

$\tilde{p}_i(x_1^n)=\int_0^\infty p(x_1^n|\,\theta=i,\lambda_0=\lambda)p_i(\lambda)d\lambda; p_i(\lambda)=p(\lambda|\theta=i)$ - апріорна щільність ймовірності величини λ_0 за умови, що $\theta=i, L_{ni}=\Lambda_{ni}-A_{ni}$; $A_{ni}=P(\lambda_0\geq\pi\Delta|\,\theta=i)$; $v_i=\pi_{0i}/\pi_{00}=\pi_{0i}/(1-\mu)$; $\tilde{\pi}_{jn}=P(\lambda_0<j\Delta|x_1^n)$;

$\pi_{s+1n}^{(s)}=P\{\lambda_0\in[s\Delta,(s+1)\Delta]|x_1^n\}$ – апостеріорна ймовірність появи будь-якої КА до моменту $j\Delta$ і в інтервалі $[s\Delta,(s+1)\Delta]$ відповідно;

$\tilde{p}(\lambda|x_1^n)=p(\lambda|x_1^n,\lambda_0<n\Delta)=p(\lambda|x_1^n)/\tilde{\pi}_{nn}$ – апостеріорна щільність λ_0 за умови, що одна з КА з'являється до моменту $n\Delta$;

$p(\lambda|x_1^n)$ – апостеріорна щільність λ_0;

$m_n^{(k)}=\int_0^{n\Delta}\lambda^k\,\tilde{p}(\lambda|x_1^n)d\lambda$ – k-й нецентральний момент апостеріорного розподілу $p(\lambda|x_1^n)$;

$D_n = (\lambda - m_n^{(1)})^2 \tilde{p}(\lambda|x_1^n)d\lambda$ - дисперсія апостеріорного розподілу $p(\lambda|x_1^n)$.

Використовуючи (3) і (4) можна показати, що апостеріорний ризик (АР), пов'язаний з вирішеннями $u_N = 0, u_n = (j\ ,\ \widehat{\lambda}_n^{(j)})$ дорівнює:

$$R_{N0}(x_1^N) = (1 + \overline{\Lambda}_N)^{-1} G_{N0}(L_N) + c\sum_{j=0}^{N} \tilde{\pi}_{jN}\,; \quad (5)$$

$$R_{nj}\left(x_1^n, \widehat{\lambda}_n^{(j)}\right) = \Bigg(1 + \overline{\Lambda}_n)^{-1}\,[g_{0j}(n) + \sum_{i=1}^{M-1} \tilde{g}_{ij}(n)v_i A_{ni} + \sum_{i=1}^{M-1} g_{ij}(n)v_i L_{ni}\Bigg]$$

$$+ \sum_{i=1}^{M-1} \pi_{ni} \int_0^{n\Delta} (\lambda - \widehat{\lambda}_n^{(j)})^2\, \tilde{p}(\lambda|\theta = i, x_1^n)d\lambda + c\sum_{j=0}^{N} \tilde{\pi}_{jn}\,; \quad (6)$$

$\partial e\ \overline{\Lambda}_n = \sum_{i=1}^{M-1} v_i \Lambda_{ni};\ L_n = (L_{n1}, \dots, L_{nM-1});$

$$G_{N0}(L_N) = g_{00}(N) + \sum_{i=1}^{M-1} v_i[A_{Ni}\,\tilde{g}_{i0}(N) + L_{Ni} g_{i0}(N)]\,. \quad (7)$$

При отриманні (5)-(7) враховано, що

$$p(\lambda_0 < n\Delta|\theta = i, x_1^n) = \frac{\int_0^{m\Delta} p(x_1^n|\theta = i,\ \lambda_0 = \lambda\,)p_i(\lambda)d\lambda}{\int_0^{\infty} p(x_1^n|\theta = i,\ \lambda_0 = \lambda\,)p_i(\lambda)d\lambda} = \frac{L_{ni}}{\Lambda_{ni}}; \quad (8)$$

$$\sum_{i=1}^{M-1}\sum_{i=0}^{n-1}(n-l)P(\,\lambda_0 \in [l\Delta, (l+1)\Delta], \theta = i|\varkappa_1^n) = \sum_{i=1}^{M-1}\sum_{i=0}^{n-1} P(\,\lambda_0 < j\Delta, \theta = i|x_1^n) = \sum_{j=0}^{N} \tilde{\pi}_{jn}\,;$$

$$\pi_{ni} = \frac{v_i \Lambda_{ni}}{1 + \overline{\Lambda}_n}; \quad (9)$$

$$P(\lambda_0 < \lambda, \theta = 0|x_1^n) = 0. \quad (10)$$

З (8)-(10) слідує, що

$$\tilde{\pi}_{nn} = \textstyle\sum_{i=1}^{M-1} v_i L_{ni}/\,(1 + \overline{\Lambda}_n). \quad (11)$$

Мінімізуючи (6) вибором оцінки, неважко побачити, що оптимальна оцінка є середнім апостеріорного розподілу:

$$\tilde{p}(\lambda|x_1^n) = \frac{\sum_{i=1}^{M-1} \pi_{ni}\, p(\lambda|\theta = i, x)}{\tilde{\pi}_{nn}}. \quad (12)$$

Тобто:

$$\widehat{\lambda}_n^0(j) = m_n^{(1)}, j = \overline{1, M-1}, a\ AP\ R_{nj}(x_1^n, m_n^1\,) = inf_{\widehat{\lambda}_n^{(j)}} R_n\left(\varkappa_1^n, \widehat{\lambda}_n^{(j)}\right) G_{nj}(L_n, D_n)(1 + \overline{\Lambda}_N)^{-1} + c\sum_{j=0}^{n} \tilde{\pi}_{jn}\,; \quad (13)$$

де

$$G_{nj}(L_n, D_n) = g_{0j}(n) + \sum_{i=1}^{M-1} v_i\{\tilde{g}_{ij}(n)A_{ni} + L_{ni}[\,g_{ij}(n) + D_n]\}. \quad (14)$$

Із (5), (7), (12) та (13) слідує, що якщо рішення приймається безпосередньо по N спостереженням, то оптимальне багатоальтернативне правило виявлення-оцінювання має вигляд:

$$u_N^0\left(L_N, D_N, m_N^{(1)}\right) = \begin{cases} (j, m_N^{(1)}, L_N \in V_{Nj}(D_N), \\ 0,\ L_N \in V_{Nj}(D_N), \end{cases} \quad (15)$$

де:

$$V_{Nj}(D_N) = \left[L_N\colon G_{Nj}(L_N, D_N) \le G_{N0}(L_N)\right], \quad (16)$$

$$V_{N0}(D_N) = \left[L_N\colon {}_{j \in \overline{1, M-1}}^{\ min}\, G_{Nj}(L_N, D_N) > G_{N0}(L_N)\right]. \quad (17)$$

При отриманні співвідношень (5)-(17) ніде не використовувалась незалежність спостережень, тобто результати справджуються для загальної моделі, що включає корельовані спостереження та послідовний збій. Однак при побудові оптимальної послідовної процедури виявлення-оцінювання та виводу алгоритмів формування статистик L_n, $m_n^{(1)}$, D_n буде використана незалежність спостережень.

За допомогою (1), (2) аналогічно [2] можна показати, що для статистик L_{ni} справджуються рекурентні співвідношення:

$$L_{n+1\,i} = \gamma_{n+1\,i}(x_{n+1})(L_{ni} + \alpha_{n+1\,i}), n \ge 0, L_{0i} = 0, i = \overline{1, M-1}, \quad (18)$$

де $\gamma_{ni}(x_n) = p_{in}(\frac{x_n}{p_{Qn}(x_n)})$;

$$\alpha_{ni}(x_n) = P[(n-1)\Delta \le \lambda_0 < n\Delta|\ \theta = i].$$

Тепер визначимо алгоритм формування статистик $m_n^{(k)}$.

З урахування (9), (11) та (12) отримаємо:

$$m_n^{(k)} = \sum_{i=1}^{M-1} v_i \Lambda_{ni} \int_0^{n\Delta} \lambda^k\, p(\lambda|\theta = i, d\lambda\,|\sum_{i=1}^{M-1} v_i L_{ni}. \quad (19)$$

Очевидно, що:

$$\widehat{\lambda}_{ni}^k \equiv \textstyle\int_0^{n\Delta} \lambda^k\, p(\lambda|\theta = i, x_1^n)d\lambda = \frac{\int_0^{n\Delta} \lambda^k p_i(\lambda)\Lambda_{ni}\left(x_1^n|\lambda\right)d\lambda}{\Lambda_{ni}\left(\Lambda_{ni}\left(x_1^n|\lambda\right)\right)} = \frac{p\left(x_1^n|\theta = i,\ \lambda_0 = \lambda\right)}{p_0(x_1^n)}.$$

Звідки за допомогою (1) і (2) знаходимо:

$$\widehat{\lambda}_{ni}^k = \sum_{i=0}^{n-1} v_{j+1l}^{(k)} \prod_{l=j+1}^{n} \gamma_{nl}(x_l)/\Lambda_{nl}, \quad (20)$$

де $v_{j+1l}^{(k)} = \int_{j\Delta}^{(j+1)\Delta} \lambda^k\, p_i(\lambda)d\lambda.$

Позначаючи через $r_{ni}^{(k)} = \sum_{i=0}^{n-1} v_{j+1l}^{(k)} \prod_{l=j+1}^{n} \gamma_{li}(x_l)$, з (19) і (20) знаходимо:

$$m_n^{(k)} = \frac{\sum_{i=1}^{M-1} v_i r_{ni}^{(k)}}{\sum_{i=1}^{M-1} v_i L_{ni}}. \quad (21)$$

До того ж, неважко показати, що $r_{ni}^{(k)}$ задовольняє рекурентне співвідношення:

$$r_{n+1i}^{(k)} = \gamma_{n+1\,i}(x_{n+1})\left(r_{ni}^{(k)} + v_{n+1i}^{(k)}\right), n \ge 0, r_{0i}^{(k)} = 0. \quad (22)$$

Зазначимо, що, $r_{n1}^{(0)}$ відповідає L_{ni}.

При K=1 співвідношення (18), (21) та (22) дають ефективний апарат формування оптимальної оцінки. Оскільки апостеріорний розподіл $D_n(x_1^n)$ пов'язаний зі статистиками $m_{n1}^{(1)}$ та $m_n^{(2)}$ є очевидним рівняння:

$$D_n = m_n^{(2)} - \left(m_n^{(1)}\right)^2. \quad (23)$$

Співвідношення (18), (21)-(23) при k=1,2 визначає алгоритм формування статистики D_n. З (18), (21)-(23)випливає, що

$$D_n(\varkappa_1^n) = D_n[T_n(\varkappa_1^n)], n \ge 1, \quad (24)$$

де:

$$T_n = \left(L_n, r_n^{(1)}, r_n^{(2)}\right);\ r_n^{(k)} = (r_{n1}^{(k)}, r_{n1}^{(2)}, \dots, r_{nM-1}^{(k)})\,.$$

Введемо позначення:

$\overline{p}(x) = \sum_{i=1}^{M-1} \pi_{0i}\overline{p}_i(x_1^n) + (1-\mu)p_0(x_1^n)$ - безумовна щільність розподілу вектора x;

$$p_{n+1}(x_{n+1}|x_1^n) = \overline{p}(x_1^{n+1})/(\overline{p}(x_1^n)) = ((\overline{\Lambda}_{n+1} + 1)/(\overline{\Lambda}_n + 1))P_{0n+1}(x_{n+1}) \ . \quad (25)$$

Останнє рівняння в (25) справедливе при виконанні (1). $M(x_1^n)$ математичне сподівання, що відповідає щільності (25).

Розглянемо лему, яку будемо використовувати надалі.

Лема. Нехай модель спостережень має вигляд (1), (2). Тоді статистика π_{jn} є мартингалом:

$$M(\overline{\pi}_{jn+1}|x_1^n) = \tilde{\pi}_{jn}, n \geq 0; \quad (26)$$

$$M\pi_{jn} < \infty, n \geq 0. \quad (27)$$

Доведення. Відомо, що

$$\tilde{\pi}_{jn} = \sum_{l=0}^{j-1} \tilde{\pi}_{l+1n}^{(l)}, \quad (28)$$

Причому

$$\tilde{\pi}_{l+1n}^{(l)} = \sum_{i=1}^{M-1} \pi_{ni} P\{\lambda_0 \in [l\Delta, (l+1)\Delta] | \theta = i, x_1^n\}. \quad (29)$$

Використовуючи (1), (2), (9), і (29) неважко показати, що:

$$\tilde{\pi}_{l+1n}^{(l)} = \sum_{i=1}^{M-1} v_i \alpha_{l+1i} \prod_{s=l+1}^{n} \gamma_{si}(x_s)/(1 + \overline{\Lambda}_n). \quad (30)$$

За допомогою (25) і (30) знаходимо:

$$M\left(\tilde{\pi}_{l+1n+1}^{(l)} \middle| x_1^n\right) = \{\sum_{i=1}^{M-1} v_i \alpha_{l+1i} \prod_{s=l+1}^{n} \gamma_{si}(x_s)\}/(1 + \overline{\Lambda}_n) = \tilde{\pi}_{l+1n}^{(l)}. \quad (31)$$

Рівності (28) і (31) показують справедливість (26). Справедливість (27) очевидна. Відповідно, лему доведено.

Оптимальна послідовна N-усічена процедура виявлення-оцінювання на N-му кроці має вигляд (15). Переходячи до (N-1)-го кроку, з урахуванням (5), (13), (24), (25), леми і транзитивності статистик [4]:

$$L_{n+1}(x_1^{n+1}) = L_{n+1}(x_{n+1}, L_n), T_{n+1}(x_1^{n+1}) = L_{n+1}(x_{n+1}, T_n), \quad (32)$$

випливає з (18) і (22), отримуємо, що найменший апостеріорний ризик в області продовження спостережень:

$$R_{N-10}^N(x_1^{N-1}) = (1 + \overline{\Lambda}_{N-1})^{-1} \int_{x_N} \min\{G_{N0}[L_N(x_N, L_{N-1})]\}; \min_{j \in \overline{1, M-1}} G_{Nj}[L_N(x_N, L_{N-1}), D_N(T_N(x_N, T_{N-1}))] p_{0N}(x_N) d\varkappa + c\sum_{j=1}^{N} \tilde{\pi}_{jN-1}, \quad (33)$$

Використовуючи (11), (30) і той факт, що $\tilde{\pi}_{n+1n} = \tilde{\pi}_{nn} + \tilde{\pi}_{n+1n}^{(n)}$, отримуємо:

$$\tilde{\pi}_{n+1n} = (1 + \overline{\Lambda}_N)^{-1} \sum_{i=1}^{M-1} v_i(L_{ni} + \alpha_{n+1\,i}). \quad (34)$$

Підставивши (34) в (33), знаходимо:

$$R_{N-10}^N(x_1^{N-1}) = (1 + \overline{\Lambda}_N)^{-1} G_{N-10}^N(T_{N-1}) + c\sum_{j=0}^{n} \tilde{\pi}_{jN-1}, \quad (35)$$

де

$$G_{N-10}^N(T_{N-1}) = \int_{x_N} \min\{\min_{j \in \overline{1, M-1}} G_{Nj}[L_N(x_N, L_{N-1}), D_N(T_N(x_N, T_{N-1}))]; G_{N0}[L_N(\varkappa_N, L_{N-1})]\} P_{N0}(\varkappa_N) d\varkappa_N + c\sum_{i=1}^{M-1} v_i(L_{N-1i} + \alpha_{Ni}).$$

З (35), (13), (24) слідує, що оптимальне правило на (N-1)-му кроці має вигляд:

$$u_{N-1}^0(T_{N-1}) = \begin{cases} (j, m_{N-1}^{(1)}, T_{N-1} \in V_{N-1j}^N, \\ 0, \quad T_{N-1} \in V_{N-10}^N, \end{cases}$$

де

$$V_{N-1j}^N = [T_{N-1}: G_{N-10}^N(T_{N-1}) \geq G_{N-1j}(T_{N-1})];$$

$$V_{N-10}^N = \left[T_{N-1}: G_{N-10}^N(T_{N-1}) < \min_{j \in \overline{1, M-1}} G_{N-1j}(T_{N-1})\right].$$

Продовжуючи далі для кроків (N-2), (N-3), … неважко показати, що для $n = \overline{1, N-1}$ найменшому апостеріорному ризику в області продовження спостережень (згідно з [5]):

$$R_{n0}^N(x_1^n) = (1 + \overline{\Lambda}_N)^{-1} G_n^N(T_n) + c\sum_{j=0}^{n} \tilde{\pi}_{jn},$$

де:

$$G_{n0}^N(T_n) = \int_{x_{n+1}} \min\left\{\min_{j \in \overline{1, M-1}} G_{n+1j}[T_{n+1}(x_{n+1}, T_n)]\right\}; G_{n+10}^N[T_{n+1}(x_{n+1}, T_n)]\} P_{0n+1}(x_{n+1}) dx_{n+1} + c\sum_{i=1}^{M-1} v_i(L_{ni} + \alpha_{n+1\,i}), \quad (36)$$

а оптимальна байєсова багатоальтернативна послідовна процедура спільного виявлення КА і оцінювання їх моментів появи має вигляд

$$u_n^0(T_n) = \begin{cases} (j, m_n^{(1)}, T_n \in V_{nj}^N, j = \overline{1, M-1}, \\ 0, \quad T_n \in V_{n0}^N, n = \overline{1, N}. \end{cases} \quad (37)$$

Тут

$$V_{n0}^N = \left[T_n: G_{n0}^N(T_n) < \min_{j \in \overline{1, M-1}} G_{nj}(T_n)\right];$$

$$V_{nj}^N = [T_n: G_{n0}^N(T_n) \geq G_{nj}(T_n)]. \quad (38)$$

Таким чином із (37) і (38) слідує, що достатньою є $3(M-1)$-мірна статистика T_n, алгоритми формування компонентів якої визнаються рекурентними співвідношеннями (18) і (22).

В момент зупинки:

N, якщо такого n не існуєтворюється оцінка $m_{\tau N}^{(1)}(\tau_{\tau N}^{(1)}, L_{\tau N})$ моменту появи КА, яка визначається рівнянням (21) при k = 1.

У випадку роздільного вирішення задач виявлення і оцінювання (квадратичні втрати в (3) відсутні) достатньою для виявлення моменту зупинки при моделі (1) та (2) є статистика L_n розмірності $M-1$, так як член з D_n в (14) відсутній.

Висновки

Всі отримані результати можуть бути розповсюджені на випадок поступового збою при появі КА з припущенням, що встановлений режим настає за час, менший інтервалу Δ між послідовними відліками.

Список літератури:

[1] Хорошко В. А. Виявлення і оцінювання кібератак в інформаційних мережах з випадковим моментом виявлення / Хорошко В.А. Шелест М.Е., Ткач Ю.Н., Браиловский Н.Н. // Scientific and Practical Cyber Security Journal (SPCSJ) 5(2): 65-68 ISSN 2587-4667 Scientific Cyber Security Association (SCSA), Vol 5, No 2, 2021. – С. 10-15.

[2] Опірський І. Р. Загальні проблеми прогнозування НСД в інформаційних системах держави / І.Р.

Опірський // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні, Вип. 2(30), 2015. – С. 31-40.

[3] Закс Ш. Теорія статистичних висновків. Вид. 2 доп./ Ш. Закс. – М:Мир, 1995. – 775 с.

[4] Ширяєв А. Н. Статистичний послідовний аналіз. Оптимальні правила зупинки. Вид. 3 доп./ А. Н. Ширяєв. – М: Наука, 2002. – 282 с.

[5] Конс Д. Статистичний аналіз послідовних подій. Вид. 2 доп. / Д. Конс, П. Луїс. – М: Наука, 2001. – 315 с.

УДК 004.081.3

Хорошко В.А., Ткач Ю.Н., Шелест М.Е.

МНОГОАЛЬТЕРНАТИВНОЕ ВЫЯВЛЕНИЕ КИБЕРАТАК В ИНФОРМАЦИОННЫХ СЕТЯХ

Аннотация. *Развитие информационных сетей и информационных технологий невозможно без комплексного решения задач повышения эффективности передачи информации совместно с решением задачи защиты передаваемой информации. Известные методы и средства защиты информационных сетей и информации в них нуждаются в применении программного, программно-аппаратного и аппаратного обеспечения. В статье выделены признаки, по которым происходит группирование информационных сетей в классы, к ним относятся: наличие в сетях информации разного уровня конфиденциальности; уровень полномочий обслуживающего персонала и пользователей сети на доступ к конфиденциальной информации; режимы функционирования сетей – коллективный или индивидуальный. В качестве одной из возможностей противодействия современным кибератакам предложено выявление кибератак в информационных сетях со случайным моментом ее появления, что позволяет увеличить эффективность киберзащищенности информационных сетей и циркулирующей в них информации.*

Ключевые слова: *информационная сохранность, информационная сеть, кибератака, обнаружение кибератак, информационные технологии.*

Khoroshko V.A., Tkach Yu.N., Shelest M.E.

MULTIALTERNATIVE DETECTION OF CYBERATACS IN INFORMATION NETWORKS

Abstract. *The development of information networks and information technologies is impossible without a comprehensive solution to the problems of improving the efficiency of information transmission together with the solution of the problem of protection of transmitted information. Known methods and means of protection of information networks and information in them require the use of software, software and hardware and hardware. The article highlights the features by which information networks are grouped into classes, they include: the presence of information networks of different levels of confidentiality; the level of authority of service personnel and network users to access confidential information; modes of operation of networks - collective or individual. As one of the possibilities of counteracting modern cyberattacks, it is proposed to detect cyberattacks in information networks with a random moment of its appearance, which allows to increase the effectiveness of cybersecurity of information networks and information circulating in them.*

Key words: *information security, information network, cyber attack, cyber attack detection, information technology.*

Хорошко Володимир Олексійович, д.т.н., професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.

Хорошко Владимир Алексеевич, д.т.н., профессор, профессор кафедры безопасности информационных технологий Национального авиационного университета.

Khoroshko Volodymyr, Doctor of Technical Sciences, Professor, Professor of the Department of Information Technology Security of the National Aviation University.

Шелест Михайло Євгенович, д.т.н., професор, професор кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет.

Шелест Михаил Евгеньевич, д.т.н., профессор, профессор кафедры кибербезопасности и математического моделирования, Черниговский национальный технологический университет.

Shelest Mykhailo, Doctor of Technical Sciences, Professor, Professor of the Department of Cybersecurity and Mathematical Modeling, Chernihiv National University of Technology.

Ткач Юлія Миколаївна, доктор педагогічних наук, професор, завідувач кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет.

Ткач Юлия Николаевна, доктор педагогических наук, профессор, заведующая кафедрой кибербезопасности и математического моделирования, Черниговский национальный технологический университет.

Tkach Yuliia, Doctor of Pedagogical Science, Professor, Head of Department of Cybersecurity and Mathematical Simulation, Chernihiv National University of Technology.