СЕКЦІЯ XV.
СИСТЕМНИЙ АНАЛІЗ, МОДЕЛЮВАННЯ ТА ОПТИМІЗАЦІЯ

DOI 10.62731/mcnd-07.06.2024.003

АЛГОРИТМ ДИСКРЕТНОГО ДИНАМІЧНОГО ФІЛЬТРА ДЛЯ ОЦІНЮВАННЯ ПАРАМЕТРІВ ПОТОКУ ЦІЛЕСПРЯМОВАНИХ ІНФОРМАЦІЙНИХ АТАК НА АВІАЦІЙНУ ТРАНСПОРТНУ СИСТЕМУ

Косогов Олександр Миколайович
ORCID ID: 0000-0001-6691-273X
канд.військ.наук, ст.наук.спів., доцент кафедри аеродинаміки та безпеки польотів
Національний авіаційний університет, Україна

Функціонування системи цивільної авіації в Україні на сучасному етапі безпосередньо пов'язане, насамперед, із забезпеченням належності та своєчасності інформаційних потоків, впровадженням нових інформаційних технологій, глобалізацією та інтеграцією авіаційних інформаційних систем згідно міжнародних стандартів. При цьому інформаційна безпека виступає домінантною складовою процесів інформаційного забезпечення функціонування системи цивільної авіації.

Інформаційні загрози несуть значну небезпеку для інформаційних об'єктів авіакомпаній, корпорацій, державних авіаційних установ. Необхідно зосередити увагу на найнебезпечнішій і поширеній інформаційній атаці під назвою: "атака (таргетована атака, APT)". Велика небезпека такої атаки полягає в тому, що вона в собі несе і поєднує безліч різноманітних видів і методів реалізації інформаційних атак [1].

Особливість цілеспрямованих атак (APT) полягає в тому, що зловмисників цікавить конкретна компанія або державна організація. Це відрізняє цю загрозу від масових хакерських атак - коли одночасно атакується велика кількість цілей і найменш захищені користувачі стають жертвою. Цілеспрямовані атаки зазвичай добре сплановані і включають кілька етапів – від розвідки і впровадження до знищення слідів присутності. Зазвичай унаслідок цілеспрямованої атаки зловмисники закріплюються в інфраструктурі жертви та залишаються непоміченими протягом місяців або навіть років - протягом усього цього часу вони мають доступ до всієї корпоративної інформації [1].

Виявлення цілеспрямованих атак з метою своєчасної протидії їм потребує оперативного аналізу інформаційного простору з використанням спеціалізованих систем моніторингу. Такі системи мають забезпечувати не тільки апаратний аналіз інформаційних атак, а й кількісний аналіз динаміки проявів цих атак з урахуванням їх специфіки. У разі здійснення атаки інтенсивність інцидентів потоку атак, яка являє собою часовий ряд за кількістю інформаційних інцидентів за певний проміжок часу (як правило, за добу), може містити інформацію як про сам факт APT, так і про фазу сценарію, за яким вона здійснюється.

У [1] доведено, що суперечливість між простотою моделі і її адекватністю певною мірою може бути ослаблена шляхом використання стохастичних (імовірнісних) математичних моделей. Адекватність моделі при цьому може бути оцінена опосередковано, виходячи із загальної ефективності вирішення завдання щодо виявлення інформаційних акцій (операцій, кампаній) на основі коректного використання цієї моделі.

У цій роботі пропонується модель формування тематичного інформаційного потоку, який присутній на вході системи контент-моніторингу, та базується на методах оптимального оцінювання параметрів випадкових процесів, що засновані Р.Е. Калманом, та присвячені дискретній безперервній фільтрації [2]..

Для розроблення алгоритму моделі [1] необхідно обчислити дисперсію шуму системи Q_k і параметри моделі шуму вимірювань матриці A_k та коваріаційної матриці шуму R_k. Для цього доцільно використати підхід, який викладений в [2] і забезпечує стійкість процедури оптимальної динамічної фільтрації.

Пропонується визначати матрицю A_k і коваріаційну матрицю шуму R_k, а також формувати вектор вимірювань z_k за допомогою алгоритму криволінійної апроксимації у рухомому вікні, що містить N останніх елементів випадкової послідовності x_k. В основу алгоритму покладений метод найменших квадратів.

Для апроксимуючої функції

$$\hat{x}_{k-i} = \hat{\beta}_{k0} + \hat{\beta}_{k1} i\Delta t + \hat{\beta}_{k2} i^2 (\Delta t)^2, 0 \le i \le N-1 \quad (1)$$

використання методу найменших квадратів дає такий результат:

$$\hat{\beta}_k = (X^T X)^{-1} X^T x_k, \quad (2)$$

де:

$$\hat{\beta}_k^T = [\hat{\beta}_{k0} \quad \hat{\beta}_{k1} \quad \hat{\beta}_{k2}];$$

$$X^T = \begin{bmatrix} 1 & 1 & \cdots & 1 & \cdots & 1 \\ 0 & \Delta t & \cdots & i\Delta t & \cdots & (N-1)\Delta t \\ 0 & (\Delta t)^2 & \cdots & i^2(\Delta t)^2 & \cdots & (N-1)^2(\Delta t)^2 \end{bmatrix}; \quad (3)$$

$$x_k^T = [x_k \quad x_{k-1} \quad \cdots \quad x_{k-i} \quad \cdots \quad x_{k-N+1}].$$

Частина елементів вектора z_k може бути визначена через елементи вектора $\hat{\beta}_k$:

$$z'_k = \begin{bmatrix} \hat{m}_k \\ \hat{\dot{m}}_k \\ \hat{\ddot{m}}_k \end{bmatrix} = \begin{bmatrix} \hat{\beta}_{k0} \\ -\hat{\beta}_{k1} \\ 2\hat{\beta}_{k2} \end{bmatrix}, \quad (4)$$

причому математичне сподівання вектора z'_k

$$Mz'_k = \begin{bmatrix} m_k \\ \dot{m}_k \\ \ddot{m}_k \end{bmatrix}.$$

Для визначення інших елементів вектора z_k за допомогою виразів (1), (2) з огляду на позначення (3), обчислимо вектор:

$$\hat{x}_k^T = [\hat{x}_k \quad \hat{x}_{k-1} \quad \cdots \quad \hat{x}_{k-i} \quad \cdots \quad \hat{x}_{k-N+1}]:$$

$$\hat{x}_k = X\hat{\beta}_k; \quad (5)$$

Далі сформуємо вектор:

$$q_k^T = [q_k \quad q_{k-1} \quad \cdots \quad q_{k-i} \quad \cdots \quad q_{k-N+1}],$$

$$\text{де } q_{k-i} = (x_{k-i} - \hat{x}_{k-i})^2.$$

У разі використання методу найменших квадратів для апроксимуючої функції

$$\hat{q}_{k-i} = \hat{\gamma}_{k0} + \hat{\gamma}_{k1} i\Delta t + \hat{\gamma}_{k2} i^2 (\Delta t)^2, 0 \le i \le N-1 \quad (6)$$

елементи вектора

$$\hat{\gamma}_k = \begin{bmatrix} \hat{\gamma}_{k0} \\ \hat{\gamma}_{k1} \\ \hat{\gamma}_{k2} \end{bmatrix} = (X^T X)^{-1} X^T q_k,$$

не дають змоги безпосередньо визначити іншу частину елементів вектора z_k, тому що оцінки $\hat{D}_k$, $\hat{\dot{D}}_k$, $\hat{\ddot{D}}_k$ у цьому випадку будуть зсуненими. Незсунені оцінки можна отримати так:

$$z_k'' = \begin{bmatrix} \hat{D}_k \\ \hat{\dot{D}}_k \\ \hat{\ddot{D}}_k \end{bmatrix} = \begin{bmatrix} \hat{\alpha}_{k0} \\ -\hat{\alpha}_{k1} \\ 2\hat{\alpha}_{k2} \end{bmatrix}, \quad (7)$$

де

$$\hat{\alpha}_k = \begin{bmatrix} \hat{\alpha}_{k0} \\ \hat{\alpha}_{k1} \\ \hat{\alpha}_{k2} \end{bmatrix} = (X^T U)^{-1} X^T q_k; \quad (8)$$

U – (N×3) - вимірна матриця, елементи якої обчислюються за формулами

$$\begin{gathered} u_{i0} = 1 - 2g_{ii} + \sum_{j=0}^{N-1} g_{ij}^2, \\ u_{i1} = 1 - 2ig_{ii} + \sum_{j=0}^{N-1} ig_{ij}^2, \\ u_{i2} = 1 - 2i^2 g_{ii} + \sum_{j=0}^{N-1} i^2 g_{ij}^2, \\ 0 \le i \le N-1; \end{gathered} \quad (9)$$

g_{ij}, $0 \le i \le N-1$, $0 \le j \le N-1$, *– елементи (N×N)-вимірної матриці*

$$G = X(X^T X)^{-1} X^T \quad (10)$$

Для отримання коваріаційної матриці шуму R_k і матриці A_k розглянемо N останніх елементів послідовностей $\hat{m}_k$, $\hat{\dot{m}}_k$, $\hat{\ddot{m}}_k$, $\hat{D}_k$, $\hat{\dot{D}}_k$, $\hat{\ddot{D}}_k$, які утворюють вектори:

$$\begin{gathered} \hat{m}_k^T = [\hat{m}_k \quad \hat{m}_{k-1} \quad \cdots \quad \hat{m}_{k-i} \quad \cdots \quad \hat{m}_{k-N+1}], \\ \hat{\dot{m}}_k^T = [\hat{\dot{m}}_k \quad \hat{\dot{m}}_{k-1} \quad \cdots \quad \hat{\dot{m}}_{k-i} \quad \cdots \quad \hat{\dot{m}}_{k-N+1}], \\ \hat{\ddot{m}}_k^T = [\hat{\ddot{m}}_k \quad \hat{\ddot{m}}_{k-1} \quad \cdots \quad \hat{\ddot{m}}_{k-i} \quad \cdots \quad \hat{\ddot{m}}_{k-N+1}], \\ \hat{D}_k^T = [\hat{D}_k \quad \hat{D}_{k-1} \quad \cdots \quad \hat{D}_{k-i} \quad \cdots \quad \hat{D}_{k-N+1}], \\ \hat{\dot{D}}_k^T = [\hat{\dot{D}}_k \quad \hat{\dot{D}}_{k-1} \quad \cdots \quad \hat{\dot{D}}_{k-i} \quad \cdots \quad \hat{\dot{D}}_{k-N+1}], \\ \hat{\ddot{D}}_k^T = [\hat{\ddot{D}}_k \quad \hat{\ddot{D}}_{k-1} \quad \cdots \quad \hat{\ddot{D}}_{k-i} \quad \cdots \quad \hat{\ddot{D}}_{k-N+1}]. \end{gathered}$$

Використання методу найменших квадратів для апроксимації елементів векторів $\hat{m}_k$, $\hat{\dot{m}}_k$, $\hat{D}_k$, $\hat{\dot{D}}_k$ поліномами другого (для $\hat{m}_k$ і $\hat{D}_k$) та першого (для $\hat{\dot{m}}_k$ і $\hat{\dot{D}}_k$) ступеня дозволяє обчислити вектори нев'язок

$$\Delta\hat{m}_k^T = [\Delta\hat{m}_k \quad \Delta\hat{m}_{k-1} \quad \cdots \quad \Delta\hat{m}_{k-i} \quad \cdots \quad \Delta\hat{m}_{k-N+1}],$$
$$\Delta\hat{m}_k = \hat{m}_k - G\hat{m}_k, \quad (11)$$

$$\Delta\hat{\dot{m}}_k^T = [\Delta\hat{\dot{m}}_k \quad \Delta\hat{\dot{m}}_{k-1} \quad \cdots \quad \Delta\hat{\dot{m}}_{k-i} \quad \cdots \quad \Delta\hat{\dot{m}}_{k-N+1}],$$
$$\Delta\hat{D}_k = \hat{D}_k - G\hat{D}_k, \quad (12)$$

$$\Delta\hat{D}_k^T = [\Delta\hat{D}_k \quad \Delta\hat{D}_{k-1} \quad \cdots \quad \Delta\hat{D}_{k-i} \quad \cdots \quad \Delta\hat{D}_{k-N+1}],$$
$$\Delta\hat{\dot{m}}_k = \hat{\dot{m}}_k - Y(Y^T Y)^{-1} Y^T \hat{\dot{m}}_k, \quad (13)$$

$$\Delta\hat{\dot{D}}_k^T = [\Delta\hat{\dot{D}}_k \quad \Delta\hat{\dot{D}}_{k-1} \quad \cdots \quad \Delta\hat{\dot{D}}_{k-i} \quad \cdots \quad \Delta\hat{\dot{D}}_{k-N+1}],$$
$$\Delta\hat{\dot{D}}_k = \hat{\dot{D}}_k - Y(Y^T Y)^{-1} Y^T \hat{\dot{D}}_k, \quad (14)$$

де

$$Y^T = \begin{bmatrix} 1 & 1 & \cdots & 1 & \cdots & 1 \\ 0 & \Delta t & \cdots & i\Delta t & \cdots & (N-1)\Delta t \end{bmatrix}. \quad (15)$$

Усереднення елементів векторів $\hat{\ddot{m}}_k$ і $\hat{\ddot{D}}_k$ дає змогу обчислити вектори нев'язок

$$\Delta\hat{\ddot{m}}_k^T = [\Delta\hat{\ddot{m}}_k \quad \Delta\hat{\ddot{m}}_{k-1} \quad \cdots \quad \Delta\hat{\ddot{m}}_{k-i} \quad \cdots \quad \Delta\hat{\ddot{m}}_{k-N+1}],$$
$$\Delta\hat{\ddot{m}}_{k-i} = \hat{\ddot{m}}_{k-i} - \frac{1}{N}\sum_{j=k-N+1}^{k}\hat{\ddot{m}}_j, \quad (16)$$

$$\Delta\hat{\ddot{D}}_k^T = [\Delta\hat{\ddot{D}}_k \quad \Delta\hat{\ddot{D}}_{k-1} \quad \cdots \quad \Delta\hat{\ddot{D}}_{k-i} \quad \cdots \quad \Delta\hat{\ddot{D}}_{k-N+1}],$$
$$\Delta\hat{\ddot{D}}_{k-i} = \hat{\ddot{D}}_{k-i} - \frac{1}{N}\sum_{j=k-N+1}^{k}\hat{\ddot{D}}_j \quad (17)$$

A_k можна обчислитиза формулою:

$$A_k = Mv_{k+1}v_k^T\left(Mv_kv_k^T\right)^{-1}. \quad (18)$$

Оцінку матриці A_k можна отримати на основі використання нев'язок:

$$\hat{A}_k = \hat{M}v_{k+1}v_k^T\left(\hat{M}v_kv_k^T\right)^{-1}, \quad (19)$$

де

$$\hat{M}v_{k+1}v_k^T = \frac{1}{N-1}\sum_{i=k-N+1}^{k-1}\hat{v}_{i+1}\hat{v}_i^T; \quad (20)$$

$$\hat{M}v_kv_k^T = \frac{1}{N}\sum_{i=k-N+1}^{k}\hat{v}_{i+1}\hat{v}_i^T; \quad (21)$$

$$\hat{v}_i^T = [\Delta\hat{m}_i \quad \Delta\hat{\dot{m}}_i \quad \Delta\hat{\ddot{m}}_i \quad \Delta\hat{D}_i \quad \Delta\hat{\dot{D}}_i \quad \Delta\hat{\ddot{D}}_i].$$

Матрицю R_k пропонується оцінювати на основі використання моделі [1]:

$$\hat{R}_k = \frac{1}{N-1}\sum_{i=k-N+1}^{k-1}\left(\hat{v}_{i+1} - \hat{A}_{k-1}\hat{v}_i\right). \quad (22)$$

Дисперсія шуму системи Q_k використовується для обчислення коефіцієнта підсилення дискретного лінеарізованого динамічного фільтра. Якщо відоме точне значення Q_k, фільтр є оптимальним, при цьому автокореляція нев'язок фільтра відсутня. Підхід, викладений у [3] виключає безпосереднє оцінювання Q_k, Q_k регулюється у такий спосіб, щоб статистика нев'язок фільтра наближувалась до статистики нев'язок оптимального фільтра. Тобто використовується певне співвідношення між Q_k і автокореляційною структурою послідовності нев'язок *(13)*, яке веде до збільшення Q_k при позитивній автокореляції і до зменшення Q_k – при негативній автокореляції.

Для вирішення цього завдання пропонується таке співвідношення:

$$\hat{Q}_k = \hat{Q}_{k-1}\exp\left[\omega\left(\hat{\rho}_{\tilde{m}_k} + \hat{\rho}_{\tilde{D}_k}\right)\right], \quad (23)$$

де $\hat{\rho}_{\tilde{m}_k}$, $\hat{\rho}_{\tilde{D}_k}$ – отримані методом рангової кореляції за Спірменом оцінки коефіцієнта автокореляції послідовностей $\tilde{m}_k$ і $\tilde{D}_k$, утворених відповідними елементами вектора нев'язок $\tilde{\mathbf{s}}_k$;

$$\hat{\rho}_{\tilde{m}_k} = 1 - \frac{6\sum_{i=k-N+1}^{k}\left(\mathrm{runk}(\tilde{m}_k) - \mathrm{runk}(\tilde{m}_{k-1})\right)^2}{N^2(N^2-1)}; \quad (24)$$

$$\hat{\rho}_{\tilde{D}_k} = 1 - \frac{6\sum_{i=k-N+1}^{k}\left(\mathrm{runk}(\tilde{D}_k) - \mathrm{runk}(\tilde{D}_{k-1})\right)^2}{N^2(N^2-1)}; \quad (25)$$

де:

ω – коефіцієнт, який визначається експериментально, з огляду на забезпечення компромісу між швидкістю збіжності оцінки $\hat{Q}_k$ та її флуктуації навколо точного значення Q_k.

Блок-схема розробленого алгоритму якого наведена на рис. 1.

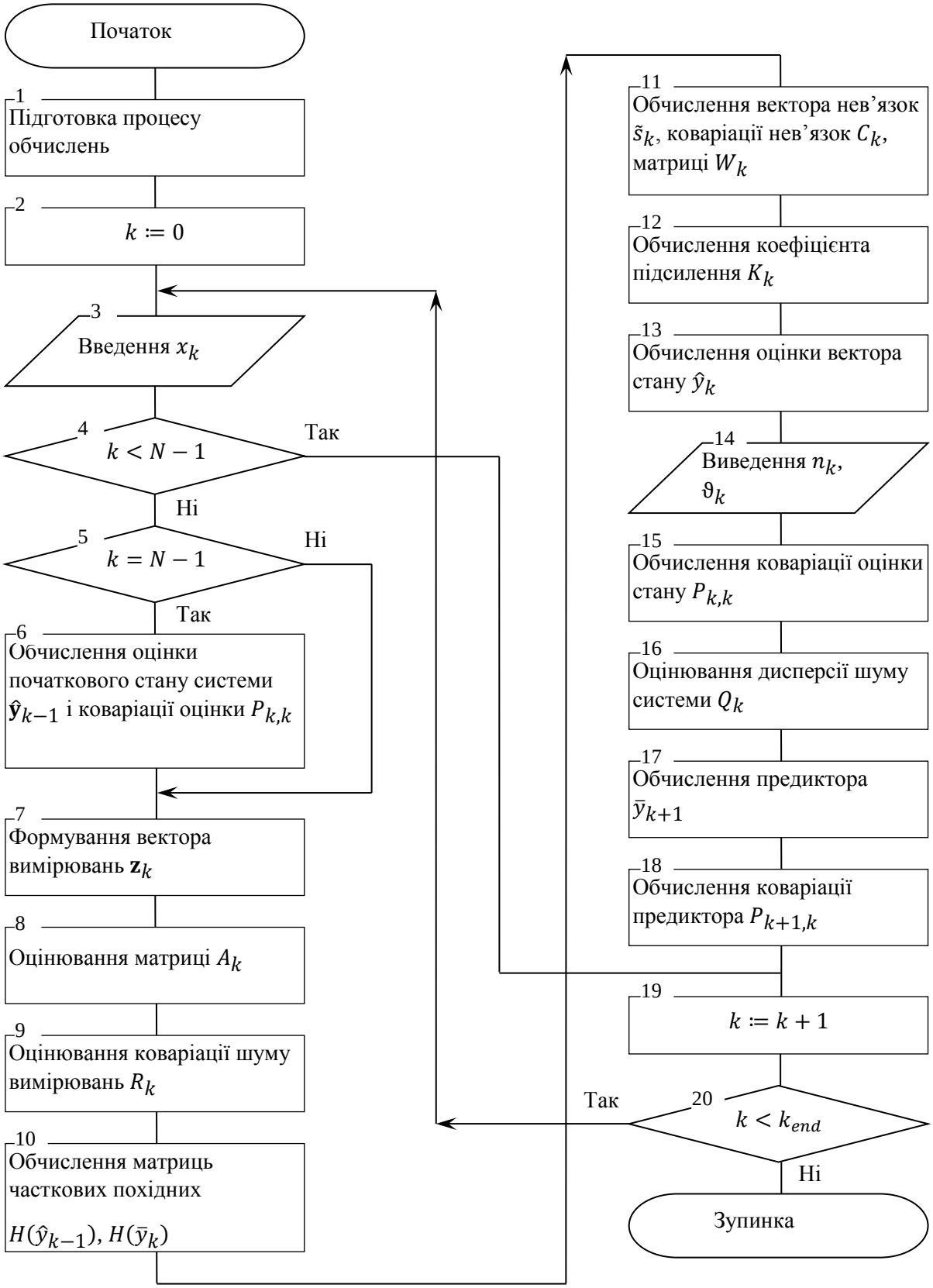

Рис. 2.1. **Блок-схема алгоритму дискретного адаптивного динамічного фільтра для оцінювання параметрів тематичного інформаційного потоку**

Таким чином, потужність співтовариства агентів, що беруть участь у формуванні тематичного інформаційного потоку, $n(t)$ і активність агентів $\vartheta(t)$ в рамках вирішення завдання щодо виявлення факту проведення інформаційних акцій (операцій, кампаній) може оцінюватись на основі використання дискретного адаптивного динамічного фільтра.

Список використаних джерел:

1. Косогов О.М. Модель динаміки інтенсивності інформаційного впливу для виявлення цілеспрямованих інформаційних атак / Наукові орієнтири: теорія та практика досліджень:збірник наукових праць з матеріалами III Міжнародної наукової конференції,м.Ужгород, 17травня, 2024р. / Міжнародний центр наукових досліджень. — Вінниця: ТОВ «УКРЛОГОС Груп, 2024. – С. 184 -189
2. Kalman R. E. A new approach to linear filtering and prediction problems // Journal of Basic Enginiering. – 1960. – Vol. 82, № 1. – P. 35–44.
3. Moghaddamjoo A., Kirlin R.L. Robust Adaptive Kalman Filtering with Unknown Inputs // Transaction on Acoustics, Speech and Signal Processing. – 1989, August. – Vol. 37, № 8. – P. 1166–1175.