УДК 004.056.5 DOI: 10.31673/2412-4338.2022.040413

Гринкевич Г.О., Захаржевський А.Г.
Державний університет телекомунікацій, м. Київ

ПОБУДОВА ЗАХИЩЕНОЇ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ В УМОВАХ ІНФОРМАЦІЙНО-ТЕХНІЧНИХ ВПЛИВІВ НА ЕЛЕМЕНТИ МЕРЕЖІ ЗВ'ЯЗКУ З ПАМ'ЯТТЮ

Анотація: *Досліджено питання побудови захищеної інфокомунікаційної мережі в умовах інформаційно-технічних впливів на елементи мережі зв'язку з пам'яттю. Представлено методику побудови захищеної інфокомунікаційної мережі в умовах інформаційно-технічних впливів на елементи мережі зв'язку з пам'яттю. Були обґрунтовані можливість здійснення переходу від об'єктового захисту кореспондентів та елементів мережі зв'язку до групового захисту, а також підвищення ймовірності передачі даних у випадку блокування розповсюдження деструктивних інформаційно-технічних впливів та вузлів їхніх джерел. Виявлено, що забезпечення стійкості інформаційного потоку можна досягти, по-перше, шляхом підвищення захищеності кореспондентів та елементів мережі зв'язку через кероване фізичне розташування трактів передачі та отримання інформації, що унеможливлює наявність фізичного шляху для здійснення деструктивних впливів. По-друге, можна забезпечити підвищення ймовірності передачі даних, зменшення часу передачі та навантаження на пропускну здатність ліній зв'язку при реконфігурації мережі, відмов та перевантажень її елементів завдяки використанню пам'яті телекомунікаційного обладнання у процесі передачі даних.*

Ключові слова: *інфокомунікаційні мережі зв'язку, інформаційні напрямки, інформаційно-технічні впливи, деструктивні впливи, інформаційна безпека.*

Grynkevych G., Zakharzhevsky A.
State University of Telecommunications, Kyiv

CONSTRUCTION OF A PROTECTED INFOCOMMUNICATION NETWORK UNDER THE CONDITIONS OF INFORMATION-TECHNICAL INFLUENCES ON THE ELEMENTS OF THE MEMORY COMMUNICATION NETWORK

Abstract: *Ensuring a secure information and communication network with memory requires a comprehensive approach that includes the use of modern encryption algorithms, hash functions, firewalls, VPN, and multi-factor authentication, as well as continuous monitoring and auditing of the network. Only such a comprehensive approach will allow for a high level of network security.*

Digitization, informatization, and globalization have provided the foundation for the formation of one of the most complex systems - cyberspace, which provides a wide range of information and communication services to the international community in various areas of life. The increasing pace of development of this system, its coverage and penetration into all spheres have led to the emergence of new forms of threats in cyberspace.

The maximum damage from the realization of threats in cyberspace, which are carried out through information and technical influences, is determined by the potential harm caused to the target during its critical operational mode. Critical infrastructure has an especially high potential for harm. Its operation is usually ensured by an automated system for managing the technological process, the components of which communicate through communication networks.

The issue of building a secure information and communication network in conditions of information and technical influences on communication network elements with memory has been investigated. A methodology for building a secure information and communication network in conditions of information and technical influences on communication network elements with memory has been presented. The possibility of transitioning from object protection of correspondents and

communication network elements to group protection, as well as increasing the likelihood of data transmission in the event of blocking the spread of destructive influences and nodes of their sources, has been substantiated. It has been found that ensuring the stability of the information flow can be achieved, firstly, by increasing the security of correspondents and communication network elements through controlled physical placement of transmission and reception paths, as well as the use of modern means of protection, and secondly, by creating a system of continuous monitoring and auditing of the network.

Keywords: *information communication networks, information directions, information and technical influences, destructive influences, information security.*

1. Вступ

Сьогодні відомості є найціннішим ресурсом для бізнесу та громадянського суспільства. Однак, ці відомості є уразливими перед зловмисниками, які намагаються отримати несанкціонований доступ до них. Тому створення захищеної інфокомунікаційної мережі стає дедалі більш важливим завданням для бізнесу та держави.

Одним з найважливіших елементів будь-якої мережі зв'язку є пам'ять. Вона зберігає всі дані, які проходять через мережу, включаючи конфіденційну інформацію про користувачів. Тому забезпечення захисту елементів мережі з пам'яттю є однією з ключових складових для створення захищеної інфокомунікаційної мережі.

Першим кроком в побудові захищеної інфокомунікаційної мережі є вибір правильного алгоритму шифрування для забезпечення конфіденційності даних, що пересилаються через мережу. Алгоритми шифрування захищають дані від несанкціонованого доступу шляхом перетворення їх у нечитабельний формат до того, як вони будуть відправлені через мережу. Найпоширенішим алгоритмом шифрування є AES (Advanced Encryption Standard).

Наступним кроком є використання протоколів безпеки, таких як SSL (Secure Sockets Layer) та TLS (Transport Layer Security), для забезпечення захищеної передачі даних через мережу. Ці протоколи застосовуються в основному для захисту веб-сайтів, але їх можна використовувати і для захисту інших типів мереж.

Для забезпечення цілісності даних, які передаються через мережу, можна використовувати хеш-функції, яка перетворює будь-який блок даних на фіксований хеш-код. Якщо блок даних буде змінений під час передачі, хеш-код також зміниться, що дозволяє виявити будь-які зміни в даних. Хеш-функції, такі як SHA-2 (Secure Hash Algorithm 2), можуть бути використані для забезпечення цілісності даних.

Для захисту від атак на мережевий рівень можна використовувати брандмауери, які дозволяють обмежувати доступ до мережевих ресурсів. Брандмауери можуть контролювати вхідні та вихідні з'єднання, фільтрувати мережевий трафік та блокувати певні типи трафіку, що дозволяє зменшити ризик атак на мережевий рівень.

Іншими методами захисту є використання VPN (Virtual Private Network), що дозволяє створювати захищені тунелі для передачі даних через неприхильні мережі, а також використання мультифакторної аутентифікації, котра вимагає двох або більше методів аутентифікації, таких як пароль та код підтвердження, що дозволяє забезпечити вищий рівень безпеки.

Нарешті, важливо вести постійний моніторинг та аудит мережі для виявлення потенційних загроз та вразливостей, а також для запобігання вторгненням та шкідливому програмному забезпеченню. Цей процес допомагає виявляти незвичайну активність на мережі та реагувати на неї з метою забезпечення безпеки мережі.

Отже, забезпечення захищеної інфокомунікаційної мережі з пам'яттю вимагає комплексного підходу, що включає в себе використання сучасних алгоритмів шифрування, хеш-функцій, брандмауерів, VPN та мультифакторної аутентифікації, а також постійного моніторингу та аудиту мережі. Тільки такий комплексний підхід дозволить забезпечити високий рівень безпеки мережі з пам'яттю.

2. Аналіз досліджень і публікацій. Цифровізація, інформатизація та глобалізація послугували підґрунтям для формування однієї з найскладніших систем – кіберпростору, що надає широкий спектр інфокомунікаційних послуг міжнародному співтовариству в різних сферах життєдіяльності. Наростаючі темпи розвитку цієї системи, її охоплення і проникнення в усі сфери зумовили виникнення нових форм загроз у кіберпросторі [1,2].

Максимальний збиток від реалізації загроз у кібер-просторі, що здійснюються за допомогою інформаційно-технічних впливів (ІТВ), визначається потенційною шкодою, яка завдається об'єктом атаки під час його виходу в закритичний режим експлуатації. Особливо високий потенціал шкоди має критична інфраструктура. Її функціонування, як правило, забезпечується автоматизованою системою управління технологічним процесом, складові елементи якої комунікують за допомогою мереж зв'язку [3-5].

Виникнення нових форм загроз [6] призвело до створення теорії та практики захисту від ІТВ. Сучасні масово застосовувані методи і способи захисту інфокомунікаційних послуг реалізують різні напрямки: розмежування ресурсів – фізичних (наприклад, просторовий рознос напрямних середовищ) і логічних (таких, як технологія VPN [7, 8]), а також міжмережеве екранування [9], антивірусний захист [10, 11] тощо. Необхідно зазначити, що в наявних методах і способах використовується, як правило, об'єктовий підхід.

Ступінь уразливості послуг і сервісів інфокомунікаційних мереж для деструктивних ІТВ залежить від їхнього рівня в моделі OSI (Open Systems Interconnection model). Так, підвищення рівня акумулює уразливості всіх нижчих рівнів, розширюючи можливий перелік загроз. Справедливе і зворотне твердження: усунення вразливостей на нижчому рівні ліквідує загрози і на всіх вищих рівнях.

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

Таким чином, виникає актуальне наукове завдання – забезпечення стійкості інформаційних напрямків шляхом блокування ІТВ на нижньому (фізичному) рівні моделі OSI мережі зв'язку.

3. Мета дослідження. Метою дослідження даної статті є розгляд питань, пов'язаних з побудовою захищеної інфокомунікаційної мережі з пам'яттю в умовах інформаційно-технічних впливів на елементи мережі зв'язку з пам'яттю, тобто забезпечення безпеки інфокомунікаційної мережі з пам'яттю в умовах інформаційно-технічних впливів на елементи мережі зв'язку з пам'яттю.

4. Сутність методики побудови захищеної інфокомунікаційної мережі в умовах інформаційно-технічних впливів на елементи мережі зв'язку з пам'яттю

Запропонована методика ґрунтується на принципі блокування напряму (лінії зв'язку), за яким поширюється ІТВ. Надалі відбувається блокування і самого джерела ІТВ, що досягається шляхом керованого фізичного рознесення трактів передавання і приймання інформаційних напрямків між кореспондентами в структурі мережі зв'язку. Завдяки цьому виключається наявність доступного фізичного шляху для реалізації деструктивних впливів. Компенсація можливих втрат даних під час реконфігурації напрямків роботи ліній мережі зв'язку здійснюється за рахунок пам'яті її елементів.

Показником ефективності методики є ймовірність своєчасного отримання даних в інформаційному напрямку $P_{пер}\ (t|t< \tau_h)$ на необхідному часовому інтервалі t_y.

Для побудови захищеної інфокомунікаційної мережі в умовах інформаційно-технічних впливів на елементи мережі зв'язку з пам'яттю запроваджуються такі обмеження:

- розглядають мережу зв'язку з пам'яттю в стаціонарному стані з дуплексними лініями зв'язку (графічно подано на рис. 1, де пр - приймання; пер - передавання; кз - канал зв'язку; КУ - канальне устаткування; ЛО -лінійне устаткування);
- елементи мережі зв'язку функціонують в умовах ІТВ;

- кореспонденти інформаційних напрямків не переміщуються.

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

Вихідні дані в методиці:

- склад мережі зв'язку, що включає G вузлів і L ліній, і структура у вигляді графа R = (G, L);
- H категорій даних, які задають за різними ознаками (як ознаки можуть виступати, наприклад, пріоритет передавання даних, граничний час доставки, вид даних, що передаються, та ін.);
- вимоги кореспондентів до інформаційного обміну, які визначаються категорією переданих даних, швидкістю введення/виведення вихідного/вхідного трафіку, достовірністю передання, граничним часом доставки (тобто своєчасністю - допустимим часом тл передачі h-ї категорії даних, що визначаються потребами кореспондентів, де h = 1,2,...,H), пріоритетом передавання, часом сталого функціонування ty, протягом якого буде забезпечено своєчасність передавання даних з імовірністю $P_{пер}$ и др.;
- вимоги до маршрутів, які обумовлюють порядок вибору алгоритму маршрутизації на кожен сеанс зв'язку між кореспондентами в інформаційному напрямку;
- правила рознесення трактів приймання і передавання на транзитних елементах мережі зв'язку, що беруть участь у складанні маршрутів між кореспондентами інформаційних напрямків, які унеможливлюють перетин трактів приймання і передавання на фізичних елементах мережі. До мережі зв'язку передавання даних в інформаційних напрямках у різних умовах;
- інтервали оновлення даних про метрики елементів мережі, що залежать від показників динаміки. Оновлення даних у маршрутно-адресних таблицях здійснюється на основі протоколів взаємодії;
- інформаційні напрямки кореспонденти-користувачі підключаються дуплексними лініями (див. рис. 1), тому рознесення трактів приймання та передавання інформаційних напрямків у лінії прив'язки до вузла-корреспондента не здійснюється;
- P метрик елементів мережі, які дають змогу описати їхній стан із достатнім рівнем для ухвалення рішення на формування маршрутів передавання даних в інформаційних напрямках у різних умовах;
- інтервали оновлення даних про метрики елементів мережі Δt_p, що залежать від показників динаміки. Оновлення даних у маршрутно-адресних таблицях здійснюється на основі протоколів взаємодії.
- інформаційні напрямки кореспондента Ik. Місця підключення кореспондентів входять до переліку метрик елементів мережі;
- алгоритми маршрутизації. Варіант та критерії роботи алгоритмів обумовлюються вимогами до стійкості інформаційного напряму 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 [16-18].

Критерієм імовірності функціонування інформаційного напряму на необхідному часовому інтервалі є нормативні значення вимог системи управління до зв'язку.

У процесі роботи використовувалися такі методи: метод маршрутизації даних у мережах зв'язку з пам'яттю, відмовами і перевантаженнями; теорія графів; теорія ймовірності.

5. Опис процесу роботи запропонованої методики

Розглянемо роботу методики щодо одного інформаційного напряму, що функціонує на ресурсах мережі зв'язку з пам'яттю. Основні елементи методики подано блок-схемою на рис. 2 і рис. 3.

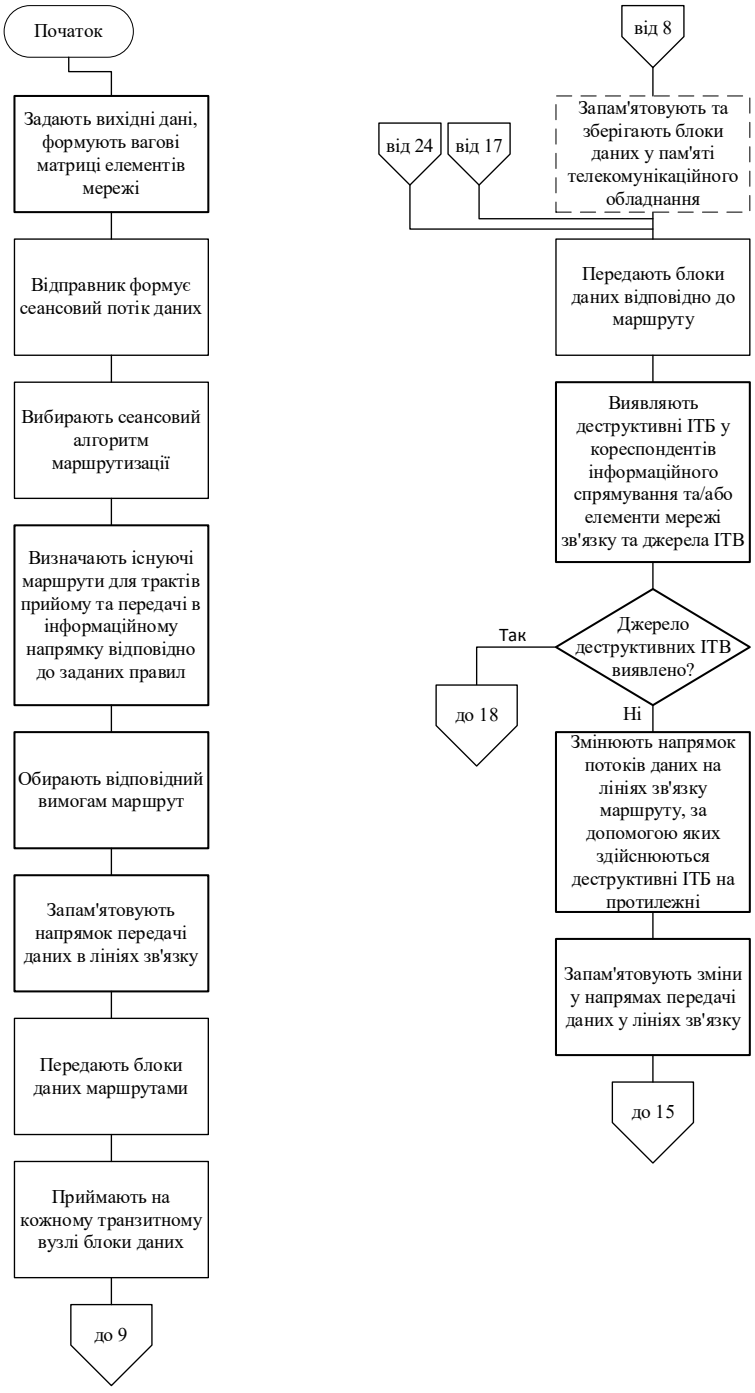

Рис. 2. Алгоритм побудови захищеної інфокомунікаційної мережі в умовах інформаційно-технічних впливів на елементи мережі зв'язку з пам'яттю (частина перша)

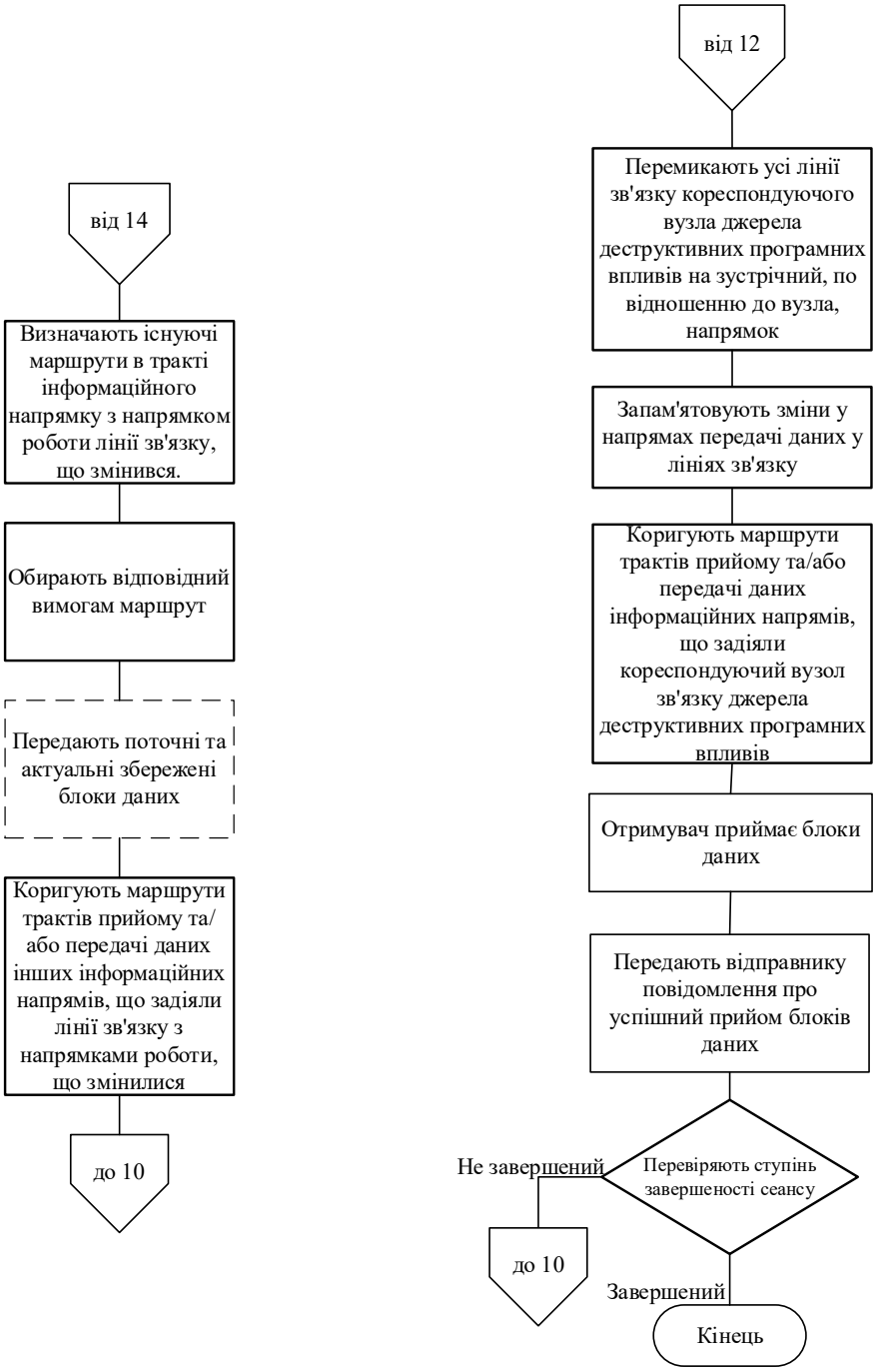

Рис. 3. Алгоритм побудови захищеної інфокомунікаційної мережі в умовах інформаційно-технічних впливів на елементи мережі зв'язку з пам'яттю (частина перша)

У *блоці 1* задають вихідні дані та формують P вагових матриць графа мережі за відповідними метриками, включно з метриками, які описують напрямок роботи ліній зв'язку і мають період оновлення t_p:

$$D_p(t) = (d_{p\,qj}(t))^{R,R}_{q=1,\,j=1}; \quad (1)$$

$$D_{Pdc}(t) = (d_{Pdc\,qj}(t))^{R,R}_{q=1,\,j=1}, \quad (2)$$

де d_{pqj} и $d_{Pdc\,qj}$ 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:

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

яка характеризується односпрямованістю ребер графа мережі.

У блоці 2 кореспонденти інформаційного напрямку формують сеансовий потік даних. Його характеристики є умовами вибору алгоритму маршрутизації на поточний сеанс у блоці 3. На основі обраного алгоритму маршрутизації в блоці 4 визначають, з урахуванням завантаження ресурсів мережі, кількість M наявних маршрутів в інформаційному напрямку, за якими можна передавати неподільні складові потоку даних.

Кількість маршрутів обчислюється покроково методом динамічного програмування, причому вони будуть збільшуватися поетапно – по мірі просування вершинами мережі. Кількість маршрутів до поточної вершини M залежатиме тільки від кількості маршрутів до попередніх вершин $M_{поп}$, ребра яких входять у поточну вершину:

$$M = \sum_{поп} M_{поп}.$$

У блоці 5 обирають ті, що відповідають вимогам маршрути передач і даних, по одному з яких у блоці 7 передають блоки даних. При цьому в блоці 6 запам'ятовують параметри напряму передачі даних у лініях зв'язку у відповідних матрицях.

У блоках 7-10 передають дані в інформаційних напрямках із проміжним дублюванням у пам'яті елементів складових каналів (за методом маршрутизації даних у мережі зв'язку з пам'яттю, відмовами та перевантаженням і) і допустимим часом tdon g, для того, щоб забезпечити стійкість інформаційного обміну в умовах масових незалежних і залежних збоїв елементів мережі.

Пропоноване рішення щодо реакції мережі зв'язку на деструктивні ІТВ для кореспондентів інформаційного напряму, а також елементи мережі зв'язку, які надходять по трактах приймання/передавання даних, описується блоками 11-21. При цьому залежно від факту виявлення джерела ІТВ (блок 12) передбачається можливість двох варіантів реконфігурації роботи елементів мережі.

У першому варіанті (якщо джерело не виявлено) змінюють напрямок роботи ліній зв'язку маршрут, за допомогою якого здійснюють вплив, на протилежний (блок 13), а в блоці 14 відображають ці зміни в матрицях (1)-(3). У блоці 15 визначаються, існуючі маршрути в тому тракті інформаційно, напрямки, на який вплинули зміни напряму роботи ліній зв'язку (визначення маршрутів можна здійснити за блоком 4). Маршрути визначають, згідно з вимогами, позначеними в блоці 1, і в блоці 16 обирають один із них відповідно до правил рознесення (рис. 4).

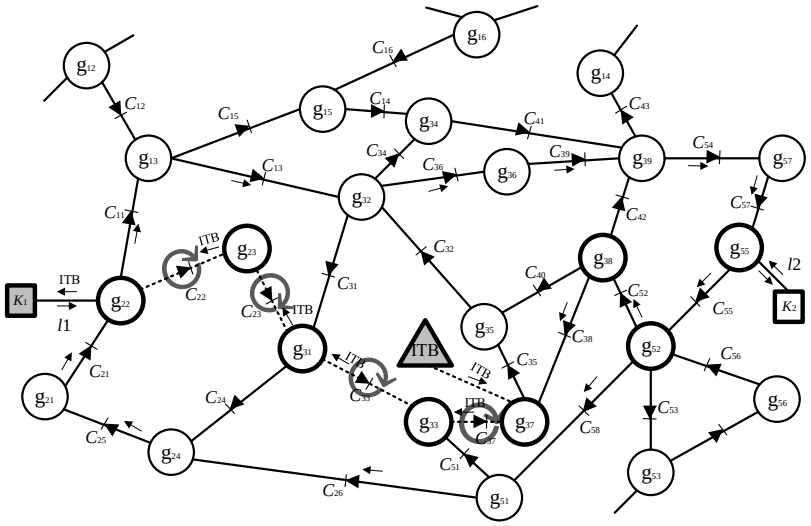

Рис. 4. Реконфігурація маршруту тракту приймання кореспондента К1 в інформаційному напрямі між кореспондентами $К_1$ і $К_2$, зумовлена деструктивними ІТВ та їхнім блокуванням, шляхом перемикання напрямків роботи ліній зв'язку, якими здійснюється вплив, на

протилежний, де ІТВ - джерело інформаційно-технічних впливів; Кі - кореспондент інформаційного напряму, що зазнав деструктивного впливу.

У блоці 17 передають поточний потік даних і актуальні збережені блоки даних, накопичених за час реконфігурації маршруту зміненого тракту.

Реалізація дій за першим варіантом дає змогу заблокувати напрямок поширення деструктивних ІТВ; передача даних політикам зв'язку триває в протилежному напрямку. При цьому здійснюється корекція маршрутів трактів трактів приймання та/або передавання даних решти інформаційних напрямків, у яких були задіяні лінії зв'язку зі зміненими напрямками роботи.

Реконфігурація маршруту тракту приймання кореспондента К1 в інформаційному напрямі між кореспондентами К1 і К2, зумовлена деструктивними ІТВ та їхнім блокуванням шляхом перемикання напрямків роботи ліній зв'язку.

У другому варіанті (при виявленні джерела деструктивних ІТВ) виконуються дії блоків 19-21. У блоці 19 перемикають усі лінії зв'язку вузла-корреспондента джерела ІТВ на зустрічний (стосовно вузла) напрямок, що дає змогу фізично заблокувати передавання даних від цього вузла (рис. 5). Зміна напрямку потоків даних у лініях здійснюється за допомогою керованих ПОПД. Унаслідок цієї дії унеможливлюється цільове функціонування джерела впливів стосовно будь-якого об'єкта мережі, окрім його вузла зв'язку, який кореспондує і який буде виключено з усіх маршрутів передавання даних, що задіяли його.

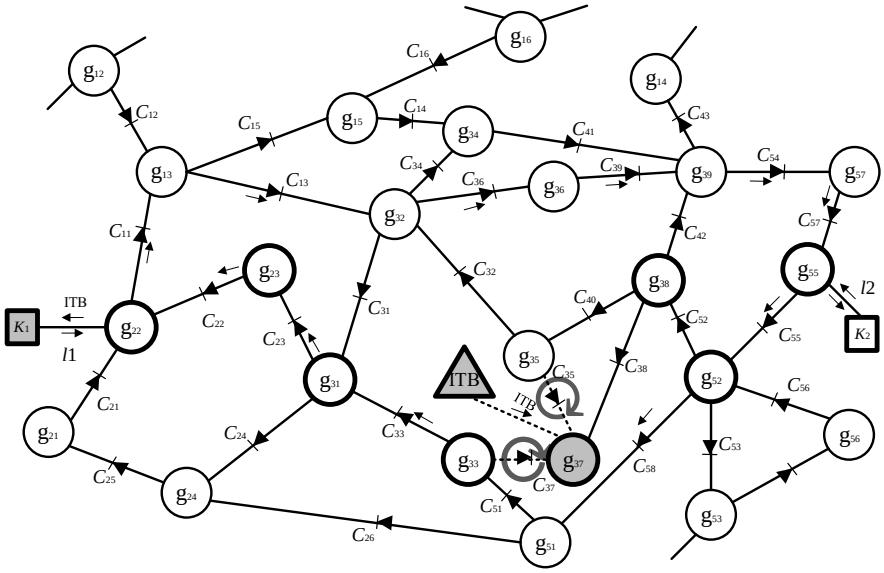

Рис. 5. Блокування джерела деструктивних ІТВ у разі його виявлення шляхом перемикання напрямку роботи всіх ліній зв'язку вузла, що його кореспондує, на зустрічний, де g_{17} - заблокований кореспондуючий вузол зв'язку джерела деструктивних ІТВ.

Таким чином, перехід від підходу об'єктового захисту кореспондентів і елементів мереж зв'язку до підходу групового захисту шляхом ізоляції джерел деструктивних ІТВ можливий.

Дії блоків 20 і 21 аналогічні діям блоків 14 і 18 відповідно.

У блоці 22 одержувач приймає блоки даних і в блоці 23 передає відправнику повідомлення про успішний прийом. У блоці 24 із заданою періодичністю перевіряється ступінь завершеності сеансу. Періодичність перевірки може задаватися на найгірший випадок або варіюватися відповідно до інтенсивності зміни показників стану елементів мережі.

6. Аналіз ефективності використання запропонованого методу

Ефективність захисту кореспондента інформаційного напряму та елементів мережі зв'язку від деструктивних ІТВ визначається реалізацією системного підходу до захисту – шляхом блокування кореспондуючого вузла зв'язку джерела впливів (груповий захист). Однак при цьому неминуче виникають затримки передач і даних в напрямку пов'язаного з необхідністю реконфігурації мережі. Крім того, функціонування мережі зв'язку супроводжується збоями процесів передавання даних, що спричиняють відповідні затримки tсб. Причинами затримок можуть бути відмови обладнання tотк і перевищення пропускної спроможності каналів зв'язку tпрев.

Ефективність своєчасності передавання даних в інформаційному напрямку визначається можливістю зберігання блоків даних під час збоїв і реконфігурації в постійній пам'яті телекомунікаційного обладнання. Потім відбувається їх подальше передавання після відновлення (появи) маршруту, На відміну від способів передавання даних, в яких при переповненні черги в оперативній пам'яті телекомунікаційного устаткування блоки даних видаляються, у розробленій методиці вони переносяться в постійну пам'ять до відновлення маршруту.

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

6. Висновки

У світі, де все більше інформації передається через мережі зв'язку, забезпечення захищеної інфокомунікаційної мережі з пам'яттю стає дедалі важливішим завданням. Водночас, з'являється все більше нових загроз та вразливостей, що вимагає постійного удосконалення методів захисту мереж. Застосування сучасних методів шифрування, контролю доступу та моніторингу мережі може допомогти забезпечити безпеку інфокомунікаційної мережі з пам'яттю в умовах інформаційно-технічних впливів на елементи мережі зв'язку з пам'яттю.

Запропонована методика спрямована на забезпечення стабільності інформаційних напрямків, що функціонують в умовах інформаційно-технологічної війни. Очікується, що впровадження цієї методики значно підвищить стійкість процесів передачі даних в інформаційних напрямках. Також, використання нових підходів до захисту інформаційних напрямків дозволяє реалізувати перехід від підходу об'єктового захисту до підходу групового захисту, що забезпечує більш ефективний захист мережі від деструктивних інформаційних впливів. Крім того, використання кореспондентської маршрутно-адресної таблиці та вузлів маршрутизації дозволяє знизити час передавання потоку даних та підвищити ймовірність їх успішного передавання.

Отже, представлена методика дозволяє забезпечити стійкість інформаційних напрямків в умовах ІТВ та підвищити ефективність передавання даних в мережах зв'язку, що забезпечує її наукову новизну та практичну значущість.

Список використаної літератури:

1. Шкода від кібератак на критичну інфраструктуру: механізми вимагання викупу / О. О. Башков, В. М. Кузьмін // Проблеми захисту інформації. - 2018. - Т. 21, № 1. - С. 36-45. (https://doi.org/10.20535/2307-7502.2018.21.1.128456)

2. Міністерство цифрової трансформації України. Кібербезпека: захист критичної інфраструктури (https://thedigital.gov.ua/ua/post/kiberbezpeka-zahist-krytychnoi-infrastruktury)

3. Захист критичної інфраструктури від кіберзагроз / Ю. П. Волков, В. В. Куценко, А. С. Рак // Науковий вісник Міжнародного гуманітарного університету. - 2017. - Вип. 25, Ч. 1. - С. 39-41. (http://nbuv.gov.ua/UJRN/Nvmgu_2017_25_1_13)

4. Кібербезпека критичної інфраструктури: проблеми та шляхи їх вирішення / В. М. Борисенко, О. О. Ліщук, І. В. Колінько та ін. // Проблеми захисту інформації. - 2019. - Т. 22, № 1. - С. 43-49. (https://doi.org/10.20535/2307-7502.2019.22.1.178439)

5. Кібербезпека критичної інфраструктури: технології та методи захисту / Н. В. Колодяжна, С. В. Пархоменко, І. В. Роговенко та ін. // Електронне наукове фахове видання "Інформаційні технології та комп'ютерна інженерія". - 2020. - Вип. 1(47). - С. 37-48. (http://ite.khpi.edu.ua/article/view/195054/193638)

6. Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.011

7. Cisco Systems, Inc. (2017). VPNs and VPN Technologies. https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/index.html

8. Microsoft Corporation. (2022). Virtual Private Network (VPN). https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/about-vpn-devices-for-always-on-vpn

9. Zhang, J., Huang, D., & Zhang, Y. (2019). A novel hybrid intrusion detection system for network security in the IoT environment. Journal of Network and Computer Applications, 136, 108-119. https://doi.org/10.1016/j.jnca.2019.03.020

10. Symantec Corporation. (2022). Endpoint Protection. https://www.symantec.com/products/endpoint-protection

11. McAfee, LLC. (2022). Antivirus Software. https://www.mcafee.com/enterprise/en-gb/products/antivirus-software.html

References:

1. Damage from cyber attacks on critical infrastructure: ransomware mechanisms / O. O. Bashkov, V. M. Kuzmin // Information Security Problems. - 2018. - Vol. 21, No. 1. - P. 36-45. (https://doi.org/10.20535/2307-7502.2018.21.1.128456)

2. Ministry of Digital Transformation of Ukraine. Cybersecurity: protection of critical infrastructure (https://thedigital.gov.ua/ua/post/kiberbezpeka-zahist-krytychnoi-infrastruktury)

3. Protection of critical infrastructure from cyber threats / Yu. P. Volkov, V. V. Kutsenko, A. S. Rak // Scientific Bulletin of the International Humanities University. - 2017. - Issue 25, Part 1. - P. 39-41. (http://nbuv.gov.ua/UJRN/Nvmgu_2017_25_1_13)

4. Cybersecurity of critical infrastructure: problems and ways to solve them / V. M. Borisenko, O. O. Lishchuk, I. V. Kolin'ko et al. // Information Security Problems. - 2019. - Vol. 22, No. 1. - P. 43-49. (https://doi.org/10.20535/2307-7502.2019.22.1.178439)

5. Cybersecurity of critical infrastructure: technologies and protection methods / N. V. Kolodyazhna, S. V. Parkhomenko, I. V. Rohovenko et al. // Electronic Scientific Professional Publication "Information Technologies and Computer Engineering". - 2020. - Issue 1(47). - P. 37-48. (http://ite.khpi.edu.ua/article/view/195054/193638)

6. Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.011

7. Cisco Systems, Inc. (2017). VPNs and VPN Technologies. https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/index.html

8. Microsoft Corporation. (2022). Virtual Private Network (VPN). https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/about-vpn-devices-for-always-on-vpn

9. Zhang, J., Huang, D., & Zhang, Y. (2019). A novel hybrid intrusion detection system for network security in the IoT environment. Journal of Network and Computer Applications, 136, 108-119. https://doi.org/10.1016/j.jnca.2019.03.020

10. Symantec Corporation. (2022). Endpoint Protection. https://www.symantec.com/products/endpoint-protection

11. McAfee, LLC. (2022). Antivirus Software. https://www.mcafee.com/enterprise/en-gb/products/antivirus-software.html