УДК 004.725.7 **doi: 10.26906/SUNZ.2021.1.090**

А. А. Коваленко[1], Г. А. Кучук[2], В. М. Ткачов[1]

[1] Харківський національний університет радіоелектроніки, Харків, Україна
[2] Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

МЕТОД ЗАБЕЗПЕЧЕННЯ ЖИВУЧОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ НА ОСНОВІ VPN-ТУНЕЛЮВАННЯ

Анотація. В статті проаналізовано основні підходи до забезпечення живучості комп'ютерних мереж. Показано, що методологія забезпечення живучості, яка застосовується до комп'ютерних систем має часткову відмінність за ту, що застосовується до комп'ютерних мереж, що пов'язано з активним розвитком технологій віртуалізації. **Метою** статті є розробка методу, який дозволяє забезпечити живучість комп'ютерної мережі, яка є інформаційним середовищем для гарантованого надання цифрових послуг, шляхом використання віртуальних тунелів, заснованих на принципах VPN-тунелювання для делегування «білих» IP-адрес в комп'ютерні мережі, або схеми маршрутизації потоків даних при використанні внутрішніх VPN-серверів з єдиною «білою» IP-адресою. Отримані **результати** дозволяють: сформулювати наукову задачу з формалізацією необхідних технічних вимог до розроблюваної комп'ютерної мережі; розробити прикладне рішення забезпечення живучості комп'ютерної мережі, засноване на використанні множинних VPN-тунелів; провести ряд експериментів з дослідження ефективності використання різних мережних протоколів в VPN-тунелях; створити підґрунтя для подальший розвитку методології забезпечення живучості комп'ютерних систем для забезпечення безперервності процесів управління мережними інфраструктурами. Дослідження дозволяють зробити **висновки**, що запропонований метод може бути використаний на етапах проектування комп'ютерних мереж в частині визначення показників надлишковості при реалізації принципів управління елементами мережі як то сервери, шлюзи, технологічне обладнання тощо.

Ключові слова: живучість, комп'ютерна мережа, віртуалізація, VPN.

Вступ

Постановка проблеми. Технологічний прогрес стоїть на порозі п'ятої промислової революції. Її особливістю є зміна характеру виробничої діяльності: якщо цифрова трансформація четвертої промислової революції робить продукцію клієнтоорієнтованою, то в епоху п'ятої – продукція стане масово персоналізованою [1]. Це означає, що ланцюг поставок товарів і послуг буде орієнтованим на персонального клієнта. Якість та гарантія надання цифрових послуг персонально кожному клієнту в таких умовах є запорукою сталого розвитку вендорів IT-сервісів з огляду показника стійкості середовища їх поставки [2].

Таким чином, актуальною задачею є розробка технологічних засад щодо забезпечення на задовільному рівні показника стійкості інформаційного середовища, в якому відбувається гарантоване надання цифрових послуг.

Одним із підходів до вирішення цієї задачі є використання технології віртуальних тунелів (приватних віртуальних мереж) в комп'ютерних мережах між клієнтами, сервісними майданчиками, хмарними інфраструктурами тощо. Стійкість комп'ютерної мережі проти факторів зовнішнього впливу, що призводять до втрати нею основних функцій, лежить в основі поняття живучості комп'ютерної мережі.

Аналіз останніх досліджень і публікацій. На сьогоднішній день існує велика кількість методів та технологій забезпечення живучості комп'ютерних мереж. Зокрема, відома наукова школа проф. Додонова О.Г., вченими якої створено апарат формалізації задач, пов'язаних з забезпеченням живучості інформаційних систем, запропоновано ряд стратегій та концепцію забезпечення живучості, розроблено ряд методів та цілих методологій [3]. В їх основі лежить ідея, що будь-який вузол будь-якої системи характеризується рядом станів, які визначають виконання ними основної функції. Для кожного стану необхідно напрацьовувати рішення, які відносяться до функцій системи: вибір набору функцій, які складають ціль функціонування системи та вибір алгоритму реалізації цих функцій, при яких необхідно вирішувати задачу протидії порушенням функціонування системи.

Недоліком відомого рішення є доволі складна його адаптація при створенні прикладних комплексів, заснованих на сучасній технологічній базі.

В роботі [4] наведені показники і параметри, що характеризують живучість телекомунікаційної мережі, запропоновано метод забезпечення її живучості на основі перерозподілу ресурсів мережі для обслуговування потоків вимог при виникненні несприятливих впливів дозволяє. Авторами декларується, що використання їх методу дозволяє виконати оцінку працездатності мережі на основі запропонованого в роботі показника та знайти «вузькі місця» мережі для можливості їх резервування за рахунок збитковості ресурсів мережі.

Однак, запропонований метод дозволяє оперувати виключно з вузлами, які піддаються реконфігурації, що не завжди можливо в умовах гетерогенності мережі Інтернет, використання віртуальних мереж вендорів хмарних послуг тощо.

Метою статті є розробка методу, який дозволяє забезпечити живучість комп'ютерної мережі, яка є інформаційним середовищем для гарантованого надання цифрових послуг, шляхом використання віртуальних тунелів, заснованих на принципах VPN-тунелювання.

Основна частина

Теоретичне обґрунтування. На відміну від показників живучості, які застосовуються до інформаційних систем [4, 5], до комп'ютерних мереж можна застосувати найбільш суттєві з них:

• кількість зовнішніх деструктивних впливів, при яких комп'ютерна мережа втрачає можливість виконувати основну функцію;

• мінімальна кількість функціонуючих елементів мережі, при яких вона не втрачає можливість виконувати основну функцію;

• ймовірність збереження комп'ютерною мережею стану відновлення протягом запланованого часу.

В основі запропонованого рішення лежить використання принципів VPN-тунелювання [6]. Найбільш уживаною критеріальною базою цього рішення є наведене у [4, 5]. Зокрема варто виділити такі критерії як:

• критерій динаміки швидкості передачі даних в умовах деградації елементів мережі;

• критерій оцінки ефективності застосування сценаріїв відновлення функціональних можливостей комп'ютерної мережі після збоїв або перебудови віртуальних тунелів;

• критерій відповідності елементів та всієї комп'ютерної мережі визначеним показниками якості та безпеки передачі даних.

Спочатку розглянемо модель комп'ютерної мережі для якої потрібно вирішити сформульовану задачу. Нехай у комп'ютерній мережі є три компоненти [7]:

• деякий сегмент комп'ютерної мережі підприємства, що складається з n обчислювальних станцій. (n+1)-обчислювальна станція підключена через комунікаційне обладнання, що забезпечує низькошвидкісний, нестабільний канал передачі даних. В мережі функціонує сукупність обчислювальних станцій, які виконують операції реєстрації, обробки, збереження та передачі інформації;

• вендор ІТ-послуг, що надає «білі» IP-адреси за технологією VPN-тунелювання;

• власне, обчислювальна станція користувача, підключена до мережі Інтернет.

Метою обчислювальної станції користувача є підключення до обчислювальних станцій або модулів, які інтегровані в ці обчислювальні станції, та виконують операції реєстрації, обробки, збереження та передачі інформації, шляхом емуляції віддаленого USB-інтерфейсу.

Модель запропонованої комп'ютерної мережі відноситься до класу структурних систем, саме тому актуальним є забезпечення саме структурної живучості шляхом вибору відповідного критерію живучості. За показником ефективності доцільно обрати здатність комп'ютерної мережі перерозподіляти потоки даних і продовжувати виконувати покладену на неї основну функцію після того, як окремі елементи вийшли з ладу, порушуючи структуру мережі, як то нестабільний канал зв'язку або VPN-тунель.

Аналізуючи існуючі методи забезпечення живучості комп'ютерних мереж, можна сказати, що вони спираються на такі базові принципи як розпізнавання загроз, протидії їм, відновлення у разі деструктивного впливу, адаптації до нових умов функціонування шляхом структурної реконфігурації.

Отже, для організації віртуальної мережної інфраструктури, яка б характеризувалася відповідним рівнем живучості в умовах використання низькошвидкісних, нестабільних і незахищених каналів передачі даних, пропонується наступна послідовність дій.

Крок 1. Необхідно здійснити налаштування механізму трансляції «білої» IP-адреси в сегмент мережі підприємства шляхом використання VPN-сервера. Для цього існує широкий спектр відомих технічних рішень, заснованих на використанні протоколу PPTP. Згідно умови задачі, якщо будуть використані виключно функції видачі «білої» IP-адреси, то процеси передачі інших даних (керуючих команд, часової синхронізації і т.д.) з боку одержувача (спеціальна обчислювальна станція в мережі підприємства) здійснюватися не будуть. Тому, враховуючи останні досягнення в криптостійкості протоколів шифрування, що забезпечують функціонування протоколу PPTP, вибір цього протоколу є очевидним. Однак, можна використовувати більш криптостійкі рішення, наприклад, OpenVPN, однак додатково необхідно вирішувати задачу мінімізації часових затрат, які можуть з'явитися при надмірному потоці даних, які відлягають шаруванню.

Крок 2. У сегменті комп'ютерної мережі підприємства на обчислювальній станції, який має доступ до мережі Інтернет через нестабільний канал зв'язку, створюється клієнтська частина VPN-тунелю. Згідно умов задачі, у якості нестабільного каналу зв'язку, який впливає на живучість комп'ютерної мережі передачі даних, є мережа мобільного оператора. Цей оператор, надаючи доступ до мережі Інтернет обчислювальній станції сегменту мережі підприємства, адресує їй «сірі» IP-адреси. Таким чином, VPN-тунель між сервером та клієнтом є середовищем, через яке здійснюється адресація «білої» IP-адреси в сегмент мережі підприємства.

Крок 3. На базі (n+1)-обчислювальної станції розгортається VPN-сервер, який у якості WAN-інтерфейсу буде використовувати отриману раніше «білу» IP-адресу. Тобто, VPN-сервер буде приймати вхідні запити від користувача з мережі Інтернет на WAN-інтерфейс, а у відповідь на запит, транслювати «сірі» IP-адреси з сегменту комп'ютерної мережі підприємства.

Крок 4. Користувач виконує налаштування своєї частини VPN-тунелю. При підключенні до VPN-сервер обчислювальна станція користувача буде вузлом комп'ютерної мережі підприємства. Важливо зауважити, що використання шлюзу, який одночасно є VPN-сервером, – не рекомендується, так як це збільшує навантаження на тунель, що в свою чергу, може призвести до зменшення пропускної можливості VPN-тунелю.

Крок 5. У разі використання гібридних моделей створення віртуальних мереж, які засновані на використанні комп'ютерних мереж провайдерів, які не

використовуються у якості опорних вузлів схеми маршрутизації, можлива додаткова оцінка часових затримок між сегментами мереж провайдерів. Створення оверлейних мереж за таким принципом дозволяє зменшувати часові затримки, тим самим підвищуючи показник живучості мережі у разі деструкції міжпровадерських опорних мереж зв'язку.

На рис. 1 наведена схема методу, описана в роботі.

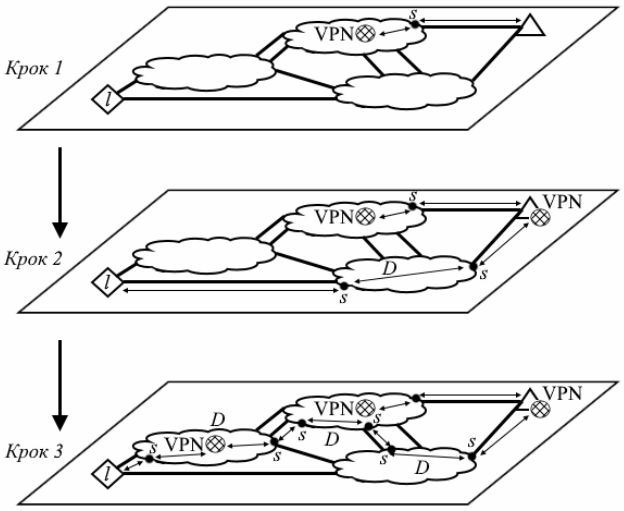

Рис. 1. Схема методу забезпечення живучості

Виходячи з того, що користувачів, які надсилають запити на підключення до сегменту мережі підприємства, може бути більш одного, доцільно виконати оцінку стану пропускної здатності каналу передачі даних між кожною обчислювальною станцією користувачів і VPN-сервером. Це необхідно при розрахунку показників мережного балансування в разі коливання пропускної здатності нестабільного каналу зв'язку, тобто, коли виникає класична проблема дефіциту ресурсу пропускної здатності.

Отже, для оцінки стану пропускної здатності VPN-тунелів необхідно, щоб всі прикордонні пристрої маршрутизації потоків даних користувачів передавали спеціальні пакети даних до VPN-серверу підприємства [8]. Для прикладу розглянемо доставку пакета від обчислювальної станції в сегменті комп'ютерної мережі підприємства до всіх підключених обчислювальних станцій користувачів VPN-мережі і визначимо значення пропускної здатності, яка не ефективно використовується під час обміну даними.

Загальну пропускну здатність VPN-тунелю окремо взятого підключення до сегменту комп'ютерної мережі підприємства через VPN-тунель можна обчислити аналітично як з'єднання «точка-точка»:

$$\Psi = D\ell(2S + (2i-1)\sum_{i=1}^{\log_2 S} 2^{i-1}, \qquad (1)$$

де D – кількість проміжних вузлів маршрутизації між VPN-мережами (в тому числі віртуальних вузлів); S – кількість прикордонних вузлів маршрутизації; ℓ – кількість обчислювальних станцій користувачів.

З іншого боку, якщо, наприклад, схема передачі даних реалізована за принципом «точка – три точки» для кожного з VPN-тунелів всім користувачам VPN-мережі (наприклад, для широкомовної відправки телеметрії), то загальна пропускна здатність має вигляд:

$$\Psi' = D(1+\log_2 S + \sum_{i=1}^{\log_2 S} 2^i + \ell S), \qquad (2)$$

Таким чином, для запропонованого прикладу комп'ютерної мережі значення пропускної здатності, яка використовується неефективно та може бути використана у якості фактору підвищення збитковості комп'ютерної мережі у разі настання події забезпечення її живучості є:

$$\theta = D(\ell S - YW), \qquad (3)$$

де Y – середня кількість вершин VPN-мережі, залежна від кількості вузлів маршрутизації в сегменті мережі з організації транспорту трафіку через «білі» IP-адреси; $\underline{W}$ – кількість гілок дерева маршрутизації в каскадних (або резервних) схемах підключення [8].

Прикладне обгрунтування. У 2019 р. на базі лабораторії кафедри Електронних обчислювальних машин Харківського національного університету радіоелектроніки, в рамках виконання наукового проекту з розробки прикладного рішення дистанційного керування мікроконтролерним обладнанням і здійснення доступу до локальної обчислювальної станції збору телеметричної інформації лабораторії було апробовано розроблений метод забезпечення живучості віртуальної мережі з використанням багатошляхового VPN-тунелювання [9]. Додатковими вимогами і умовами виконання прикладної задачі були: комп'ютерна мережа лабораторії організована через мережний шлюз, який, в свою чергу, підключений до 4G-модему; мобільний провайдер Інтернет-послуг не надає «білих» IP-адрес; нестабільний канал зв'язку провайдера Інтернет-послуг.

Щодо користувачів, то виділяється два типи: ті, які можуть надсилати команди управління мікроконтролерному обладнанню (через спеціалізоване програмне забезпечення) і спостерігати за виконанням задачі на своїй обчислювальній станції (в цьому випадку обчислювальна станція носить назву дистанційно-керуючої); і ті, які можуть надсилати команди управління мікроконтролерному обладнанню, завантажуючи їх з локальної обчислювальної станції комп'ютерної мережі лабораторії і періодично перевіряти виконання задачі за допомогою відділеного доступу до цієї станції.

Виходячи з вищесказаного, умовно задачу можна розбити на кілька підзадач: організація зовнішнього інтерфейсу комп'ютерної мережі лабораторії для можливості підключення користувачів із зовнішньої мережі Інтернет (реалізується ідея безперервної взаємодії з мікроконтролерним обладнанням); і організація дистанційного доступу до локальної обчислювальної станції лабораторії з метою локальної постановки задачі і моніторингу виконання роботи мікроконтролерного обладнання. Так як мікроконтролерне обладнання може взаємодіяти з локальною обчислювальною станцією лабораторії, яка знахо-

диться в одному сегменті мережі з нею, обчислювальна станція користувача повинна мати ту ж IP-адресацію, що і в комп'ютерній мережі лабораторії.

В даному випадку був використаний вище запропонований метод. В даному випадку одна з обчислювальних станцій комп'ютерної мережі лабораторії була налаштована в ролі VPN-сервера. Однак, так як Інтернет-провайдер не мав можливості делегувати «білу» IP-адресу, було прийнято рішення отримувати «білу» IP-адресу в мережі третього провайдера. Тепер обчислювальна станція, що виконує функцію шлюзу комп'ютерної мережі лабораторії, підключаючись до VPN-сервера третього провайдера отримує «білу» IP-адресу. Далі була вирішена зворотна задача, коли на обчислювальній станції, що виконує функцію шлюзу комп'ютерної мережі лабораторії, встановлений VPN-сервер, у якого, в якості WAN-інтерфейсу, використовувалася «біла» IP-адреса, отримана від VPN-сервера третього провайдера.

Обчислювальна станція користувача, підключаючись до VPN-сервера в лабораторії по «білій» IP-адресі, отримує «сіру» IP-адресу комп'ютерної мережі лабораторії. Таким чином, обчислювальна станція користувача виступає в ролі дистанційно-керуючої, маючи можливість відправляти і приймати дані з мікроконтролерного обладнання.

Основні проблеми даного рішення полягають нестійкому каналі зв’язку з мережею Інтернет та коливанні часу затримки при передачі даних в залежності від завантаження прикордонних маршрутизаторів на стику провайдерів. У разі розриву з'єднання одним з провайдерів в ланцюгу з’єднання або в силу інших причин, обчислювальна станція, що виконує функції шлюзу, виконує процедуру повторного підключення до VPN-сервера третього провайдера. Цю процедуру повторює і дистанційно-керуюча обчислювальна станція. І хоча після відправки команд управління на мікроконтролерне обладнання, останнє їх виконує, то при відсутності зв'язку між учасниками віртуальної мережі, звіт про виконання команд, відповідно, перестає бути актуальним. Тому, при тривалих дистанційних роботах з мікроконтролерним обладнанням недоцільно використовувати вищевказаний підхід. Досить завантажити команди управління на локальну обчислювальну станцію лабораторії та періодично перевіряти виконання задачі спостереження за допомогою підключення до локальної обчислювальної станції лабораторії відомими способами.

У 2020 році, в зв'язку з введенням карантинних обмежень та переходом на дистанційне навчання в Україні [10] виникла необхідність віддаленого управління деякими модулями в вищеописаній лабораторії, підключеними за допомогою інтерфейсу USB до однієї з обчислювальних станцій. В основі запропонованого рішення є використання відкритого програмного продукту USB/IP. Це ПЗ дозволяє здійснювати обмін даними з USB-пристроями через локальну комп’ютерну мережу. ПЗ призначене для спільного використання USB-пристроїв між обчислювальними станціями. При повному збереженні функціоналу USB/IP трансформує «USB I/O повідомлення» в формат TCP/IP-пакетів і передає їх в комп’ютерну мережу.

Загальним в цих рішеннях є те, що для обчислювальної станції, яка виконує функції шлюзу, в комп’ютерній мережі з нестабільним низькошвидкісним зовнішнім каналом зв’язку виділяється через VPN-тунель «біла» IP-адреса. Однак це не завжди може бути можливим. Наприклад, якщо відсутня можливість підключення третього провайдера, який є постачальником «білих» IP-адрес, а є в наявності динамічно змінювана «біла» IP-адреса, то мови про надання виділеного адреси для комп’ютерної мережі підприємства може і не йти.

У цьому випадку на прикордонному вузлі, що виконує функції маршрутизатора, в комп’ютерній мережі VPN-сервера необхідно виконати перенаправлення забезпечуючих портів для того, щоб VPN-сервер був доступний для підключення з мережі Інтернет. Обчислювальна станція, що знаходиться в комп’ютерній мережі підприємства, при підключенні до такого VPN-сервера буде отримувати «сіру» IP-адресу. Для підключення до комп’ютерної мережі підприємства необхідно для отриманої «сірої» IP-адреси виконати перенаправлення портів на шлюзі підмережі VPN-сервера, які забезпечують підключення до VPN-сервера мережі підприємства.

Тепер користувач, в налаштуваннях VPN-тунелю вказує «білу» IP-адресу шлюзу. Запит на заданий порт буде переадресований по VPN-тунелю вузлу з «сірою» IP-адресою, який, в свою чергу, адресує обчислювальній станції користувача IP-адресу з підмережі підприємства. Досить задати правило маршрутизації підмережі підприємства через шлюз – і зв'язок буде встановлений.

Експериментальні дослідження. Завданням експериментального дослідження було визначення оптимального схеми використання протоколу UDP для передачі інформації по захищеним SSL-VPN-тунелів, реалізованим із застосуванням програмного забезпечення OpenVPN в умовах нестабільних каналів зв’язку та визначення порогового значення показника живучості у разі деструкції VPN-тунелів Припустимо, що якщо основний VPN-тунель налаштований на роботу з протоколом TCP, сервер буде отримувати TCP-пакети OpenVPN, які містять інші TCP-сегменти від користувача. У результаті в ланцюзі виходить подвійна перевірка на цілісність інформації, що абсолютно не має сенсу, тому що надійність не підвищується, швидкість з'єднання знижується [11–16]).

Проведено вимірювання залежності швидкості передачі команд управління на мікроконтроллерне обладнання лабораторії від ймовірності втрати пакетів в мережі для протоколу UDP. У якості сценарію експерименту була використана методика [11], в основі лежить ідея тестування алгоритмів тунелювання UDP поверх UDP. Дані експерименти ставилися для всіх VPN-тунелів.

Вихідні дані: розмір пакетів, переданих на мікроконтролерне обладнання – 32050 байт; розмір пакетів, що передавалися у зворотньому напрямку – 4020 байт; співвідношення інтенсивності передачі

відправлених і прийнятих пакетів - 1/10. Експеримент проводився 01 грудня 2021 року на кафедрі Електронних обчислювальних машин Харківського національного університету радіоелектроніки.

Результати експерименту по тунелюванню «Обчислювальна станція користувача» – «Комп'ютерна мережа лабораторії» при відпрацюванні команд управління мікроконтролерному обладнанню з використанням схеми тунелювання по UDP та TCP представлені в табл. 1.

Таблиця 1 – **Результати тунелювання при відправці даних**

№ п/п	Ймовірність відкидання пакетів, %	Інтенсивність, пакет/с	Кількість втрачених пакетів, шт.
Схема тунелювання по UDP			
1	0	50	0
2	1	75	1
3	2	100	1
4	3	125	2
5	4	150	10
6	5	175	12
7	6	200	14
8	7	225	18
9	8	250	19
10	9	275	25
11	10	300	39
Схема тунелювання по TCP			
1	0	50	0
2	1	75	0
3	2	100	0
4	3	125	0
5	4	150	1
6	5	175	1
7	6	200	2
8	7	225	3
9	8	250	3
10	9	275	5
11	10	300	7

У табл. 2 представлені результати експерименту в разі прийому телеметричних даних з мікроконтролерного обладнання лабораторії обчислювальною станцією користувача.

Як видно з результатів проведених експериментів, використання протоколу UDP в якості основного можна вважати ефективним для прийому телеметричних даних (UDP-трафіку) по VPN-тунелям. Однак при передачі команд управління, представленої у вигляді неінтенсивного трафіку, доцільно використовувати протокол TCP поверх протоколу UDP. Це пояснюється тим, що існує велика ймовірність втрати пакетів, через відсутність механізмів адаптації до поточного стану нестабільного каналу зв'язку, а саме механізму регулювання розміру вікна. Очевидно, що протокол UDP показує більш низькі результати, ніж TCP. Механізм повторних передач, що реалізується з використанням протоколу TCP (для еластичного трафіку) дозволяє компенсувати втрачені пакети за рахунок повторних команд.

Таблиця 2 – **Результати тунелювання при прийомі даних**

№ п/п	Ймовірність відкидання пакетів, %	Інтенсивність, пакет/с	Кількість втрачених пакетів, шт.
Схема тунелювання по UDP			
1	0	50	1
2	1	75	5
3	2	100	8
4	3	125	18
5	4	150	30
6	5	175	49
7	6	200	55
8	7	225	58
9	8	250	62
10	9	275	68
11	10	300	71

Необхідно відзначити, що об'єднання VPN-тунелів в каскадні схеми є не ефективним для побудови великих віртуальних мережних інфраструктур. Незважаючи на те, що пропускна здатність залежить від виду топології мережі, необхідно проводити аналіз розподілу VPN-підмереж з метою підвищення надійності процесу передачі даних. Таким чином, можна зробити висновок, що аналіз загальної пропускної здатності VPN-тунелів мереж багато в чому залежить від правильної організації розподілу ресурсів системи. Це також в деякій мірі пов'язано з маршрутизацією даних і правилами призначення шлюзів для обчислювальних станцій підприємства і користувачів в якості опорних вузлів мережі – для уникнення можливих неефективних маршрутів передачі інформації, мережних петель тощо.

Висновки

В результаті проведеної роботи поставлена і успішно вирішена науково-прикладна задача розробки методу, який дозволяє забезпечити живучість комп'ютерної мережі, яка є інформаційним середовищем для гарантованого надання цифрових послуг, шляхом використання віртуальних тунелів, заснованих на принципах VPN-тунелювання. Зокрема, досягнуто такі результати:

• сформульована наукову задачу з формалізацією необхідних технічних вимог до розроблюваної комп'ютерної мережі;

• розроблено прикладне рішення забезпечення живучості комп'ютерної мережі, засноване на використанні множинних VPN-тунелів;

• проведені експерименти з дослідження ефективності використання різних мережних протоколів в VPN-тунелях;

• отримала подальший розвиток методологія забезпечення живучості комп'ютерних систем для забезпечення безперервності процесів управління мережними інфраструктурами.

Запропонований метод може бути використаний на етапах проектування комп'ютерних мереж в частині визначення показників надлишковості при реалі-

зації принципів управління елементами мережі як то сервери, шлюзи, технологічне обладнання тощо.

У якості подальшої дослідницької роботи за даним напрямом пропонується розглянути ефективність застосування багатошарових оверлейних мереж [17] у якості транспортного середовища при вирішенні задачі підвищення живучості комп'ютерних мереж.

СПИСОК ЛІТЕРАТУРИ

1. Nahavandi, S. (2019). Industry 5.0—A human-centric solution. Sustainability, 11(16), 4371.
2. Kharchenko, V., Kondratenko, Y., & Kacprzyk, J. (Eds.). (2017). Green IT engineering: concepts, models, complex systems architectures. Springer International Publishing.
3. Додонов А.Г., Ландэ Д.В. Живучесть информационных систем. - К.: Наук. думка, 2011. - 256 с.
4. Князева Н. А. Метод обеспечения живучести телекоммуникационной сети на основе перераспределения ресурсов сети / Н. А. Князева, И. В. Грищенко, С. В. Шестопалов // Холодильна техніка та технологія. - 2014. - № 4. - С. 65-71.
5. Кучук Г.А. Метод перерозподілу пропускної здатності критичної ділянки мережі на основі удосконалення ON/OFF-моделі трафіку / Г.А. Кучук, А.С. Свиридов, А. А. Коваленко. // Сучасні інформаційні системи. Харків: НТУ «ХПІ», 2018. – Том 2, № 2. – С. 139-144.
6. L.D. Orda, T.V. Jensen, O. Gehrke, & H.W. Bindner (2019). "Efficient Routing for Overlay Networks in a Smart Grid Context". Proceedings of the 8th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS 2019), Heraklion, Crete, Greece, 2019, pp. 251-258.
7. Tkachov, V., Bondarenko, M., Ulyanov, O., & Reznichenko, O. (2019, December). Overlay Network Infrastructure for Remote Control of Radio Astronomy Observatory. In 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT) (pp. 161-165).
8. Кулаков А. Ю. Способ повышения эффективности GRID систем на базе виртуальных сетей VPN / А. Ю. Кулаков // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка : зб. наук. пр. – 2007. – № 47. – С. 280–286.
9. R. Wróbel, M. Andrych-Zalewska, & R. Dimitrov (2016). Diagnostic telemetry system. Journal of KONES. Powertrain and Transport, 23(4), pp.569-574.
10. Doghonadze, N., Aliyev, A., Halawachy, H., Knodel, L., & Adedoyin, A. S. (2020). The Degree of Readiness to Total Distance Learning in the Face of COVID-19-Teachers' View (Case of Azerbaijan, Georgia, Iraq, Nigeria, UK and Ukraine). Journal of Education in Black Sea Region, 5(2), 2-41.
11. Шейда, В. В. (2010). Использование протоколов TCP и UDP для защищенной передачи информации по SSL-VPN-туннелям. Доклады Томского государственного университета систем управления и радиоэлектроники, (1-2 (21)).
12. Amin Salih M., Potrus M.Y. A Method for Compensation of TCP Throughput Degrading During Movement Of Mobile Node. *ZANCO Journal of Pure and Applied Sciences*. 2015. Vol. 27, No 6. P. 59–68.
13. Nechausov A., Mamusuĉ I., Kuchuk N. Synthesis of the air pollution level control system on the basis of hyperconvergent infrastructures. Сучасні інформаційні системи. 2017. Т. 1, № 2. С. 21 – 26. DOI: https://doi.org/10.20998/2522-9052.2017.2.04
14. Amin Salih Mohammed, Saravana Balaji B., Saleem Basha M S, Asha P N and Venkatachalam K (2020), FCO — Fuzzy constraints applied Cluster Optimization technique for Wireless AdHoc Networks, *Computer Communications*, Volume 154, , Pages 501-508, DOI: https://doi.org/10.1016/j.comcom.2020.02.079.
15. Sivaram, M., Yuvaraj, D., Mohammed, A. S., Manikandan, V., Porkodi, V., & Yuvaraj, N. (2019). Improved Enhanced Dbtma with Contention-Aware Admission Control to Improve the Network Performance in Manets. *CMC-COMPUTERS MATERIALS & CONTINUA*, *60*(2), pp. 435-454, DOI: https://doi.org/10.32604/cmc.2019.06295
16. Mozhaiev, M., Kuchuk, N. and Usatenko, M. (2019), " The method of jitter determining in the telecommunication network of a computer system on a special software platform", *Innovative technologies and scientific solutions for industries*, Vol. 4 (10), pp. 134-140. doi: https://doi.org/10.30837/2522-9818.2019.10.134.
17. Tkachov V. Principles of Constructing an Overlay Network Based on Cellular Communication Systems for Secure Control of Intelligent Mobile Objects / Vitalii Tkachov, Andriy Kovalenko, Mykhailo Hunko and Kateryna Hvozdetska // Информационные технологии и безопасность. Материалы XIX Международной научно-практической конференции ИТБ-2020. – К.: ООО "Инжиниринг", 2020. – С. 51-55.

Received (Надійшла) 23.10.2020
Accepted for publication (Прийнята до друку) 20.01.2021

Method of ensuring the survivability of the computer network based on VPN-tunneling

Andriy Kovalenko, Heorhii Kuchuk, Vitalii Tkachov

Abstract. The article analyzes the main approaches to ensuring the survivability of computer networks. It is shown that the survivability methodology that is applied to computer systems is partially different from that used in computer networks, which is associated with the active development of virtualization technologies. The **purpose** of the article is to develop a method to ensure the survivability of a computer network, which is an information environment for guaranteed provision of digital services, by using virtual tunnels based on the principles of VPN tunneling to delegate "white" IP addresses to computer networks, or routing schemes for data flows when using internal VPN servers with a single "white" IP address. The results obtained make it possible: to formulate a scientific problem with the formalization of the necessary technical requirements for the developed computer network; develop an application solution for ensuring the survivability of a computer network based on the use of multiple VPN tunnels; conduct a series of experiments to study the effectiveness of using various network protocols in VPN tunnels; to create a basis for further development of the methodology for ensuring the survivability of computer systems to ensure the continuity of network infrastructure management processes. The studies allow us to **conclude** that the proposed method can be used at the design stages of computer networks when determining redundancy indicators when implementing the principles of managing network elements such as servers, gateways, technological equipment, etc.

Keywords: survivability, computer network, virtualization, VPN.