УДК 621.396 DOI: 10.31673/2412-4338.2023.010416

Бондарчук А.П., Жебка В.В.
Державний університет телекомунікацій, м. Київ

ЗАХИСТ ГЕТЕРОГЕННОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ВІД ВПЛИВУ ДЕСТАБІЛІЗУЮЧИХ ФАКТОРІВ

Анотація: *Проаналізовано небезпеки природно-антропогенного характеру та їх вплив на гетерогенну телекомунікаційну мережу. Проаналізовано існуючі на сьогодні заходи захисту телекомунікаційної мережі. Розглянута гетерогенна мережа, яка складається з ділянок ліній зв'язку з передаванням сигналів різної фізичної природи по різних середовищах передавання. Лінії зв'язку по різному реагують на загрози, що дозволяє для передавання інформації вибирати лінію з кращими показниками. Представлено приклади посилених запобіжних заходів для захисту підземних лінійно-кабельних споруд Представлена причинно-наслідкова діаграма подій, які обумовлюють стан мережі передавання інформації – зміни аварійних/безаварійних інтервалів часу. Показана схема застосування заходів захисту від небезпечних подій. Для верифікації заходів розроблена матриця їх відповідності типовим природним стихійним лихам і наведені відповідні приклади. Пропонується оцінювати гнучкість телекомунікаційної мережі її зв'язністю, яка характеризується числами вершинної і реберної зв'язності, імовірності зв'язності. Побудовано алгоритм розрахунку зв'язності шляху. Представлена схема пристрою для здійснення багатоканального передавання інформації в гібридній мережі, який дозволяє вибір для передавання інформації каналу з кращими показниками. Запропоновано загальна схема роботи інтелектуального блоку. Висунута пропозиція щодо підвищення гнучкості мережі, що полягає у використанні цього пристрою. В статті пропонується оцінювати гнучкість телекомунікаційної мережі її зв'язністю. Запропоновано при управлінні гетерогенною телекомунікаційною мережею використовувати машинне навчання, яке дозволить спрогнозувати дестабілізуючий фактор, його можливий вплив та видати алгоритм попередження впливу або вирішення наслідків впливу.*

Ключові слова: *гетерогенна мережа; зв'язність мережі; матриця відповідності; гнучкість мережі; дестабілізуючі фактори.*

Bondarchuk A.P., Zhebka V.V.
State University of Telecommunications, Kyiv

PROTECTION OF A HETEROGENEOUS TELECOMMUNICATION NETWORK FROM THE INFLUENCE OF DESTABILIZING FACTORS

Abstract: Natural and anthropogenic hazards and their impact on a heterogeneous telecommunication network are analyzed. The currently existing telecommunication network protection measures have been analyzed. A heterogeneous network is considered, which consists of sections of communication lines with the transmission of signals of different physical nature over different transmission media. Communication lines react differently to threats, which allows you to choose the line with the best indicators for transmitting information. Examples of enhanced

precautionary measures for the protection of underground line-cable structures are presented. A cause-and-effect diagram of events that determine the state of the information transmission network - changes in emergency/non-emergency time intervals - is presented. The scheme of application of protection measures against dangerous events is shown. To verify measures, a matrix of their compliance with typical natural disasters was developed and relevant examples were given. It is proposed to evaluate the flexibility of the telecommunications network by its connectivity, which is characterized by the numbers of vertex and edge connectivity, connectivity probability. An algorithm for calculating path connectivity has been built. The scheme of the device for carrying out multi-channel transmission of information in a hybrid network is presented, which allows the selection of the channel with the best indicators for the transmission of information. The general scheme of the operation of the intelligent block is proposed. A proposal has been put forward to increase the flexibility of the network, which consists in the use of this device. The article proposes to evaluate the flexibility of the telecommunications network by its connectivity. It is proposed to use machine learning in the management of a heterogeneous telecommunication network, which will allow predicting a destabilizing factor, its possible impact, and issue an algorithm for preventing the impact or solving the consequences of the impact.

***Keywords**: heterogeneous network; network connectivity; correspondence matrix; network flexibility; destabilizing factors.*

1. Вступ

Останнім часом у світі зростає кількість катастроф природного характеру, які обумовлені глобальною зміною клімату на Землі (наприклад, [1–5]).

Навколишнє середовище змінюється людиною свідомо та головним чином несвідомо. Характерною рисою сучасності є масове будівництво потенційно небезпечних підприємств, які становлять реальну загрозу виникнення надзвичайних ситуацій. Це обумовлює безпрецедентне зростання кількості карастроф неприродного характеру [1,3,5–7].

Такі екстремальні явища періодично відбуваються в кожному з регіонів світу. Економічний збиток від них вимірюється величезними сумами [3,8].

В інформаційному суспільстві важливою діяльністю є використання, створення, поширення, маніпулювання та впровадження інформації. Основними рушійними силами суспільства стають інформаційно-комунікаційні технології, які призвели до швидкого зростання різноманітності інформації та так чи інакше змінюють усі сторони соціальної організації. Зростання кількості катастроф потребує вироблення рекомендацій щодо захисту від них однієї з основних галузей сучасного виробництва – телекомунікацій [4,7,9,10].

В умовах мінливості сучасного природно-антропогенного середовища важливим критерієм оцінки якості мережі передавання інформації стає її здатність оперативно адаптуватися до подій, які можуть нести і несуть загрозу працездатності. Ця здатність визначається як гнучкість і полягає в можливості швидко, з мінімальними зусиллями, пристосовуватися до нової обстановки [1,5,7,11–14].

Критерію гнучкості відповідає гетерогенна мережа. Вона складається з ділянок ліній зв’язку з передаванням сигналів різної фізичної природи (електричний, оптичний) по різних середовищах передавання (вільний простір, штучні напрямні). Лінії зв’язку по різному реагують на загрози, що дозволяє для передавання інформації вибирати лінію з кращими показниками [15,16].

Причиною підвищення мотивації цієї роботи є наявні теоретичні розробки щодо гібридної мережі [12,16–18].

2. Аналіз досліджень і публікацій.

Невпинне дослідження причин аварій мережі передавання інформації обумовлюється взаємодією мінливих процесів. Це, по-перше, природні зміни середовища, по-друге, антропогені зміни технологій передавання. Результати досліджень представлені у роботах багатьох дослідників: for example, Claude de Ville de Goyet, Ricardo Zapata Marti, and Claudio Osorio (2006); M. M. Bonch-Bruevich (2012); Tolubko, V., Vyshnivskyi, V., Mukhin, V., Haidur, H., Dovzhenko, N., Ilin, O., Vasylenko, V. (2018); F. Rahman (2019); A. Gyasi-agyei (2019); V. V. Zhebka and P. V. Anakhov (2021).

З метою встановлення єдиних технічних вимог у сфері експлуатації мережі, узагальнення наявних досліджень і досвіду експлуатації, створюються стандарти і рекомендації, in particular State standard of Ukraine 2860 (1994); IEC 62508 (2010); State Classifier of Ukraine 019 (2010); State standard of Ukraine 3899 (2013).

Відповідно до причин небезпек розробляються заходи. До таких можна віднести захист кабелів зв'язку від дії шкідників згідно Recommendation ITU-T L.46 (2000); запобіжні заходи для захисту підземних лінійно-кабельних споруд згідно Recommendation ITU-T L.92 (2012).

P. Anakhov, A. Makarenko, V. Zhebka, V. Vasylenko and M. Stepanov (2020) розробили універсальну схему застосування заходів захисту від небезпек.

На основі вказаної схеми V. V. Zhebka (2021) розробила гнучкий пристрій для здійснення багатоканального передавання інформації в гібридній мережі, який дозволяє вибір для передавання інформації каналу з кращими показниками[9].

3. Мета дослідження. Метою статті є розробка захищеної від небезпек природно-антропогенного характеру гнучкої мережі передавання інформації.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- систематизувати причини аварій;
- розробити схему застосування заходів захисту;
- верифікувати заходи захисту;
- розробити рекомендації по захисту мережі.

4. Аналіз заходів щодо захисту телекомунікаційної мережі від дії дестабілізуючих чинників

З літератури відомі конкретні заходи щодо захисту апаратних засобів телекомунікаційної мережі від дії визначених природних загроз. Узагальнені заходи, що розкриваються далі, зводяться до рекомендацій із захисту лінійно-кабельних споруд і організаційних заходів.

Для захисту лінійно-кабельних споруд від атмосферних і гідрологічних загроз пропонується їх прокладання під землею. На рис. 1 представлено приклади посилених запобіжних заходів для захисту підземних лінійно-кабельних споруд.

Для захисту апаратних засобів від природних загроз пропонуються наступні організаційні заходи:

– для захисту від геофізичних (код 20100) і геологічних явищ – підтримувати готовність систем спостереження, прогнозування, оповіщення; вирішувати питання доцільності будівництва в небезпечних районах; підтримувати готовність сил і засобів до ліквідації наслідків дії;

– для захисту від метеорологічних явищ (код 20300) – виявляти провісники, детектувати лиха; оповіщувати населення; встановлювати суворий порядок будівельних норм в районах підвищеного ризику; розроблювати плани з надзвичайних ситуацій в районах підвищеного ризику;

– для захисту від гідрологічних морських явищ (код 20400) – проводити та уточнювати оцінки ризиків та ідентифікації загроз; організовувати централізовану систему спостережень

і контролю; виявляти і уточнювати зони з найбільш небезпечними і частими аномаліями і визначати ризики виникнення НС в них; посилювати заходи із захисту територій в небезпечних зонах; створювати резерв засобів і устаткування для відновлення;

– у міру можливості усувати або зводити до мінімуму прив'язку інфраструктури зв'язку до інфраструктури електромережі, забезпечуючи резервну потужність за рахунок дизель-генераторів, автономних вітрових і сонячних електростанцій.

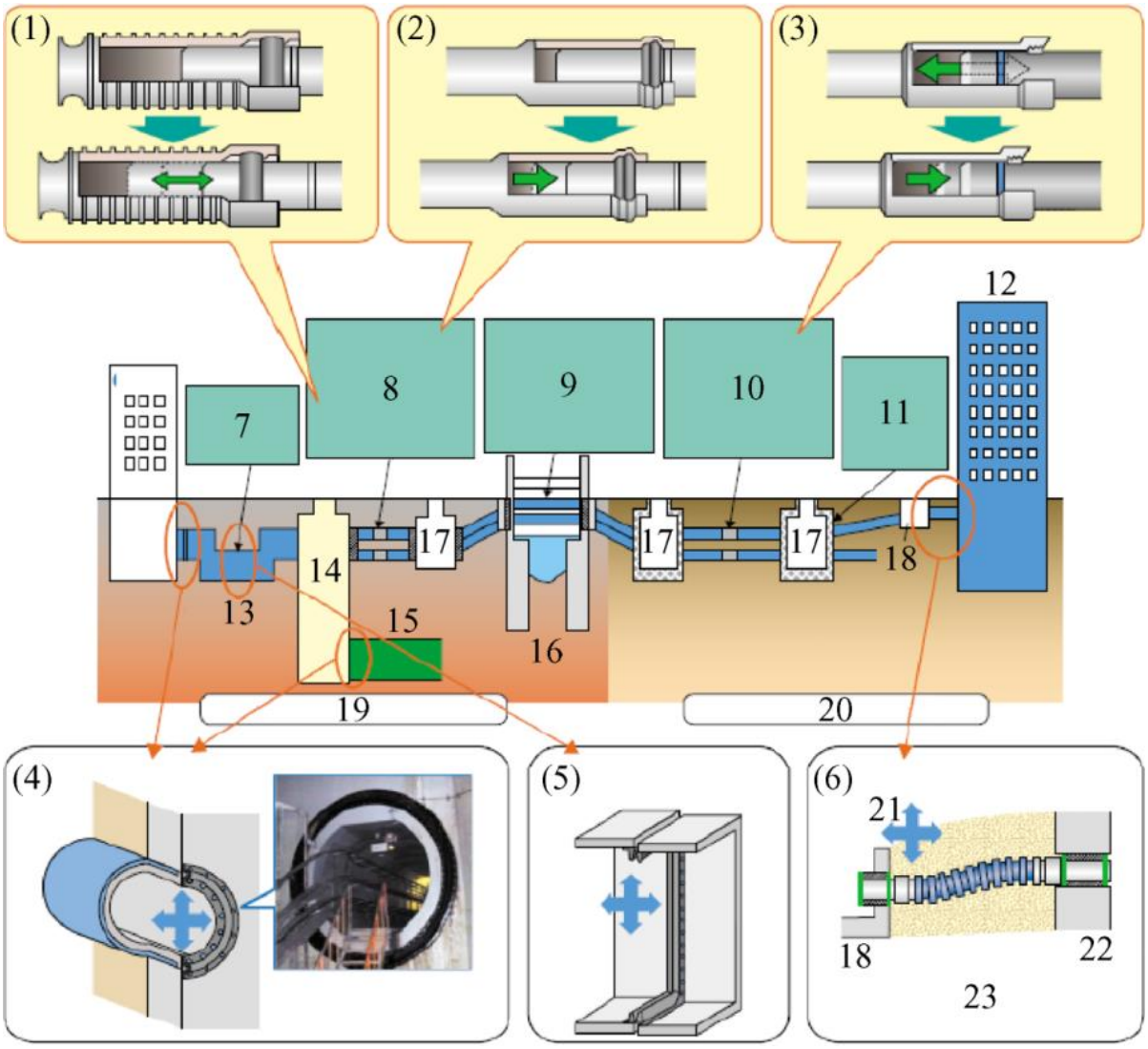

Рис. 1. Приклади запобіжних заходів для захисту підземних лінійно-кабельних споруд з досвіду спеціалістів з телекомунікацій Японії: (1) – ковзне з’єднання для оглядових колодязів (з’єднувальна муфта газопроводу); (2) – ковзне з’єднання для газопроводів; (3) – ковзне з’єднання із стопором; (4) – гнучке з'єднання для проходки стінки кабельної шахти; (5); – гнучке з'єднання кабельних каналів; (6) – гнучке з'єднання ділянок газопроводу для проходки в будівлю; 7 – гнучке з'єднання; 8 – ковзне з’єднання + з’єднувальна муфта; 9 – ковзне з’єднання із стопором + бетонний кабельний лоток; 10 – ковзне з’єднання із стопором + з’єднувальна муфта; 11 – залізобетонна кришка люку; 12 – будівля користувача послуг; 13 – кабельний канал; 14 – кабельна шахта; 15 – кабельна каналізація; 16 – проходка мостового переходу; 17 – оглядовий колодязь (ОК); 18 – ревізійний колодязь (РК); 19 – нормальний ґрунт; 20 – водонасичений ґрунт; 21 – напрямки зміщень; 22 – стіна будівлі; 23 – гнучкий гофрований газопровід

Відповідно до існуючого досвіду, апаратні ресурси телекомунікаційної мережі мають відповідати принципу надмірності, за якого виконується оперативна реконфігурація. Пропонується застосовувати резервування ліній зв'язку за рахунок альтернативних технологій, наприклад, технології оптичної передачі у вільному просторі, високочастотний зв'язок по лініям електропередач. Все це в першу чергу стосується спільної для користувачів телекомунікаційних послуг транспортної мережі.

Запобіжні заходи щодо зменшення збитків від наслідків стихійних лих для ТКМ, які пропонуються згідно Рекомендацій ITU-T L.92, розділено на групи. Окремо виділено групи заходів (Г) щодо запобігання дії стихійних явищ: запобіжні заходи (З), заходи протидії (П), моніторинг (М) [95].

Рекомендації МСЕ [95, 93] обмежуються переліком найбільш руйнівних на сьогоднішній день небезпек і способами захисту від їх дії. Проте в них не розглядаються інші, потенційно можливі для телекомунікацій, небезпеки.

Розширений перелік стихійних лих в кількості 38 позицій, які можуть виникнути на території України в різних галузях національного господарства країни, наведено у Національному класифікаторі ДК 019:2010 "Класифікатор надзвичайних ситуацій" (від 11.10.2010, №457) [171].

Проте, в ДК 019:2010 відсутні "показові" небезпеки періоду глобального потепління: підвищення температури [80, 93], підвищення рівня моря [80, 93], зміна режимів опадів [80]. Крім того, в документі не розглядаються способи захисту телекомунікаційної мережі.

Виконаний аналіз літератури показав доцільність проведення дослідження, присвяченого розгляду наростаючих в результаті глобального потепління загроз телекомунікаційній мережі, аналізу їх дії на апаратні ресурси мережі і опрацюванні заходів протидії.

5. Розробка методів формування заходів захисту гетерогенної телекомунікаційної мережі від впливу дестабілізуючих факторів

Переважна більшість подій, що можуть привести до аварії в умовах дії внутрішніх та зовнішніх дестабілізуючих впливів прогнозована, тому при управлінні гетерогенною телекомунікаційною мережею доречно використовувати машинне навчання, яке дозволить спрогнозувати дестабілізуючий фактор, його можливий вплив та видати алгоритм попередження впливу або вирішення наслідків впливу.

Потрібно визнати, що стихійні лиха у багатьох випадках є невідворотними. Отже, практичним завданням стає мінімізація їх негативних наслідків. Зменшення небезпеки може передбачати: короткострокове прогнозування і оповіщення про небезпеку; довгострокове прогнозування і встановлення суворого порядку будівельних норм в районах підвищеного ризику.

При розробці проєкту захисту в якості базового критерію повинна бути покладена концепція розумної достатності. Її сенс полягає в тому, щоб при мінімальному використанні коштів та заходів захисту забезпечити вимоги з електромагнітної сумісності, функціональної та інформаційної безпеки електронних систем мережі в умовах передбачуваного впливу [45,46, 139].

Схема застосування заходів для захисту від небезпечних подій природно-антропогенного характеру показана на рисунку 2.

Рис. 2. Схема застосування заходів захисту від небезпек

Пропонована схема призначена для вироблення плану дій по запобіганню небезпекам природного і антропогенного характерів. Короткотермінове прогнозування небезпек виконується для оповіщення населення і збору даних. Дані використовуються у довготерміновому прогнозуванні. Воно застосовується при оцінці ризиків та їх прийнятних рівнів для декларування безпеки об'єктів, прийняття рішень щодо їх розташування та експлуатації, розробки заходів по запобіганню аваріям та підготовці до реагування на них. До переліку заходів захисту належать:

- застосування стійких до визначеної небезпеки матеріалів і конструкцій;
- перехоплення небезпеки, яке передбачає екранування об’єкту чи його найбільш уразливих і відповідальних елементів, від небезпеки, або екранування небезпеки від об’єкту, а також протидію небезпеці;
- застосування елементів гнучкості мережі передавання інформації, які полягають у реконфігурації систем забезпечення працездатності (електроживлення, вентиляція і кондиціонування, пожежна сигналізація, пожежогасіння, оповіщення тощо);
- реконфігурації мережі передавання.

На рис. 3 представлено схему гнучкого пристрою для здійснення багатоканального передавання інформації в гібридній мережі, який дозволяє вибір для передавання інформації каналу з кращими показниками.

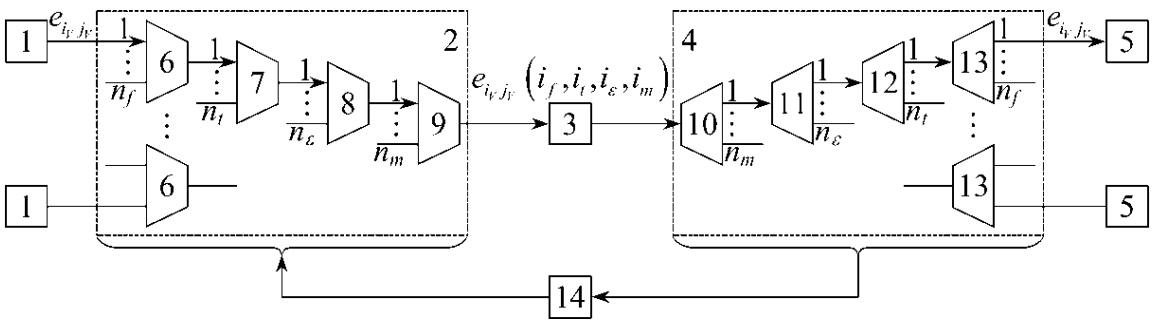

Рис. 3. Структурна схема пристрою для здійснення багатоканального передавання інформації на ділянці мережі передавання інформації, в симплексному режимі [12]

Позначення на рис. 3: e_{ij} – лінії (канали) зв'язку між станціями і вузлами мережі; i_f, $i_f = \overline{1, n_f}$, i_t, $i_t = \overline{1, n_t}$, i_ε, $i_\varepsilon = \overline{1, n_\varepsilon}$, i_m, $i_m = \overline{1, n_m}$ – ідентифікатори каналів систем мультиплексування з частотним f, з часовим t розділеннями каналів, з розділеннями каналів за фізичною природою сигналів ε, з розділенням каналів за середовищами передавання m, відповідно; n_f, n_t, n_ε, n_m – кількість каналів n систем мультиплексування з частотним f, часовим t розділеннями каналів, з розділенням каналів за фізичною природою сигналів ε, і за середовищами передавання m, відповідно.

Пристрій для здійснення багатоканального передавання інформації на ділянці мережі містить джерело інформації 1, комутатор передавача 2, лінію зв'язку 3, ресурси якої складають множини середовищ передавання, сигналів різної фізичної природи, смуг частот і інтервалів часу сигналів, комутатор приймача 4, сервер користувача 5, селектор слідкування за станом каналів і вибору каналів передавання 14. Комутатор передавача 2 містить гнучкі мультиплексори 6, які забезпечують передавання інформації з розділянням каналів кількістю n_f одиниць ($n_f \geq 1$) за частотою, гнучкі мультиплексори 7, які забезпечують передавання інформації з розділянням каналів кількістю n_t одиниць ($n_t \geq 1$) за часом, гнучкі мультиплексори 8, які забезпечують передавання інформації з розділянням каналів кількістю n_ε одиниць ($n_\varepsilon \geq 1$) за фізичною природою сигналу, гнучкі мультиплексори 9, які забезпечують передавання інформації з розділянням каналів кількістю n_m одиниць ($n_m \geq 1$) за середовищами. Комутатор приймача 4 містить гнучкі демультиплексори 10, 11, 12, 13, які забезпечують приймання інформації з розділянням каналів за середовищами, за фізичною природою сигналу, за часом і за частотою, відповідно.

Пристрій для багатоканального передавання інформації реалізується наступним чином. Інформаційний сигнал по каналу (лінії звязку) e_{ij} від джерела інформації 1 поступає на комутатор передавача 2. В комутаторі 2 шляхом послідовних перетворень в мультиплексорах 6–9 інформаційному сигналу привласнюється унікальний ресурс для незалежного передавання по лінії зв'язку 3: в гнучких мультиплексорах 6, 7, 8, 9 сигналу привласнюється частотний ресурс i_f, часовий ресурс i_t, ресурс, який належить до множини сигналів різної фізичної природи i_ε, середовищний ресурс i_m, відповідно. Переданий від комутатора передавача 2 інформаційний сигнал, використовуючи гібридну лінію зв'язку 3, по каналу $e_{ij}(i_f, i_t, i_\varepsilon, i_m)$, приймається комутатором приймача 4. В комутаторі 4 шляхом послідовних зворотних перетворень в демультиплексорах 10–13 інформаційний сигнал перетворюється в формат $e_{i'j'}$, прийнятний для передавання на комутатор приймача 5. Селектор слідкування за станом каналів і вибору каналів передавання 14 відслідковує стан ресурсів у комутаторі приймача 4, які при передаванні по лінії зв'язку 3 піддаються дії дестабілізуючих чинників, і формує команди на виключення ресурсів мережі передавання інформації в комутаторі передавача 2, які не відповідають прийнятим вимогам щодо якості передавання сигналу і включення ресурсів мережі в комутаторі передавача 2, які відповідають прийнятим вимогам щодо якості передавання сигналу.

6. Рекомендації по забезпеченню функціональної стійкості гетерогенної телекомунікаційної мережі

Основними питаннями аналізу систем зі змінною структурою є розробка моделей і методів розрахунку характеристик їх функціональної стійкості, а також управління процесом модифікацій з метою отримання найбільшої функціональної стійкості систем відповідно до обраних критеріїв.

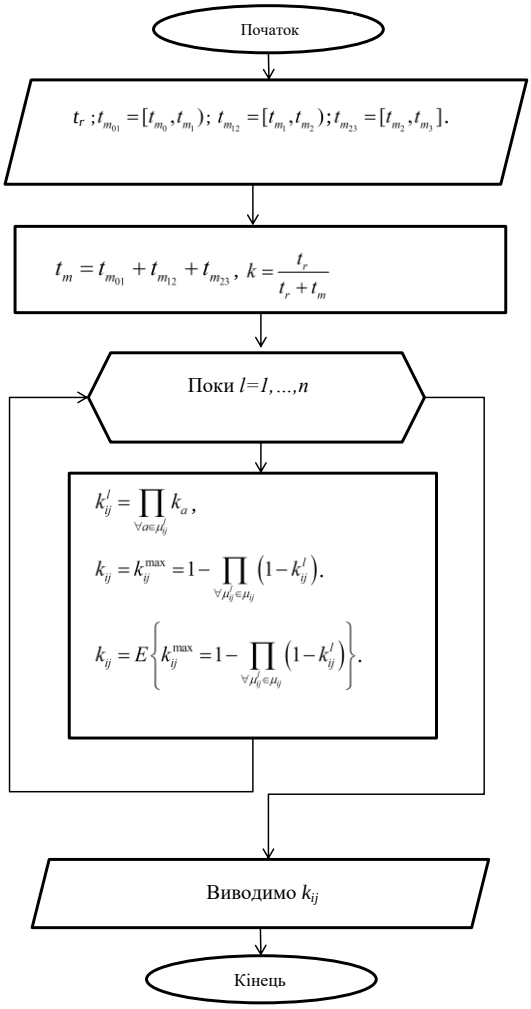

Рис. 4. Алгоритм розрахунку зв’язності шляху

Забезпечення деяких нормованих значень готовності, безвідмовності, ремонтопридатності та технічного обслуговування – це заходи, що характеризують сталість телекомунікаційної мережі та засобів телекомунікацій заходи. Перелік таких заходів, включений до рекомендації МСЕ Е.862 "Планування надійності телекомунікаційних мереж" та включає:

1) забезпечення готовності (availability performance);

2) забезпечення безвідмовності (reliability performance);

3) забезпечення ремонтів (maintainability performance), які характеризуються визначеними інтервалами часу t_m.

Для забезпечення функціональної стійкості мережі було розроблено методику для автоматизованого розрахунку зв’язності телекомунікаційної мережі (рис. 4).

Загальний алгоритм самонавчання інтелектуального блоку гетерогенної телекомунікаційної мережі представлено на рис.5.

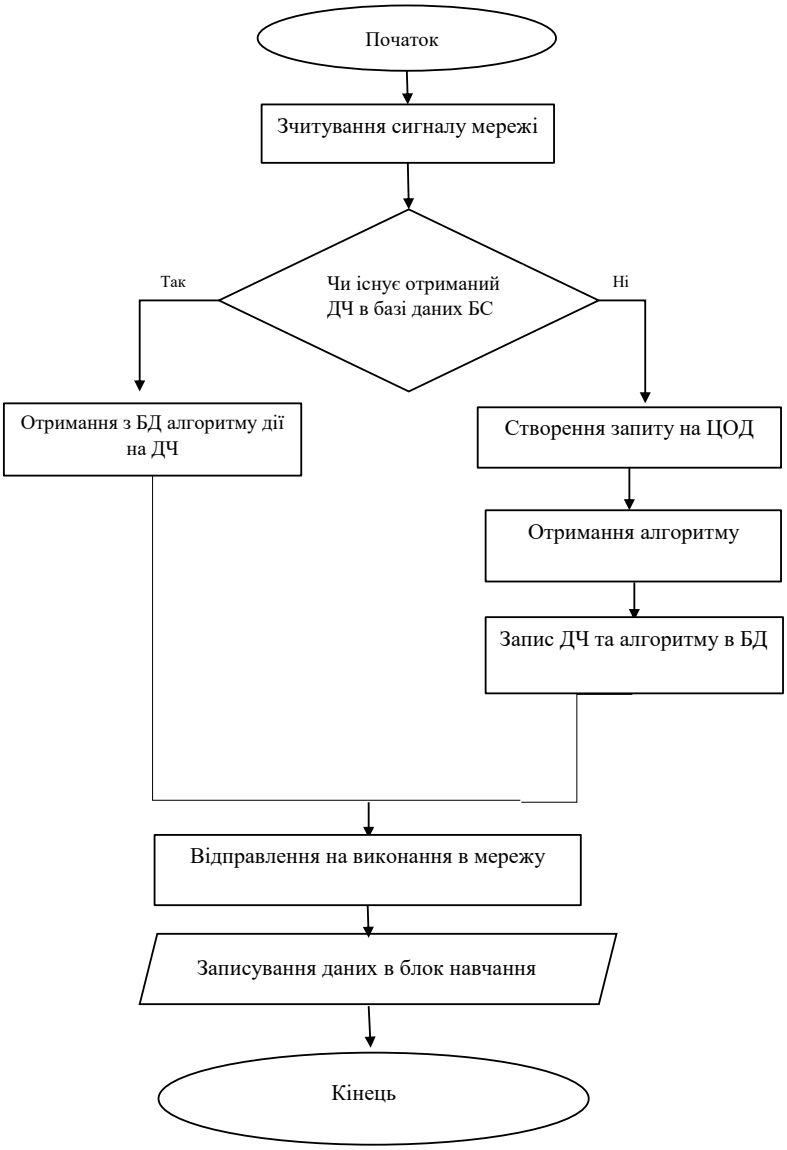

Рис. 5. Загальна схема роботи інтелектуального блоку

6. Висновки

Розглянута гетерогенна мережа, яка складається з ділянок ліній зв'язку з передаванням сигналів різної фізичної природи по різних середовищах передавання. Лінії зв'язку по різному реагують на загрози, що дозволяє для передавання інформації вибирати лінію з кращими показниками.

Систематизовані причини аварій мережі передавання інформації. Представлена причинно-наслідкова діаграма подій, які обумовлюють стан мережі – зміни аварійних/безаварійних інтервалів часу. Надані пояснення щодо цих подій.

Представлена схема застосування заходів захисту від небезпечних подій. Для верифікації заходів захисту розроблена матриця відповідності заходів типовим природним стихійним лихам. Наведені відповідні приклади.

Представлено схему пристрою для здійснення багатоканального передавання інформації в гібридній мережі, який дозволяє вибір для передавання інформації каналу з кращими показниками. Висунута пропозиція щодо підвищення гнучкості мережі, що полягає у використанні цього пристрою.

Пропонується оцінювати гнучкість телекомунікаційної мережі її зв'язністю.

Список використаної літератури:

1. George Halkos, Shunsuke Managi and Nickolaos G. Tzeremes. The effect of natural and man-made disasters on countries' production efficiency. Journal of Economic Structures. 2015. Vol. 4:10.
2. ITU-D Study Group 2. Question 6/2: ICT and climate change. Final Report. Geneva: ITU, 2017. 64 p.
3. P. Babarczi, M. Klügel, A. M. Alba, A. He, J. Zerwas, P. Kalmbach, A. Blenk and W. Kellerer. A mathematical framework for measuring network flexibility. Computer Communications. 2020. Vol. 164, pp. 13–24.
4. F. Rahman. Save the world versus man-made disaster: A cultural perspective. IOP Conference Series: Earth and Environmental Science. 2019. Vol. 235, 012071.
5. Mohamed H. A. R. A Proposed Model for IT Disaster Recovery Plan. Ijmecs. 2014. Vol. 6, No. 4, pp. 57–67. DOI: 10.5815/ijmecs.2014.04.08
6. Weather and Climate Services in Europe and Central Asia. A Regional Review / World Bank Working Paper No. 151. Washington, D.C., 2008. 79 p.
7. Angelica Valeria Ospina, David Faulkner, Keith Dickerson and Cristina Bueti. Resilient pathways: the adaptation of the ICT sector to climate change. Geneva: ITU, 2014. 62 p.
8. Zayan EL Khaled and Hamid Mcheick. Case studies of communications systems during harsh environments: A review of approaches, weaknesses, and limitations to improve quality of service. International Journal of Distributed Sensor Networks. 2019. Vol. 15, Iss. 2.
9. В. В. Жебка. Пат. 147713 України, МПК H04J 99/00. Пристрій для багатоканального передавання інформації. №u202005203; заявл. 14.08.2020; опубл. 10.06.2021; Бюл. №23.
10. Fathi A., Kia K. A Centralized Controller as an Approach in Designing NoC. IJMECS. 2017. Vol. 9, No. 1, pp. 60–67. DOI: 10.5815/ijmecs.2017.01.07
11. Boukhedouma S., Oussalah M., Alimazighi Z., Tamzalit D. Service Based Cooperation Patterns to Support Flexible Inter-Organizational Workflows. IJITCS. 2014. Vol. 6, No. 4, pp. 1–18. DOI: 10.5815/ijitcs.2014.04.01
12. Recommendation ITU-R P.1817-1 (02/2012). Propagation data required for the design of terrestrial free-space optical links.
13. P. Anakhov, V. Zhebka, G. Grynkevych and A. Makarenko. Protection of telecommunication network from natural hazards of global warming. Eastern-Europian Journal of Enterprise Technologies. 2020. No. 3/10, pp. 26–37.
14. В. В. Жебка, П. В. Анахов Моніторинг сталості інформаційно-телекомунікаційної системи і опрацювання заходів її захисту від небезпек. Метрологія та прилади. – 2021. – №1(87). – С. 23-29. DOI: 10.33955/2307-2180(1)2021.23-29
15. P. Anakhov, A. Makarenko, V. Zhebka, V. Vasylenko and M. Stepanov. Systematization of Measures on Lightning Protection of the Objects of Telecommunications Network. International Journal of Advanced Trends in Computer Science and Engineering. 2020. Vol. 9, pp. 7870–7877.
16. Gyasi-agyei A. Telecommunications Engineering: Principles And Practice. Singapore: World Scientific Publishing Company, 2019. 760 p.
17. ДК 019:2010. Державний класифікатор України. Класифікатор надзвичайних ситуацій (від 11.10.2010, №457).
18. Claude de Ville de Goyet, Ricardo Zapata Marti, and Claudio Osorio. Natural Disaster Mitigation and Relief. In: Dean T Jamison, Joel G Breman, Anthony R Measham, George

Alleyne, Mariam Claeson, David B Evans, Prabhat Jha, Anne Mills, and Philip Musgrove (Eds.), Disease Control Priorities in Developing Countries. 2nd edition. Washington (DC): The International Bank for Reconstruction and Development / The World Bank. New York: Oxford University Press, 2006. P. 1147–1162.

19. Recommendation ITU-T L.92 (10/2012). Series L: construction, installation and protection of cables and other elements of outside plant. Disaster management for outside plant facilities.

20. М. І.Стеблюк. Цивільна оборона та цивільний захист. К.: Знання-Прес, 2007. 487 с.

21. ITU-T Recommendation M.34 (11/88). Performance monitoring on international transmission systems and equipment.

22. Olaiya F., Adeyemo A. B. Application of Data Mining Techniques in Weather Prediction and Climate Change Studies. IJIEEB. 2012. Vol. 4, No. 1, pp. 51–59. DOI: 10.5815/ijieeb.2012.01.07

23. М. М. Козак. Лінійні споруди зв'язку. Під ред. С. Б. Доброчинського, Г. М. Петрунчака. Вінниця: 2009. 317 с.

24. Майданюк В. П. Кодування та захист інформації. Вінниця: ВНТУ, 2009. 164 с.

25. Alagoz B. B., Alagoz S. Towards Earthquake Shields: A Numerical Investigation of Earthquake Shielding with Seismic Crystals. Open Journal of Acoustics. 2011. Vol. 1, No. 3, pp. 63–69. doi:10.4236/oja.2011.13008

26. ДБН В.1.1-25-2009. Захист від небезпечних геологічних процесів, шкідливих експлуатаційних впливів, від пожежі. Інженерний захист територій та споруд від підтоплення та затоплення.

27. Аналіз сучасного зарубіжного та вітчизняного досвіду влаштування систем блискавкозахисту об'єктів електричних мереж. К.: НПЦР ОЕС України, 2018. 74 с.

28. П. В. Анахов. Пат. 118515 України, МПК E02B 3/04. Застосування способу придушення довгих морських хвиль у портовому підхідному каналі для придушення висоти хвиль, які виникають при обваленні у водойму зсувного масиву. №u201702195; заявл. 09.03.2017; опубл. 10.08.2017; Бюл. №15.

29. ITU-D Study Group 2. Question 6/2: ICT and climate change. Final Report. Geneva, 2017. 64 p.

30. Ahmet Yazar, Seda Doğan Tusha and Huseyin Arslan. 6G vision: an ultra-flexible perspective. ITU Journal on Future and Evolving Technologies. 2020. Vol. 1, Iss.1.

31. ITU-T Recommendation G.602. Transmission media characteristics. Reliability and availability of analogue cable transmission systems and associated equipments.

References:

1. George Halkos, Shunsuke Managi and Nickolaos G. Tzeremes. The effect of natural and man-made disasters on countries' production efficiency. Journal of Economic Structures. 2015. Vol. 4:10.

2. ITU-D Study Group 2. Question 6/2: ICT and climate change. Final Report. Geneva: ITU, 2017. 64 p.

3. P. Babarczi, M. Klügel, A. M. Alba, A. He, J. Zerwas, P. Kalmbach, A. Blenk and W. Kellerer. A mathematical framework for measuring network flexibility. Computer Communications. 2020. Vol. 164, pp. 13–24.

4. F. Rahman. Save the world versus man-made disaster: A cultural perspective. IOP Conference Series: Earth and Environmental Science. 2019. Vol. 235, 012071.

5. Mohamed H. A. R. A Proposed Model for IT Disaster Recovery Plan. Ijmecs. 2014. Vol. 6, No. 4, pp. 57–67. DOI: 10.5815/ijmecs.2014.04.08

6. Weather and Climate Services in Europe and Central Asia. A Regional Review / World Bank Working Paper No. 151. Washington, D.C., 2008. 79 p.

7. Angelica Valeria Ospina, David Faulkner, Keith Dickerson and Cristina Bueti. Resilient pathways: the adaptation of the ICT sector to climate change. Geneva: ITU, 2014. 62 p.

8. Zayan EL Khaled and Hamid Mcheick. Case studies of communications systems during harsh environments: A review of approaches, weaknesses, and limitations to improve quality of service. International Journal of Distributed Sensor Networks. 2019. Vol. 15, Iss. 2.

9. VV Zhebka. Stalemate. 147713 of Ukraine, IPC H04J 99/00. A device for multichannel information transmission. No. u202005203; statement 14.08.2020; published 10.06.2021; Bul. No. 23.

10. Fathi A., Kia K. A Centralized Controller as an Approach in Designing NoC. IJMECS. 2017. Vol. 9, No. 1, pp. 60–67. DOI: 10.5815/ijmecs.2017.01.07

11. Boukhedouma S., Oussalah M., Alimazighi Z., Tamzalit D. Service Based Cooperation Patterns to Support Flexible Inter-Organizational Workflows. IJITCS. 2014. Vol. 6, No. 4, pp. 1–18. DOI: 10.5815/ijitcs.2014.04.01

12. Recommendation ITU-R P.1817-1 (02/2012). Propagation data required for the design of terrestrial free-space optical links.

13. P. Anakhov, V. Zhebka, G. Grynkevych and A. Makarenko. Protection of telecommunication networks from natural hazards of global warming. Eastern-European Journal of Enterprise Technologies. 2020. No. 3/10, pp. 26–37.

14. V. V. Zhebka, P. V. Anakhov Monitoring the stability of the information and telecommunications system and developing measures to protect it from dangers. Metrology and devices. – 2021. – No. 1(87). - P. 23-29. DOI: 10.33955/2307-2180(1)2021.23-29

15. P. Anakhov, A. Makarenko, V. Zhebka, V. Vasylenko and M. Stepanov. Systematization of Measures on Lightning Protection of the Objects of Telecommunications Network. International Journal of Advanced Trends in Computer Science and Engineering. 2020. Vol. 9, pp. 7870–7877.

16. Gyasi-agyei A. Telecommunications Engineering: Principles And Practice. Singapore: World Scientific Publishing Company, 2019. 760 p.

17. DK 019:2010. State Classifier of Ukraine. Classifier of emergency situations (as of October 11, 2010, No. 457).

18. Claude de Ville de Goyet, Ricardo Zapata Marti, and Claudio Osorio. Natural Disaster Mitigation and Relief. In: Dean T Jamison, Joel G Breman, Anthony R Measham, George Alleyne, Mariam Claeson, David B Evans, Prabhat Jha, Anne Mills, and Philip Musgrove (Eds.), Disease Control Priorities in Developing Countries. 2nd edition. Washington (DC): The International Bank for Reconstruction and Development / The World Bank. New York: Oxford University Press, 2006. P. 1147–1162.

19. Recommendation ITU-T L.92 (10/2012). Series L: construction, installation and protection of cables and other elements of outside plant. Disaster management for outside plant facilities.

20. M. I. Stebluk. Civil defense and civil protection. K.: Znannia-Press, 2007. 487 p.

21. ITU-T Recommendation M.34 (11/88). Performance monitoring on international transmission systems and equipment.

22. Olaiya F., Adeyemo A. B. Application of Data Mining Techniques in Weather Prediction and Climate Change Studies. IJIEEB. 2012. Vol. 4, No. 1, pp. 51–59. DOI: 10.5815/ijieeb.2012.01.07

23. M. M. Kozak. Linear communication facilities. Under the editorship S. B. Dobrochynskyi, H. M. Petrunchak. Vinnytsia: 2009. 317 p.

24. Maidanyuk V. P. Coding and protection of information. Vinnytsia: VNTU, 2009. 164 p.

25. Alagoz B.B., Alagoz S. Towards Earthquake Shields: A Numerical Investigation of Earthquake Shielding with Seismic Crystals. Open Journal of Acoustics. 2011. Vol. 1, No. 3, pp. 63–69. doi:10.4236/oja.2011.13008

26. DBN V.1.1-25-2009. Protection from dangerous geological processes, harmful operational influences, from fire. Engineering protection of territories and structures against flooding and inundation.

27. Analysis of modern foreign and domestic experience in the installation of lightning protection systems for electrical network facilities. K.: NPCR of the OES of Ukraine, 2018. 74 p.

28. P. V. Anakhov. Stalemate. 118515 of Ukraine, IPC E02B 3/04. The application of the method of suppression of long sea waves in the port approach channel to suppress the height of waves that occur in and collapse of the landslide massif into the reservoir. No. u201702195; statement 03/09/2017; published 10.08.2017; Bul. No. 15.

29. ITU-D Study Group 2. Question 6/2: ICT and climate change. Final Report. Geneva, 2017. 64 p.

30. Ahmet Yazar, Seda Doğan Tusha and Huseyin Arslan. 6G vision: an ultra-flexible perspective. ITU Journal on Future and Evolving Technologies. 2020. Vol. 1, Issue 1.

31. ITU-T Recommendation G.602. Transmission media characteristics. Reliability and availability of analogue cable transmission systems and associated equipment.