УДК 004.056.5:004.73

**DOI: 10.31673/2412-9070.2023.021020**

**Г. В. ШУКЛІН**, канд. техн. наук, доцент;
**Є. В. БОНДАРЕНКО**, магістр,
Державний університет телекомунікацій, Київ

# МЕТОДИКА ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ІНФОРМАЦІЙНОГО НАПРЯМКУ ЗА УМОВ ІНФОРМАЦІЙНО-ТЕХНІЧНИХ ВПЛИВІВ НА ЕЛЕМЕНТИ МЕРЕЖІ ЗВ'ЯЗКУ З ПАМ'ЯТТЮ

***Запропоновано методику забезпечення стійкості інформаційного напрямку (вектора) за умов інформаційно-технічних деструктивних впливів (ІТДВ) на складові мережі зв'язку з пам'яттю. Обґрунтовано можливість здійснити реалізацію переходу від системи об'єктового захисту кореспондентів та складових мереж зв'язку до системи групового захисту, а також підвищити ймовірність передавання даних під час здійснення блокування поширення ІТДВ та вузлів, які взаємодіють один з одним у власних джерелах. Показано, що забезпечення стійкості інформаційного напрямку (вектора) досягається, по-перше, завдяки підвищенню захищеності кореспондентів та складових мережі зв'язку за допомогою керованого фізичного рознесення трактів приймання й передавання інформаційних напрямків (векторів), що не допускає наявності фізичного шляху реалізації ІТДВ, і, по-друге, підвищенням імовірності передавання даних, зменшенням часу їх передавання та навантаження на пропускну здатність ліній зв'язку за умов зміни конфігурації мережі, відмов і перевантажень її складових під час забезпечення її захисту від ІТДВ.***

**Ключові слова:** стійкість; інформаційні напрямки; інформаційно-технічні впливи; деструктивні впливи; інформаційна безпека.

## *ВСТУП*

Сьогодні процеси цифровізації, інформатизації та глобалізації зумовили формування однієї з найскладніших систем суспільної взаємодії — кіберпростору, що надає широкий спектр інформаційно-комунікаційних послуг міжнародному співтовариству в різних галузях життєдіяльності. Щораз вищі темпи розвитку цієї системи, її охоплення та проникнення в усі сфери спричинили появу нових типів загроз у кіберпросторі [1; 2].

Завдяки інформаційно-технічним деструктивним впливам (ІТДВ), такі загрози спроможні нанести максимальний збиток об'єкту кіберпростору в разі успішної реалізації кібератаки протягом періоду часу, коли здійснюється експлуатація його в режимі, вищому за критичний. Особливо високий ризик загрози зазнає критична інфраструктура. Її функціонування в сучасних умовах забезпечується автоматизованою системою керування технологічним процесом, складові якої взаємодіють між собою за допомогою мереж зв'язку [3-5].

Поява нових типів загроз [6] зумовила створення нових підходів у теорії та практиці захисту інформаційно-комунікаційних систем від ІТДВ. Сучасні підходи та системи захисту інформаційно-комунікаційних систем у наданні послуг реалізують різні напрями: розмежування ресурсів — фізичних (наприклад, просторове рознесення напрямних середовищ) і логічних (таких, як технологія VPN [7; 8]), а також міжмережне екранування [9], антивірусний захист [10; 11] тощо. Варто зауважити, що в сучасних методах та способах захисту інформаційно-комунікаційних систем головним підходом є об'єктовий.

Стан уразливості інформаційно-комунікаційних мереж у процесі надання послуг під час реалізації ІТДВ залежить від їхнього рівня в моделі OSI (*Open Systems Interconnection model*). Це пов'язано з тим, що на більш вищому рівні здійснюється акумуляція вразливості всіх нижчих рівнів із подальшим розширенням переліку загроз. Справедливе й обернене твердження, а саме, усунення вразливості на нижчому рівні ліквідує загрози на наступному вищому рівні.

Реалізація процесів захисту мережі від деструктивних впливів зумовлює зниження її комунікаційних характеристик, що безпосередньо впливає на процеси інформаційного обміну між користувачами.

З огляду на викладене можна сформулювати актуальне наукове завдання, сутність якого полягає в забезпеченні стійкості інформаційних напрямків (векторів) через блокування ІТДВ на нижньому (фізичному) рівні моделі OSI мережі зв'язку.

## *ОСНОВНА ЧАСТИНА*

### *Суть методики*

Методика ґрунтується на принципі блокування напрямку (лінії зв'язку), за яким поширюється ІТДВ, із подальшим блокуванням і самого джерела ІТДВ, яке досягається керованим фізичним розмежуванням трактів передавання та приймання інформаційних потоків між кореспондентами в струк-

турі мережі зв'язку. Завдяки цьому втрачається наявність доступного фізичного шляху для реалізації деструктивних впливів [12]. Компенсація можливих втрат даних у разі зміни конфігурації напрямків роботи ліній мережі зв'язку здійснюється завдяки пам'яті її елементів.

Показником ефективності методики є ймовірність своєчасного одержання даних в інформаційному напрямку $P_{\text{пер}}(t/t \le \tau_h)$ протягом заданого часового інтервалу $t_\gamma$.

Мережу зв'язку з пам'яттю, яка перебуває в стаціонарному стані з дуплексними лініями зв'язку, зображено на рис. 1, де «пр» — це процес прийняття інформації; «пер» — процес передавання інформації; «кз» — канал зв'язку; КО — канальні обладнання; ЛУ — лінійні устаткування. Припускаємо, що елементи мережі зв'язку, яку наведено на рис. 1, функціонують за умов ІТДВ і при цьому кореспонденти інформаційних напрямків не переміщуються.

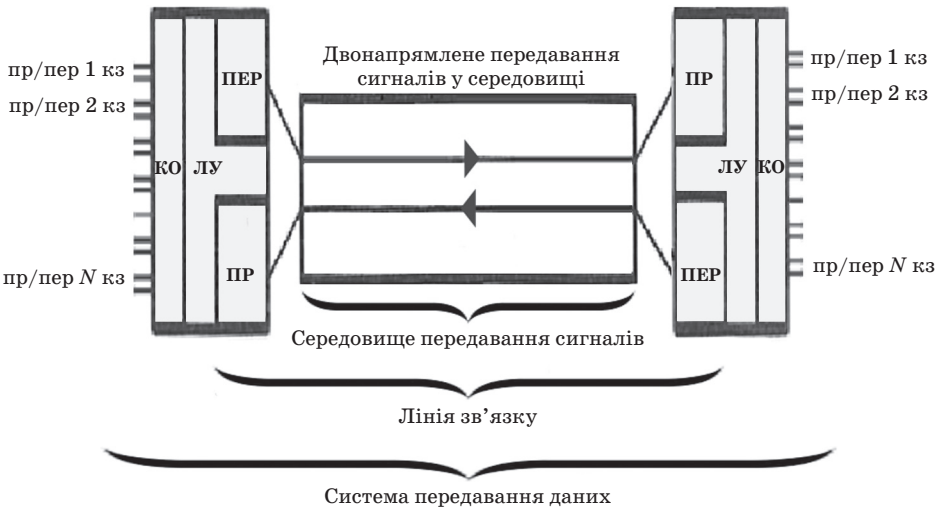


**Рис. 1. Мережа зв'язку з пам'яттю в стаціонарному стані**

Вважатимемо, що обсяг пам'яті елементів мережі зв'язку достатній для зберігання переданих даних протягом заданого проміжку часу і водночас структура мережі зв'язку забезпечує формування не менш як два фізичні маршрути для кожного інформаційного напрямку кореспондентів, а лінії зв'язку обладнано керованими перемикачами односпрямованого передавання даних (ПОПД).

У сучасних мережах зв'язку передавання сигналів (потоків даних) у лініях здійснюється в обидва напрямки. Структуру графа двонапрямленого маршруту між кореспондентами $K_1$ і $K_2$ наведено на рис. 2.

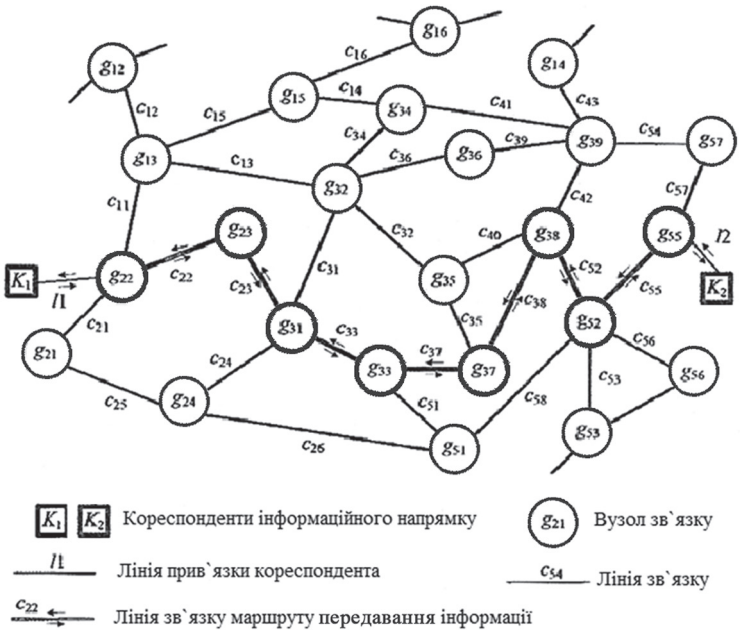


**Рис. 2. Структура графа двонапрямленого маршруту між кореспондентами $K_1$ і $K_2$**

За допомогою ПОПД, підімкнених на кінцях ліній зв'язку, можна здійснити односпрямоване передавання даних. Керовані ПОПД графічно можна подати як схему, зображену на рис. 3.

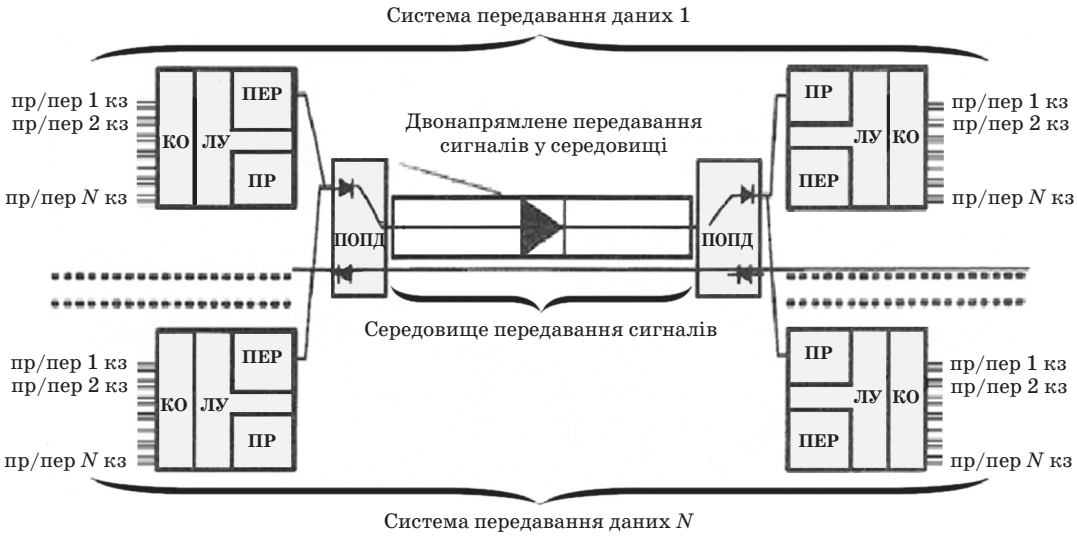


**Рис. 3. Схема керованого ПОПД**

До складу схеми, наведеної на рис. 3, входять два діоди [13] і ключ, що перемикає лінію зв'язку на один із діодів. Функцію діода, наприклад в оптичних системах, можуть виконувати оптичні ізолятори [14].

Один із діодів ПОПД відкритий для тракту приймання лінійного обладнання станційного комплекту системи передавання даних, а другий — для тракту передавання (тобто має зворотний напрямок щодо першого діода). Наявність ключа не дає змоги під'єднати відразу обидва діоди, а односпрямованість діода — під'єднати обидва тракти через один ключ. Станційний комплект із протилежного боку лінії зв'язку підмикається до лінії протилежним трактом. Комплекти інших систем передавання приєднуються до тих самих ПОПД. У результаті лінія зв'язку разом із середовищем передавання сигналів стає односпрямованою. Усі $N$ канали зв'язку, утворені системою передавання даних у такий самий спосіб, у середині потоку даних, тобто лінійного спектра, мають тільки один тракт у лінії зв'язку. Зокрема, маршрут тракту передавання кореспондента $K_1$ в інформаційному напрямку $K_1 \rightarrow K_2$ забезпечується вузлами зв'язку g22, g13, g32, g36, g39, g57, g55, як це унаочнює рис. 4.

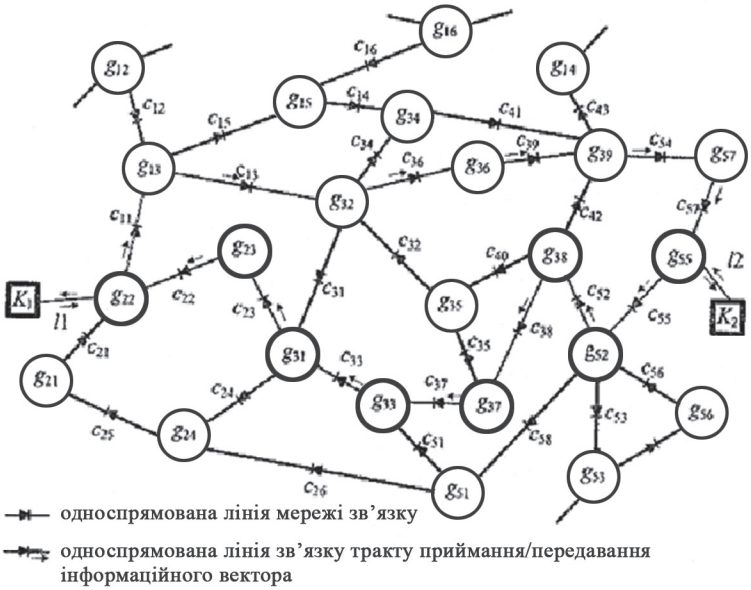


**Рис. 4. Варіант побудови односпрямованих маршрутів (передавання та приймання даних) між кореспондентами $K_1$ і $K_2$ у мережі з ПОПД**

Другий тракт каналів зв'язку і системи передавання приєднується до іншої лінії зв'язку: наприклад, маршрут тракту приймання кореспондента $K_1$ підтримується вузлами зв'язку g55, g52, g38, g37, g33, g31, g23, g22. У такий спосіб відбувається рознесення трактів приймання і передавання даних в інформаційному напрямку під час їхнього проходження в мережі зв'язку. Напрямок роботи ліній зв'язку відображається матрицею ваг мережі за відповідним показником.

У запропонованій методиці вихідними даними є такі:

• склад мережі зв'язку являє собою граф $R = (G,L)$, де $G$ — множина вузлів, а $L$ — множина ліній (зв'язки між вузлами);

• число $H$, яке визначає кількість категорій даних, що задаються за різними ознаками, зокрема пріоритетом передавання даних, граничним часом надходження даних кінцевому кореспонденту, видом даних, що передаються, тощо;

• вимоги кореспондентів до інформаційного обміну, які визначаються категорією переданих даних, швидкістю введення/виведення вихідного/вхідного трафіку, вірогідністю передавання, граничним часом надходження, тобто протягом заданого часу $\tau_h$ передавання $h$-ї категорії даних, які визначаються потребами кореспондентів, де $h = \overline{1,H}$;

• пріоритет передавання, час сталого функціонування $t_\gamma$, протягом якого буде забезпечено своєчасність передавання даних з імовірністю $P_{\text{пер}}$, тощо;

• вимоги до маршрутів, що зумовлюють порядок вибору алгоритму маршрутизації на кожний сеанс зв'язку між кореспондентами в інформаційному напрямку (векторі);

• правила рознесення трактів приймання та передавання на транзитних елементах мережі зв'язку, що беруть участь у складанні маршрутів між кореспондентами інформаційних напрямків, які унеможливлюють перетинання трактів приймання та передавання на фізичних елементах мережі.

Користувачі під'єднуються дуплексними лініями, що схематично подано на рис. 1, тому рознесення трактів приймання та передавання інформаційних потоків у лінії прив'язування до вузла, що кореспондує, не здійснюється.

Наступними вихідними даними в процесі реалізації запропонованої методики є такі:

• метрика $P$ для елементів мережі, за допомогою якої здійснюється опис їхніх станів із достатнім рівнем для ухвалення рішення на формування маршрутів передавання даних в інформаційних напрямках за різних умов;

• інтервали часу $\Delta t_\rho$ оновлення даних за метрикою елементів мережі, які визначаються динамічними показниками. Оновлення даних у маршрутно-адресних таблицях здійснюється на основі протоколів взаємодії;

• інформаційні напрямки кореспондента $I_k$.

Варто зазначити, що місця підімкнення кореспондентів також задаються метрикою елементів мережі.

Варіант і критерії роботи алгоритмів маршрутизації зумовлюються вимогами до стійкості інформаційного напрямку та забезпечення безпеки переданих даних, а також їхньою категорією, часом актуальності переданих даних для кореспондентів тощо. Алгоритми маршрутизації можуть бути унікальними, тобто розробленими під конкретну задачу; можливе також застосування наявних алгоритмів та їх модифікацій [15; 16].

Критерієм імовірності функціонування інформаційного напрямку на потрібному часовому інтервалі є нормативні значення вимог до систем керування зв'язком.

З огляду на викладене створено загальний алгоритм забезпечення стійкості інформаційного напрямку (вектора), схему якого подано на рис. 5 та на рис. 6 за наявності ІТДВ (с. 14).

### *Опис методики*

Розглянемо роботу методики щодо одного інформаційного напрямку, що функціонує з використанням ресурсів мережі зв'язку з пам'яттю. Основні елементи методики подано схемою на рис. 5 і 6, де напівжирним виділено блоки, що відрізняють пропоновану методику від відомих.

У блоці 1 задають вихідні дані та формують матрицю ваг графа мережі за відповідними метриками, включно з метриками, що описують напрям роботи ліній зв'язку і мають період оновлення $\Delta t_\rho$:

$$D_p(t) = (d_{pqj}(t))_{q=1,j=1}, \quad (1)$$

$$D_{pdc}(t) = (d_{pdcqj}(t))_{q=1,j=1}, \quad (2)$$

де $d_{pqj}$ і $d_{pdcqj}$ — вагові коефіцієнти, що враховують відповідно метрику елемента мережі та напрямки роботи лінії зв'язку.

На основі даних вагових матриць формується загальна динамічна маршрутно-адресна таблиця мережі зв'язку:

$$T(t) = \{D_1(t), D_2(t), \ldots, D_N(t),\}, \quad (3)$$

яка характеризується напрямком дуг графа мережі. У блоці 2 кореспонденти інформаційного напрямку формують протягом сеансу потік даних. Його характеристики є умовами вибору алгоритму маршрутизації на поточний сеанс у блоці 3. На основі вибраного алгоритму маршрутизації в блоці 4 визна-

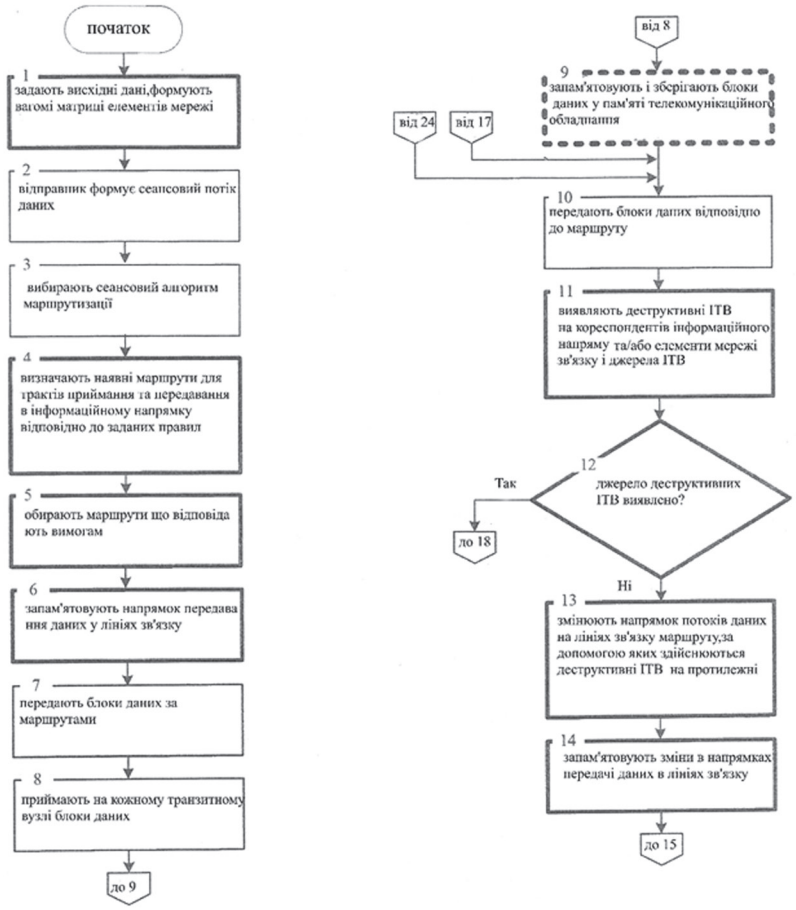


**Рис. 5. Схема забезпечення стійкості інформаційного напрямку (вектора) за наявності ІТДВ (перша частина схеми)**

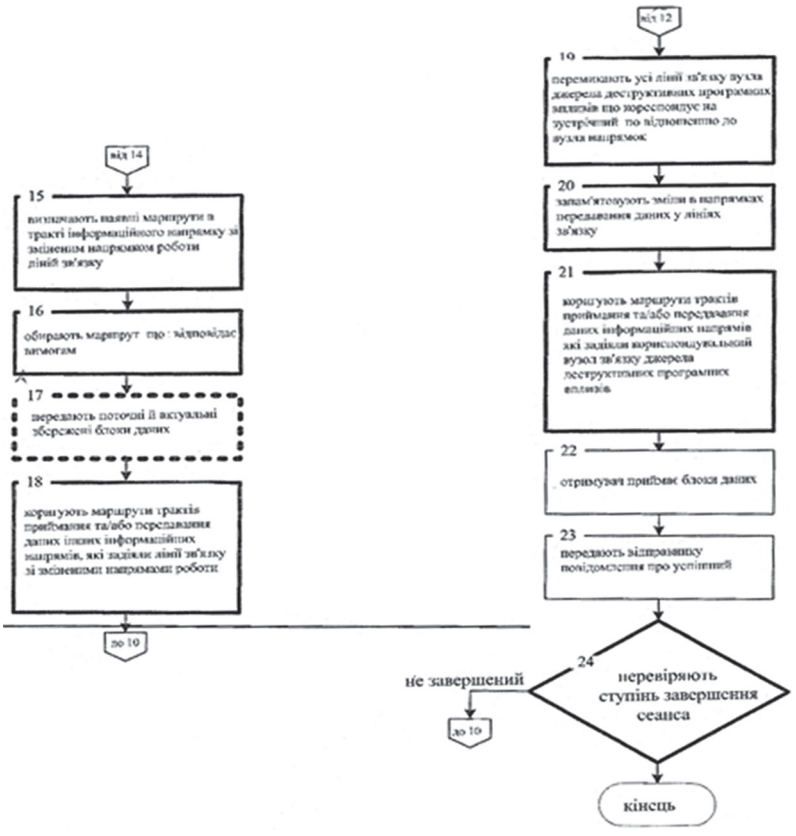


**Рис. 6. Схема забезпечення стійкості інформаційного напрямку (вектора) за наявності ІТДВ (друга частина схеми)**

чають, з огляду на завантаження ресурсів мережі, кількість наявних маршрутів у інформаційному напрямку, за якими існує можливість передавати неподільні складові потоку даних.

Кількість маршрутів обчислюється методом динамічного програмування, причому ця кількість буде збільшуватися поетапно із просуванням через вершини мережі. Кількість маршрутів до поточної вершини залежить тільки від кількості маршрутів до попередніх вершин $M_{k-1}$, дуги яких інцидентні з вершиною $M_k$:

$$M_k = \sum_{i=1}^{k-1} M_i. \quad (4)$$

У блоці 5 вибирають відповідні до вимог маршрути передавання даних, за одним з яких у блоці 7 передають пакети даних. Водночас у блоці 6 здійснюється запис у пам'ять параметрів напрямку передавання даних у лініях зв'язку у відповідний масив.

У блоках 7-10 відбувається передавання даних в інформаційних напрямках із проміжним дублюванням у пам'яті елементів складових каналів за допомогою методу маршрутизації даних у мережі зв'язку з пам'яттю, відмовами та перевантаженнями протягом заданого моменту часу $t_\gamma$. Даний процес спрямовано на забезпечення стійкості інформаційного обміну за умов масових збоїв елементів мережі, які виникають під час її функціонування.

Запропоноване вирішення щодо реакції мережі зв'язку на ІТДВ щодо кореспондентів інформаційного напрямку, а також елементи мережі зв'язку, що надходять по трактах приймання/передавання даних, описуються блоками 11-21. При цьому залежно від факту виявлення джерела ІТДВ, який забезпечується блоком 12, передбачається можливість двох варіантів зміни конфігурації роботи елементів мережі.

У першому варіанті, тобто коли джерело не виявлено, відбувається зміна напрямку роботи ліній зв'язку маршруту, забезпечується зворотний напрямок за допомогою блока 13, а в блоці 14 відображаються такі зміни, які фіксуються відповідними елементами матриць (1)-(3). У блоці 15 відбувається визначення наявних маршрутів у тому тракті інформаційного напрямку, на який вплинули зміни напряму роботи ліній зв'язку (визначення маршрутів можна здійснити за допомогою блока 4).

Маршрути визначають згідно з вимогами, описаними у блоці 1, а в блоці 16 вибирають один із них відповідно до правил рознесення, як це наведено на рис. 7.

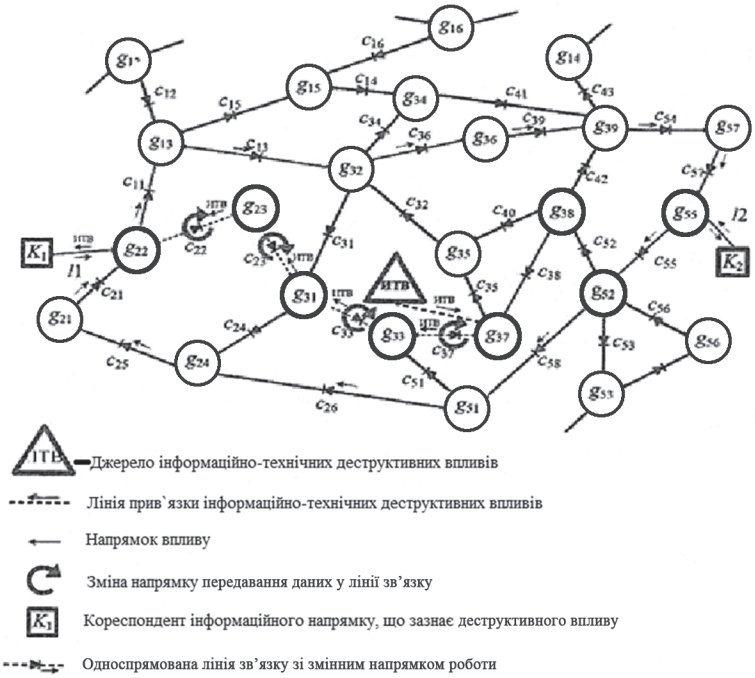


**Рис. 7. Схема зміни конфігурації маршруту тракту приймання кореспондента $K_1$ в інформаційному напрямку між кореспондентами $K_1$ і $K_2$, зумовлена ІТДВ та їхнім блокуванням, через перемикання напрямку, в якому здійснюється деструктивний вплив, на зворотний**

У блоці 17 здійснюється передавання поточного потоку даних зі збереженням актуального пакета даних, нагромаджених протягом часу зміни конфігурації маршруту тракту. Реалізація заходів за першим варіантом здатна заблокувати напрямок поширення ІТДВ, при цьому передавання даних лініями зв'язку продовжується у зворотному напрямку. Одночасно здійснюється корекція маршрутів трактів

приймання і/або передавання даних іншими інформаційними напрямками, в яких було задіяно лінії зв'язку зі зміненими напрямками роботи.

У другому варіанті, коли виявлено джерела ІТДВ, відбувається реалізація блоків 19-21. У блоці 19 здійснюється перемикання всіх ліній зв'язку вузла-кореспондента джерела ІТДВ на зворотний відносно вузла напрямок, що дає змогу фізично заблокувати передавання даних від цього вузла, як це показано на рис. 8.

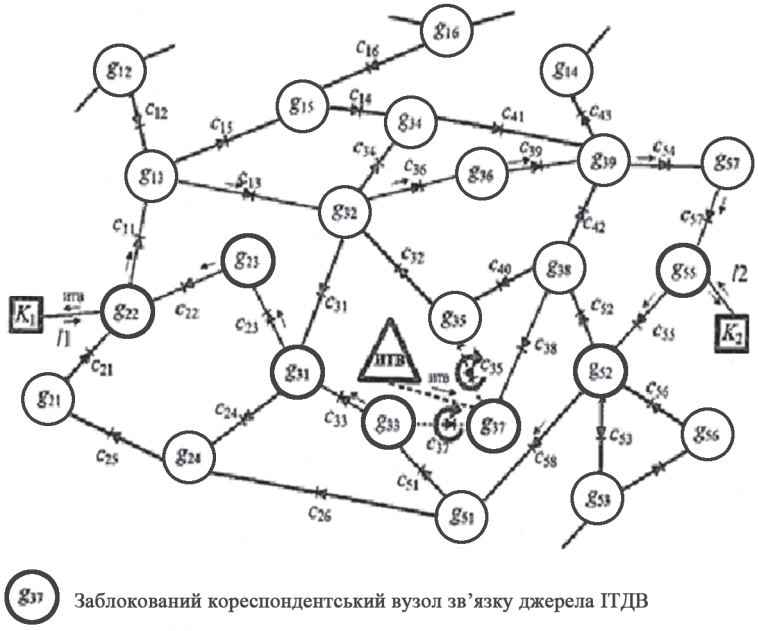


**Рис. 8. Схема блокування джерела ІТДВ у разі його виявлення через перемикання напрямку роботи всіх ліній зв'язку вузла, що його кореспондує, на зворотний**

Зміна напрямку потоків даних у лініях здійснюється за допомогою керованих ПОПД, як це схематично подано на рис. 3. У результаті такої реалізації унеможливлюється цільове функціонування джерела впливів відносно будь-якого об'єкта мережі, окрім власного вузла зв'язку, який кореспондує і якого буде вилучено з усіх маршрутів передавання даних, котрі його задіяли.

Отже, перехід від підходу об'єктового захисту кореспондентів і елементів мереж зв'язку до підходу групового захисту завдяки ізоляції джерел ІТДВ має право на існування. Реалізація блоків 20 та 21 аналогічні реалізаціям блоків відповідно 14 та 18.

У блоці 22 отримувач приймає пакети даних, а в блоці 23 здійснює передавання відправнику повідомлення про успішне приймання.

У блоці 24 із заданим періодом здійснюється перевірка ступеня завершеності сеансу. Період перевірки визначається на основі спостережень роботи мережі та інтенсивності ІТДВ.

### *Підвищення стійкості інформаційного напрямку завдяки пам'яті елементів телекомунікаційного обладнання*

Блоки 9 і 17, які відображені на рис. 5 і 6, забезпечують зберігання пакетів даних у пам'яті телекомунікаційного обладнання. Алгоритм збереження пакетів даних в оперативній пам'яті протягом допустимого часу їхнього перебування в черзі, що забезпечується блоками 1-5, з подальшим, за потреби, записом у постійну пам'ять елементів мережі, наведено на рис. 9.

Блок 6 забезпечує формування збереженої інформації в кореспондентську маршрутно-адресну таблицю, яка має таке подання:

$$T_{sk} = \{D_{1sk}, D_{2sk}, \ldots, D_{isk,\ldots,}, D_{Nsk},\}, \quad (5)$$

де $D_{isk}$ — матриця ваг, елементи якої $d_{isk}$ характеризують відомості про параметр збережених для $i$-го кореспондента даних.

У пам'яті елементів мережі пакети даних зберігаються доти, доки не надійшла команда видалення їх або через проміжок часу, протягом якого ці пакети були актуальні. Цей процес забезпечується блоками 7-13, в яких відбувається перевірка такої умови:

$$\tau_b \le t_{вд} + t_{вн} + t_{ввв}, \quad (6)$$

де $\tau_b$ — час актуальності передавання даних, який визначається протягом сеансу передавання даних для кожного з пакетів $b$ даних, $b = \overline{1,l}$, $l$ — кількість пакетів у потоці даних; $t_{вд}$ — час підготовки до

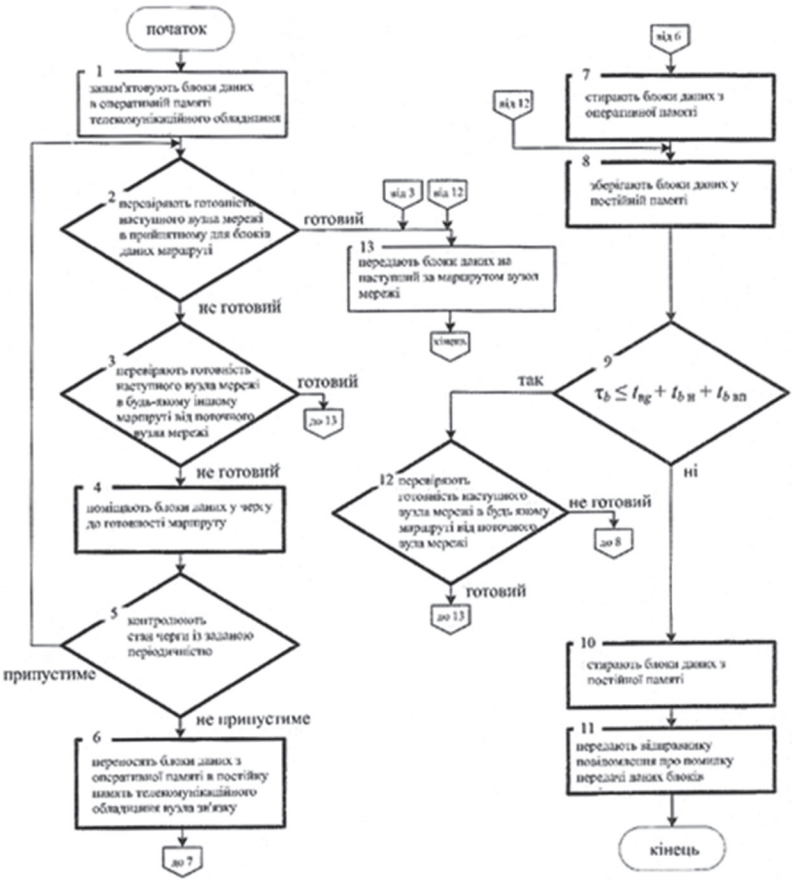


**Рис. 9. Алгоритм збереження пакетів даних у пам'яті телекомунікаційного обладнання**

передавання пакета даних на наступний вузол маршруту, який визначається найбільшим значенням імовірності; $t_{вн}$ — час, витрачений на передавання пакета даних; $t_{ввв}$ — час, протягом якого за умови справності всіх елементів мережі, здійснюється передавання даних від поточного вузла до одержувача.

У разі виявлення кореспондентом у блоці 22 (див. рис. 6) пошкоджених пакетів даних здійснюється аналіз елементів таблиці $T_{sk}(t)$ для ухвалення рішення щодо передавання потрібних пакетів із найбільш вигідних, тобто близьких за встановленими метриками алгоритму маршрутизації, вузлів зв'язку. Це зумовлює скорочення часу та підвищення ймовірності отримання кореспондентом актуальних даних, а також зменшення навантаження на пропускну здатність ліній мережі зв'язку.

Використання ресурсів постійної пам'яті телекомунікаційного обладнання вузлів зв'язку дасть змогу забезпечити цілісність потоків даних, яку може бути порушено внаслідок тимчасових затримок, що з'являються під час реалізації блоків 13-18 і 19-21 (див. рис. 5 і рис. 6).

### *Оцінювання ефективності*

Ефективність захисту кореспондента інформаційного напрямку й елементів мережі зв'язку від ІТДВ визначається реалізацією системного підходу до захисту, тобто завдяки блокуванню кореспондентського вузла зв'язку джерела впливів, який має назву групового захисту. Однак недоліком є те, що при цьому виникають затримки передавання даних в інформаційних напрямках. Це пов'язано з потребою в реконфігурації мережі. Крім того, функціонування мережі зв'язку супроводжується помилками процесів передавання даних внаслідок затримок. Причинами затримок можуть бути відмови роботи обладнання і/або перевищення пропускної здатності каналів зв'язку.

Здатність своєчасності передавання даних в інформаційному напрямку визначається можливістю зберігання пакетів даних протягом присутності помилок та зміни конфігурації в пам'яті телекомунікаційного обладнання. (На відміну від способів передавання даних, за яких у разі переповнення черги в оперативній пам'яті телекомунікаційного обладнання пакети даних видаляються). За допомогою запропонованої методики пакети даних у таких випадках записують у постійну пам'ять і відбувається їх збереження, поки не буде відновлено маршрут.

Переміщення пакетів даних за маршрутом інформаційного напрямку можна задавати за допомогою функції відстані від часу, як це зображено на рис. 10.

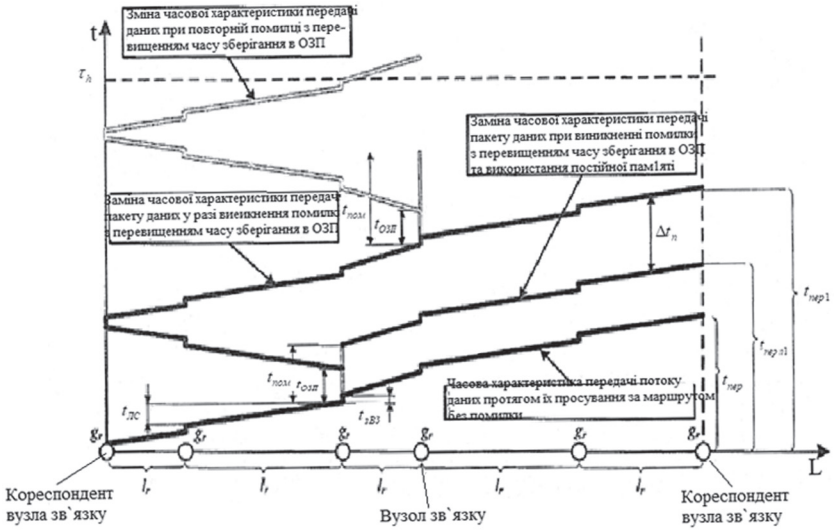


**Рис. 10. Процес просування блоків даних інформаційного напрямку за маршрутом**

Процес просування даних охоплює час передавання даних лініями зв'язку $t_{ЛЗ}$ та час їх проходження через вузли зв'язку $t_{зВЗ}$, а також часи зміни конфігурації маршруту, відмов і збоїв.

Процес передавання даних в інформаційному напрямку між вузлами зв'язку, що кореспондують без збоїв елементів мережі, характеризується сумарним часом: часом $t_{ЛЗ}$ проходження ліній зв'язку та часом $t_{зВЗ}$ їх проходження через вузли зв'язку. У разі виникнення помилки протягом часу $t_{пом}$ пакети даних протягом часу $t_{ОЗП}$ перебувають у черзі в оперативній пам'яті. Якщо маршрут відновлюється або з'являється новий протягом часу $t_{ОЗП}$, передавання пакетів даних триває. Через час $t_{ОЗП}$, у разі використання традиційних способів, кореспондент, який передає дані, отримує сигнал про помилку передавання пакетів даних, які передаються протягом часу $\tau_h$, дані передаються повторно або вони видаляються без повідомлення. У розробленій методиці передбачається, що після завершення часу $t_{ОЗП}$ пакети даних записуються в постійну пам'ять, де зберігаються протягом часу $t_{пом}$ помилки з подальшим передаванням їх за маршрутом. При зіставленні з традиційними способами цей варіант забезпечує виграш у часі передавання $\Delta t_п$, пропорційний до часу передавання даних від кореспондента до елемента, що відмовив. Крім того, під час використання традиційного підходу в разі повторних збоїв час передавання $\Delta t_п$ даних зростає порівняно з показниками рішення, запропонованого авторами.

Ефективність зменшення навантаження на пропускну здатність ліній зв'язку визначається вивільненням їхніх ресурсів завдяки відсутності повторного передавання даних в інформаційних напрямках у разі зміни конфігурації мережі зв'язку та збоїв її елементів.

Імовірність своєчасного передавання даних визначається в разі виконання нерівності $t_{пер} \le \tau_h$ та обчислюється так:

$$P_{пер} = \frac{\sum m(t/t \le \tau_h)}{n}, \qquad (7)$$

де $n$ — загальна кількість пакетів у відправленому потоці інформаційного напрямку; $m(t/t \le \tau_h)$ — своєчасно прийнятий пакет даних. Порівняльна характеристика, наведена на рис. 10, підтверджує зростання ймовірності своєчасного приймання даних за реалізації розробленої методики відносно традиційних підходів.

## *ВИСНОВКИ*

Запропонована методика дає можливість забезпечити стійкість інформаційних напрямків (векторів), які функціонують за умов ІТДВ. Очікуваний ефект від її впровадження полягає в істотному підвищенні стійкості процесів передавання даних в інформаційно-комунікаційних системах.

У підсумку забезпечується таке:

♦ підвищення захищеності кореспондентів і елементів мережі зв'язку завдяки керованому фізичному рознесенню в структурі мережі зв'язку трактів приймання і передавання інформаційних напрямків, що виключає наявність фізичного шляху реалізації деструктивних ІТДВ;

♦ підвищення ймовірності передавання даних, зниження часу їхнього передавання та навантаження на пропускну здатність ліній зв'язку за умов зміни конфігурації мережі, відмов і перевантажень її елементів завдяки використанню в процесі передавання даних пам'яті телекомунікаційного обладнання.

Запропонована методика, на відміну від наявних, дає можливість здійснювати такі дії:

• реалізовувати перехід від підходу об'єктового захисту кореспондентів і елементів мереж зв'язку до підходу групового захисту (ізоляції джерел ІТДВ);

• підвищувати ймовірність передавання даних у мережах зв'язку з пам'яттю за умов блокування поширення ІТДВ та кореспондентських вузлів їхніх джерел;

• зменшувати час передавання потоку даних і навантаження на пропускну здатність простих каналів із боку інформаційного напрямку під час зміни конфігурації мережі, відмов і перевантажень її елементів завдяки використанню в процесі передавання даних пам'яті устаткування транзитних вузлів, що зумовлює наукову новизну та практичну значущість методики.

Використання ресурсів постійної пам'яті телекомунікаційного обладнання зв'язку забезпечує цілісність потоків даних, порушення якої виникає внаслідок тимчасових затримок. При цьому своєчасність одержання кореспондентами потрібних даних підтримується завдяки маршрутизації від найвигідніших вузлів, що визначаються на основі введеної в методиці кореспондентської векторно-адресної таблиці, яка систематизує інформацію про збережені на вузлах складових каналів дані.

Отже, у статті репрезентовано нову методику, що дає змогу компенсувати зниження структурної стійкості мережі зв'язку за умов ІТДВ через підвищення стійкості інформаційного обміну завдяки використанню пам'яті елементів телекомунікаційного обладнання.

***Список використаної літератури***

*1. **Грищук Р. В., Даник Ю. Г.** Основи кібернетичної безпеки: монографія / за заг. ред. проф. Ю. Г. Даника. Житомир: ЖНАЕУ, 2016. 636 с.*

*2. **Грабар І. Г., Грищук Р. В., Молодецька К. В.** Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія / за заг. ред. д.т.н., проф. Р. В. Грищука. Житомир: ЖНАЕУ, 2019. 280 с.*

*3. **Шеховцов В. І.** Зменшення впливу людських чинників як захист підвищення якості експлуатації інформаційних управляючих систем // Автоматизовані системи керування та прилади автоматики. 2019. Вип. 176. С. 74–79.*

*4. **Кількісно-якісна** оцінка та визначення рівня кібербезпеки інформаційних систем держави / І. В. Пискун, Ю. М. Ткач, В. О. Хорошко [та ін.] // Ukrainian Scientific journal of Information Security. 2020. Vol. 26, issue 3. P. 131–138.*

*5. **Золотарьов Д. О.** Автоматизоване розгортання програмного оточення для мікросервісів в умовах швидкого мінливого технологічного стеку // Сучасний стан наукових досліджень та технологій в промисловості. 2021. Вип. №4 (18). С. 23–30.*

*6. **https:**//niss.gov.ua/doslidzhennya/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya-chetvertoi-promislovoi [Електронний ресурс].*

*7. **Коваленко А. А., Кучук Г. А., Ткачов В. М.** Метод забезпечення живучості комп'ютерної мережі на основі VPN-тунелювання // Системи керування, навігації і зв'язку. 2021. Вип. 1(63). С. 90–96.*

*8. **Лемешко А. В., Новіченко Є. О., Недавній А. В.** Безпека даних в Україні за допомогою використання технологій VPN // Наук. журн. «IT synergy». 2022. Вип. 2(3). С. 28–42.*

*9. **https:**//ela.kpi.ua/bitstream/123456789/25156/1/Tarnavsky_Kuzmenko_Org_Komp_merej.pdf [Електронний ресурс].*

*10. **https:**//allref.com.ua/uk/skachaty/Suchasni_antivirusni_programi_ta_princip_yih_roboti [Електронний ресурс].*

*11. **Підходи** до захисту інформації в інформаційно-телекомунікаційних системах, що побудовані з використанням хмарних технологій / М. М. Радченко, О. В. Дикий, Н. А. Паламарчук [та ін.] // Вісник Військового інституту телекомунікацій та інформатизації імені Героїв Крут. Комунікаційні та інформаційні системи. 2021. Вип. №2. Київ: ВІТІ. С. 82–95.*

*12. **Єсін В. І., Рассомахін С. Г., Вілігура В. В.** Аналіз формальних моделей забезпечення цілісності даних і їх застосування для баз даних // Радіотехніка, №204. С. 30–39.*

*13. **https:**//tks.nau.edu.ua/wp-content/uploads/2016/05/Zahyst-informatsiyi-v-telekomunikatsijnyh-systemah.pdf [Електронний ресурс].*

*14. **Мохунь І. І., Вікторовська Ю. Ю., Галушко Ю. К.** Оптичні технології в інформаційній техніці // Чернівці, нац. ун-т., 2021. 301 с.*

*15. **https:**//ktpu.kpi.ua/wp-content/uploads/2014/02/Vorobiyenko-P.P.-Telekomunikatsijni-ta-informatsijni-merezhi.pdf [Електронний ресурс].*

*16. **https:**//ela.kpi.ua/bitstream/123456789/36689/1/Zhurakovkyi_Zeniv_Kompiuterni_merezhi_lab.pdf [Електронний ресурс].*

*G. V. Shuklin, E. V. Bondarenko*

**METHODOLOGY FOR ENSURING THE SUSTAINABILITY OF THE INFORMATION DIRECTION IN THE CONDITIONS OF INFORMATION AND TECHNICAL INFLUENCES ON THE ELEMENTS OF THE MEMORY COMMUNICATION NETWORK**

*The article presents a methodology for ensuring the stability of the information direction (vector) in the conditions of information and technical destructive impacts (ITDI) on the elements of the memory communication network. The possibility of realizing the transition from the approach of object protection of correspondents and elements of communication networks to the approach of group protection is substantiated, as well as increasing the reliability of data transmission under conditions of blocking the spread of destructive ITI and corresponding nodes of their sources. It is shown that ensuring the stability of the information direction (vector) is achieved, firstly, by increasing the security of correspondents and elements of the communication network due to the controlled physical separation of the paths for receiving and transmitting information directions (vectors), which excludes the presence of a physical path for the implementation of destructive ITEs, and, secondly, by increasing the probability of data transmission, reducing the time of their transmission and the load on the bandwidth of communication lines in the conditions of network reconfiguration, failures and overloads of its elements due to the use of in the process of protecting against destructive ITOs.*

**Keywords:** sustainability, information areas, information and technical influences, destructive influences, information security.