Scientific and Practical Cyber Security Journal (SPCSJ) 5(2): 12-17 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

IDENTIFICATION OF CYBER ATTACKS ON INFORMATION NETWORKS WITH A RANDOM MOMENT OF ITS APPEARANCE

ВЫЯВЛЕНИЕ КИБЕРАТАК В ИНФОРМАЦИОННЫХ СЕТЯХ СО СЛУЧАЙНЫМ МОМЕНТОМ ЕЕ ПОЯВЛЕНИЯ

Volodymyr Khoroshko, National Aviation University, Doctor of Engineering Science, Full Professor, Kiev, Ukraine,
Хорошко Владимир Алексеевич, доктор технических наук, профессор, профессор Национального авиационного университета (г. Киев).

Mykhailo Shelest, Chernihiv Polytechnic National University, Doctor of Technical Science, Full Professor, Chernihiv, Ukraine,
Шелест Михаил Евгеньевич, доктор технических наук, профессор, профессор Национального университета «Черниговская политехника» (г. Чернигов)

Yuliia Tkach, Chernihiv Polytechnic National University, Doctor of Pedagogical Science, Professor, Chernihiv, Ukraine,
Ткач Юлия Николаевна, доктор педагогических наук, профессор, завкафедрой кибербезопасности и математического моделирования Национального университета «Черниговская политехника» (г. Чернигов)

Nikolay Brailovskyi, Taras Shevchenko National University of Kyiv, PhD in Engineering Science, Associate Professor Kiev,
Браиловский Николай Николаевич, кандидат технических наук, доцент, доцент Киевского национального университета имени Тараса Шевченко (г. Киев).

ABSTRACT: In information networks, when detecting and recognizing cyber-attacks, they are usually interested not only in the fact of the appearance of a particular attack, but also in its informative parameters. The result of actions performed in solving the problem of the presence of a cyberattack depends on the degree of closeness of the estimate to the true value of the parameters. Therefore, losses in the process of recognizing (detecting) and evaluating a cyberattack depend both on errors in its detection and on the inaccuracy of assessment, which will not allow providing adequate countermeasures, and at the same time the task of joint development and evaluation arises. In practice, the moment of making a decision is very important, since with an increase in the observation time, the costs increase and, therefore, the fastest decision-making is desirable. At the same time, sequential detection-estimation procedures are more effective than inconsistent ones. Therefore, finding the optimal, consistent or close to them procedures will increase the cybersecurity of information.

Some results related to joint sequential detection and estimation, obtained in the works of other authors, show that in the general case it is not possible to find a constructive solution even in a two-alternative problem. Therefore, the authors made an attempt to solve the problem of multi-alternative sequential detection and evaluation of a cyberattack with a random moment of its occurrence.

АННОТАЦИЯ: В информационных сетях при обнаружении и распознании кибератак обычно интересуются не только фактом появления той или иной атаки, но и ее информативными параметрами. Результат действий, совершаемых при решении задачи о наличии кибератаки, зависит от степени близости оценки к истинному значению параметров. Поэтому потери в процессе распознания (обнаружения) и оценивания кибератаки зависят как от ошибок в ее выявлении, так и от неточности оценивания, что не позволит обеспечить адекватное противодействие, и при этом возникает задача совместного развития и оценивания. На практике момент принятия решения очень важен, поскольку с увеличением времени наблюдения возрастают затраты и, поэтому, желательно быстрейшее принятие решений. При этом последовательные процедуры обнаружения-оценивания, имеют большую эффективность

по сравнению с непоследовательными. Поэтому нахождения оптимальных, последовательных или близких к ним процедур, позволит повысить кибербезопасность информации.

Некоторые результаты, связанные с совместным последовательным обнаружением и оцениванием, получены в работах других авторов, показывают, что в общем случае найти конструктивное решение не удается даже в двухальтернативной задаче. Поэтому авторами была сделана попытка решить задачу многоальтернативного последовательного обнаружения и оценивания кибератаки со случайным моментом ее появления.

KEYWORDS: *analysis of the processes of attack and counteraction in the information space, sequential detection and assessment of cyberattacks, multi-alternative tasks.*

КЛЮЧЕВЫЕ СЛОВА*: анализа процессов нападения и противодействия в информационном пространстве, последовательное обнаружение и оценивание кибератак, многоальтернативные задачи.*

Введение

При рассмотрении проблемы кибербезопасности информации необходимо учитывать возможные виды несанкционированных действий (кибератак) ведущих к потере или модификации данных. Выявление, предотвращение или существенное затруднение действия кибератак (КА) – одно из центральных направлений области кибербезопасности в информационных сетях. Определение обобщенных требований по киберзащите информационных сетей от кибератак на информацию и оценка степени их защищенности представляют достаточно сложными задачами. Опыт практической эксплуатации информационных сетей в различных сферах деятельности государства показывает, что существуют реальные угрозы КА, приводящие к негативному воздействию на составляющие кибербезопасности.

Существуют реальные возможности возникновения непредвиденных ситуаций в следствии воздействия КА, ведущие к утрате информации либо к ее потере и потере работоспособности информационной сети. В концепции кибербезопасности информационной сети на основе угроз от КА должны определяться требуемые средства, методы и процедуры обнаружения и оценивания КА в сетях [1].

Имеет место процесс разграничения разных видов угроз. При этом необходимость понимания роли КА и кибербезопасности связана в первую очередь с активизацией международных террористических, экстремистских организаций и преступных группировок, а также отдельных государств, которые осуществляют кибератаки и кибервоздействия на граждан, общество и государства с целью реализации своих интересов.

При этом в условиях ведения гибридных войн в последние годы систематически осуществляются различные КА, кибервоздействия и несанкционированные действия в информационных сетях, что подрывает экономическую, военную, техническую и другие сферы не только государства, но и отдельных его отраслей [1,2].

Поэтому для эффективного функционирования информационных сетей в современных условиях и средств их защиты, а также для надежного обнаружения и оценивания КА необходимо развивать новые подходы и методы, их реализации.

Основная часть

При обнаружении и распознании кибератак обычно интересуются не только фактом появления той или иной атаки, но и ее информативными параметрами. Результат действий, совершаемых при решении задачи о наличии кибератаки, от степени близости оценки к истинному значению параметров. Поэтому потери в процессе распознания (обнаружения) и оценивания кибератаки зависит как от ошибок в ее выявлении, так и от неточности оценивания, что не позволит обеспечить адекватное противодействие, и при этом возникает задача совместного развития и оценивания [3,4]. Причем на практике момент принятия решения обычно не безразличен, поскольку с увеличением времени наблюдения, затраты возрастают и

желательно быстрейшее принятие решений. При этом последовательные процедуры обнаружения-оценивания, вообще говоря, имеют большую эффективность по сравнению с непоследовательными. Поэтому актуальность нахождения оптимальных, последовательных или близких к ним процедур, что позволит повысить кибербезопасность информации.

Некоторые результаты, связанные с совместным последовательным обнаружением и оцениванием, получены в [5]. Как следует из [5], в общем случае найти конструктивное решение не удается даже в двухальтернативной задаче. Поэтому попытаемся решить эту задачу многоальтернативного последовательного обнаружения и оценивания кибератаки со случайным моментом ее появления.

Пусть событие $\{\theta = 1\}$ означает наличие кибератаки (КА), которая может появиться в момент $\infty > \lambda_n = \lambda_0 > 0$, n ≥ 1, причем $\pi_{01} = P(\theta = 1) = P(\lambda_0 < \infty) < 1$ $(\pi_{00} = P(\theta = 0) = P(\lambda_0 = \infty) = 1 - \pi_{01})$. Положим, что $x_n,\ n \geq 1$, независимы или как до так и после появления КА, так что справедлива модель [6]

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

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

$$j\Delta \leq \lambda \leq (j+1)\Delta, j \leq n-1, n = 1, N,$$

где $P_{\lambda n}(x_n)$ – плотность, зависящая от λ причем

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

принятая при рассмотрении в [6] задачи обнаружения сбоя последовательности без оценки его момента.

Задача состоит в построении оптимальной N-усеченной последовательной процедуры совместного обнаружения КА и оценивания момента ее появления при функции потерь:

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

где с-стоимость задержки в вычислении решения о наличии КА u_n ее появления на один шаг; $[\lambda] = i$ при $(i-1)\Delta < \lambda \leq i\Delta$ (i – интервал между отсчетами).

Решение $u_n = 0$ на шагах n=1, N-1 эквивалентно по решению u_n о продолжении наблюдений [6]. На N-м шаге это решение является окончательным, поскольку процесс $\{x_n\}$ наблюдению более недоступен и потери $g(\theta, \lambda, u_n = 0, N)$ связанные и имеют вид:

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

Функция потерь (1), (2) отличается от [4]

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

где w_n – неубывающая неотрицательная функция, определяющая зависимость потерь от неточности оценивания информационного параметра не зависящая от принимаемых гипотез и истинной гипотезы; тем, что от значений информационного параметра зависят не только потери за счет неточности его оценивания, но и сама величина $g_{ij}(n, \lambda)$.

Например $g_{11}(n, \lambda) = g_{11}(n) + c(n - [\lambda])$ при $\lambda \leq n\Delta,\ g_{11}(n, \lambda) = \widetilde{g_{01}}(n)$ при $\lambda > n\Delta$. В частном случае, когда

$$C = 0, g_{11}(n) = \widetilde{g_{11}}(n), g_{10}(N) = \tilde{g}_{10}(N) \quad (4)$$

потери (1), (2), (3) совпадают и можно воспользоваться результатами, получаемыми в [7]. Используя (1), нетрудно показать, что оптимальная оценка отличается от результатов, полученных в [7] – она представляет собой среднее апостериорное распределение $P(\lambda_0 \le \lambda | x_1^n, \theta = 1, \lambda \le n\Delta)$ с плотностью $\widetilde{p_{01}}(\lambda) = p_1(x_1^n|\lambda)p(\lambda)/[\int_0^{-n\Delta} p_1(x_1^n|\lambda)p(\lambda)d\lambda], \lambda \le n\Delta,$

$p(\lambda)$-плотность априорного распределения $\prod(\lambda) = P_0(\lambda_0 \le \lambda | \theta = 1)$ т.е.

$\widetilde{\lambda_n^0} = \int_0^{n\Delta} \lambda \widetilde{p_{01}}(\lambda) d\lambda$ поскольку $w_n(\lambda - \widehat{\lambda_n}) = \begin{cases} F_n(\lambda - \widehat{\lambda_n})^2, \lambda < n\Delta \\ 0, \lambda \ge n\Delta \end{cases}$

Введем обозначение: $m_n^{(i)}(x_1^n) = M[\lambda_0^i | x_1^n, \theta = 1, \lambda_0 \le n\Delta], i \ge 1;$

$$D_n(x_1^n) = M[\left(\lambda_0 - m_n^{(i)}\right)^2 | x_1^n, \theta = 1, \lambda_0 \le n\Delta] \quad (5)$$

– i-й нецентральный момент и дисперсия апостериорного распределения;

$L_n(x_1^n)$ – статистика, связанная с усредненным объёмом прогноза (УОП)

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

Используя (2), можно показать [8], что для $\{m_n^{(i)}\}$ справедливы рекуррентные равенства.

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

Здесь $\gamma_n(x_n) = \frac{p_{1n}(x_n)}{p_{0n}(x_n)}$ статистика L_n удовлетворяет рекуррентному соотношению [3]:

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

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

При i = 1 соотношение (7) задает алгоритм формирования оптимальной оценки момента выявления КА (6), при i = 2 – второго апостериорного момента. Также

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

с помощью (7), (8) и [5] определяется апостериорная дисперсия, а значит

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

Если сбой последовательности при появлении КА происходит, т.е.

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

либо КА может появится лишь в дискретные моменты $n\Delta, n = 0,1,2 \ldots$

$$p(\lambda) = p_n \delta(\lambda - n\Delta), (\textstyle\sum_{n \ge 0} p_n = 1), \quad (11)$$

то $\nu_{n+1}^{(i)} = \alpha_{n+1}^{(i)} \gamma_{n+1}(x_{n+1})$ и из [3], (7) следует, что

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

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

Из 12 следует, что значение любого момента апостериорного распределения (5) на $(n+1)$ – м шаге при выполнении (10) или (11) зависит лишь от n наблюдений, причем посредством $(L_n, m_n^{(i)})$:

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

В более общем случае (7,8, [5]) можем записать

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

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

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

В силу выражения (14) Z_n–транзитивная статистика

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

Статистика π_n связана с L_n равенством

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

$A_n = P(\lambda_0 \ge n\Delta | \theta = 1), \nu = \frac{\pi_{01}}{1 - \pi_{01}}$.

Из (14), (16), (17) следует, что условия принятые в [9] выполнены, причем $T_n = Z_n = (L_n, S_n), S_n = (m_n^{(1)}, m_n^{(2)}), S_{n+1} = S_{n+1}(x_{n+1}, Z_n).$

Таким образом, можно воспользоваться теоремой [10]: последовательность $\{Z_n, n = 1, n\}$ является достаточной, а оптимальная процедура последовательного обнаружения-оценивания имеет вид приведенный в [11], где T=Z_n – трехмерная статистика согласно (9), (15), причем в соответствии с [10] $V_{n0}^N = V_{nn}^N, n = 1,\ N = 1$.

В том случае, когда (4) не выполнено, непосредственно применить теорему [10] невозможно и задача немного усложняется, однако трёхмерная статистика $Z_n = = (L_n, m_n^{(1)}, m_n^{(2)})$ остается достоверной и в этом случае. Действительно, используя (1) и (17), нетрудно показать, что

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

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

$\pi_{in} = P(\lambda_0 < i\Delta | x_1^n)$ – апостериорная вероятность наличия КА и моменту $i\Delta$. Апостериорный риск $R_{No}(x_1^N)$ определяется равенствами из [10]. С помощью (18), (19) и [12] получаем, что оптимальная процедура на N-м шаге имеет вид:

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

где L_n, $m_N^{(i)}$, D_N – находятся в соответствии с (8) и (9), а

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

- порог, зависящий от апостериорной точности оценивания момента появления КА λ_0.

Последующие результаты получаем для случая скачкообразного сбоя последовательности при появлении КА, когда выполняется условие (10), либо для случая дискретного распределения момента λ_0 (11). При этом, как следует из (13) согласно [13]:

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

где Zn – транзитная статистика. Используя (19) – (21), (16), (18), аналогично [6,14], можно показать, что наименьший апостериорный риск (НАР) в области продолжения наблюдений $V_{n0}^N = V_{n1}^N = [R_{n0}^N(x_1^n) \leq R_{n0}(x_1^n)]$ имеет вид

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

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

Величины $D_n^{(V)}$ определяются рекуррентно в соответствии с уравнениями

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

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

Функция Γ_{n0}^N определяется с помощью [15], в которых Ln заменяется на Zn, так как области

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

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

зависят не только от Ln , но и от $m_n^{(1)}, m_n^{(2)}$.

Из выражений (18) и (22) следует, что оптимальная процедура последовательного обнаружения-оценивания КА с неизвестным моментом появляется при потерях (1) в общем случае при невыполнении условий (4) имеет вид:

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

где $V_{n1}^N = [Z_n : \Gamma_{n1}(Z_n) \leq F_{n0}^N(Z_n)]$ - область остановки наблюдений, причем на N-м шаге процедура определяется соотношениями (19) и (20).

Пользуясь соотношениями (23) – (26), можно показать, что $F_{n0}^N(\pi_n, S_n)$ является непрерывной функцией π_n При каждом фиксированном значении Sn. Это свидетельствует о возможности представления правила (27) в виде

$$u_N^0(Z_n) = \begin{cases} \left(1, m_N^{(i)}\right), L_n \geq L_n^0(S_n, N) \\ 0, \qquad L_n < L_n^0(S_n, N), n = 1, N \end{cases} \quad (28)$$

где $L_n^0(S_n, N)$, - порог, находимый из уравнения

$$\tilde{\Gamma}_{n0}^{N}(y, S_n) = \Gamma_{n1}(y, S_n), n = 1, N-1, \quad (29)$$

причем при n = N порог определения равенством (20). Описание выражением (28) может оказаться более удобным с практической точки зрения, нежели (27).

Структура процедур обнаружения вида (27) и (28) остается оптимальной и при невыполнении условий (10) и (11). Однако соотношения (23) – (25) при этом уже не справедливы.

Выводы

Таким образом, если в задаче обнаружения без оценивания момент появления КА или при решении задачи обнаружения и оценивания раздельно оптимальная процедура основана на сравнении одномерной статистики Ln с детерминированным порогом, то при совместном решении этих задач оптимальные области остановки и продолжения наблюдений определяется в трехмерном пространстве при помощи равенств (23) – (26).

Литература

1. Brailovskyi N., Khoroshko V., Kozura V., Kondakova S. Analysis of the Cybersecurity Status of the Information Space. Scientific and Practical Cyber Security Journal (SPCSJ), vol2, #4, december, 2018.-p.64-74.
2. Brailovskyi N., Khokhlacheva Y., Khoroshko V., Ayasrah Ahmad. Evaluation of the Level of Cyber Security of Information. Scientific and Practical Cyber Security Journal (SPCSJ), vol3, #3, september, 2019.-p.18-24.
3. Левин Б.Р. Теоретические основы статистической радиотехники / Б.Р. Левин. – М.: Радио и связь, 1989. – 656 с.
4. Сосулин Ю.Г. Теория обнаружения и оценивание стохастических сигналов. Изд. 2-е / Ю.Г. Сосулин. – М.: Сов. радио, 2001. – 323 с.
5. Ширяев А.Н. Статистический, последовательный анализ. Оптимальные правила постановки. Изд. 3-е, допол./ А.Н. Ширяев. – М.: Наука, 2002. – 282 с.
6. Огірський І.Р. Загальні проблеми прогнозування НСД в інформаційних системах держави / І.Р. Огірський // Правове, нормативне та метрологічне забезпечення системи захисту інформаціх в Україні. Вип. 2 (30), 2015. – С. 31-34.
7. Леман Э. Проверка статистических гипотез. Изд-е 2-е / Э. Леман. М.: Наука, 2000. – 418 с.
8. Кокс Д. Статистический анализ последовательностей событий. Изд-е 2-е доп. / Д.Кокс, П. Лбюис. – М.: Наука, 2001. – 315 с.
9. Суслин Ю.Г. Теория последовательных решений и ее применение. Изд-е 2-е доп. /Ю.Г. Суслин, М.М. Фишман. – М.: Радио и связь, 2005. – 292 с.
10. Де Гроот М. Оптимальные статистические решения. Изд-е 3-е доп. / М. Де Гроот. – М.: Мир, 2004. – 506 с.
11. Иоффе А.Д. Теория экстремальных задач. Изд-е 3-е /А.Д. Иоффе, В.М. Тихомиров. – М.: Наука, 1999. – 558 с.
12. Ковалевский В.Н. Методы оптимальных решений в распознавании изображений. Изд-е 2 доп. / В.Н. Ковалевский. – М.: Наука, 1996. – 348 с.
13. Браіловський М.М. Технології захисту інформації / М.М. Браіловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова – К.: ЦП «Компринт», 2021.-296 с.
14. Козюра В.Д., Захист інформації в комп'ютерних системах: підручник / В.Д. Козюра, В.О. Хорошко, М.Е. Шелест, Ю.М. Ткач, О.О. Балюнов.
15. Закс Ш. Теория статистических выводов. Изд. 2-е доп. / Ш. Закс. – М.: Мир, 1995. – 775 с.