

Голові спеціалізованої вченої ради  
Д 64.052.09 в Харківському національному університеті радіоелектроніки  
Україна, 61166, м. Харків, пр. Науки, 14.

## ВІДГУК

офіційного опонента професора кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка, доктора технічних наук, професора Толюпи Сергія Васильовича на дисертаційну роботу Чакряна Вадима Хазаровича на тему: «Моделі та методи маршрутизації трафіку в телекомунікаційних мережах з урахуванням вимог інформаційної безпеки», поданої на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.02 – «Телекомунікаційні системи та мережі».

### 1. Актуальність теми роботи

Здобувач зосередив свою увагу на процесах динамічної маршрутизації трафіку в телекомунікаційних мережах (ТКМ). Однією з проблем є те, що найбільш поширені сучасні алгоритми динамічної маршрутизації не враховують ризики інформаційної безпеки та не забезпечують захист інформації від кібератак в процесі її передачі. Це дає змогу зловмиснику порушити інформаційну безпеку (ІБ) транзитного трафіку, що передається в мережі, шляхом перемаршрутизації трафіку з метою подальшої компрометації, чи шляхом здійснення атак відмови в обслуговуванні з метою унеможливлення доставки пакетів отримувачу.

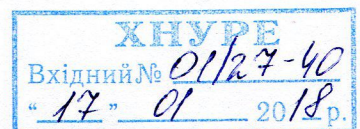
Вирішення вказаних проблем можливе лише шляхом впровадження нових моделей динамічної маршрутизації, що дозволять вибирати шлях передачі трафіку не лише на основі параметрів якості обслуговування, а й враховуючи параметри інформаційної безпеки.

Саме тому формулювання та вирішення **науково-практичної задачі**, яка полягає у підвищенні інформаційної безпеки трафіку в процесі його динамічної маршрутизації в телекомунікаційній мережі, є **актуальною**.

### 2. Наукова новизна результатів роботи.

Основними новими науковими результатами дисертаційної роботи є:

1. Вперше запропоновано метод оцінки ризику інформаційної безпеки шляхів передачі потоку пакетів, новизною якого є врахування таких



параметрів як: ефективність та вразливість маршрутизаторів мережі, а також ймовірність здійснення атаки типу відмова в обслуговуванні на маршрутизатори. Застосування даного методу дало змогу оцінювати ризики порушення конфіденційності, цілісності та доступності потоку пакетів при його передачі по заданому шляху.

2. Удосконалена модель процесу передачі пакетів від вузла-відправника до вузла-отримувача в умовах кібератак, новизною якої є можливість проведення розрахунків при наявності атак типу відмова в обслуговуванні на маршрутизатори мережі; шкідливих процесів на маршрутизаторах, які знижують пропускну здатність вузлу, чи взагалі виводять його з ладу; атак на перемаршрутизацію даних по не ефективним шляхам. Використання наведеної моделі дозволило оцінювати ризик несвоєчасної доставки пакетів на кінцевий вузол по заданому шляху в умовах завантаженості маршрутизаторів мережі внаслідок кібератак.

3. Отримали подальший розвиток моделі одношляхової та багатошляхової маршрутизації потоку пакетів в телекомунікаційній мережі в умовах кібератак. Новизною моделей є врахування ризику інформаційної безпеки разом з базовими параметрами в формулах розрахунку метрик шляхів. Використання запропонованих моделей дозволило вибирати шлях передачі потоку пакетів в телекомунікаційній мережі на основі критерію «безпека-якість» та знизити ризики порушення конфіденційності, цілісності, доступності та своєчасної доставки транзитного потоку пакетів.

### **3. Практична значимість наукових результатів**

Запропоновані моделі та методи можуть бути використані при проектуванні та підтримці сучасних мультисервісних телекомунікаційних мереж. Отримані результати використовувалися при розробці перспективних протоколів динамічної маршрутизації в сучасних мультисервісних телекомунікаційних системах, при проектуванні пристрою радіомоніторингу КХ діапазону Р-677 УИДЯ.466948.006 на Державному підприємстві «Центральне конструкторське бюро «Протон», а також в навчальному процесі кафедри інфокомунікаційної інженерії Харківського національного університету радіоелектроніки (ХНУРЕ) в дисципліні «Безпека інформації в інформаційно-комунікаційних системах», що підтверджується відповідними актами впровадження.

### **4. Достовірність отриманих результатів**

Обґрунтованість та достовірність отриманих в дисертаційній роботі наукових положень, висновків та рекомендацій забезпечується коректним

використанням можливостей добре апробованих математичних підходів, заснованих на теорії масового обслуговування, теорії графів та множин, методах математичного програмування, а також якісним і кількісним зіставленням результатів імітаційного моделювання з відомими положеннями теорії і чітким фізичним трактуванням отриманих результатів дослідження.

### **5. Особистий внесок здобувача**

Наукові результати, наведені в дисертаційній роботі, здобувач отримав самостійно. В одній з робіт автором представлена удосконалена модель пошуку оптимального шляху передачі потоку пакетів в заданій ТКМ з урахуванням ризику ІБ на основі метрики протоколу RIP; в іншій роботі автором запропонована напівмарківська модель процесу передачі потоку пакетів в ТКМ, яка дозволяє представити динаміку процесу в умовах інформаційних атак з урахуванням його ймовірнісно-часових характеристик; в окремій роботі автором запропоновано метод, який дозволяє розрахувати ризик ІБ мережевого маршрутизатора на підставі метрик стандарту NIST CCSS; також автором представлено дві окремі роботи, в одній з яких проаналізовано існуючі вразливості стека протоколів IPv6, а в іншій проведено аналіз методів захисту від загроз шляхом впровадження механізмів безпеки, покликаних збільшити ІБ для стека протоколів IPv6; в одній з робіт автором запропоновано метод, який дозволяє запобігти перевантаженню одного з каналів зв'язку при використанні стандартного методу балансування навантаження по шляхах нерівнозначної вартості протоколу EIGRP; в іншій роботі автором запропоновано метод врахування ризику ІБ в формулі розрахунку метрики протоколів динамічної маршрутизації EIGRP, який дозволяє динамічно вибирати найбільш безпечний маршрут передачі потоку пакетів, при цьому враховуючи стандартні показники метрики протоколу EIGRP. Також здобувачем отримано патент на корисну модель маршрутизації трафіку за допомогою протоколу EIGRP з урахуванням вимог ІБ, наукова новизна результатів якого полягає у врахуванні ризику інформаційної безпеки маршруту в формулі розрахунку метрики протоколу EIGRP, що дозволяє вибирати маршрут передачі потоку пакетів в ТКМ за критерієм «якість-безпека».

Основні результати дисертаційної роботи опубліковані в 22 наукових працях: одна стаття у закордонному фаховому журналі, сім статей у вітчизняних фахових науково-технічних журналах; апробація результатів дисертації проходила у ході тринадцяти міжнародних науково-технічних

конференцій, шість з яких проходили під егідою IEEE та індексуються в міжнародних наукометричних базах Scopus та IEEE Xplore Digital Library.

## **6. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації**

Дисертаційна робота носить завершений характер науково дослідної роботи та подана у вигляді вступу, чотирьох розділів, висновків, списку використаних джерел та десяти додатків. Загальний обсяг роботи становить 191 сторінку, з яких 144 сторінки основного тексту; 30 сторінок додатків; 2 сторінки переліку скорочень, умовних позначень, символів, одиниць і термінів; список використаних джерел містить 133 найменування на 17 сторінках. Дисертація містить 24 рисунка і 2 таблиці.

Автореферат дисертаційної роботи в повній мірі відображає наукові та практичні результати, що подані в дисертаційній роботі.

У *вступі* розкрито основний зміст і загальний стан проблеми і окремих завдань підвищення інформаційної захищеності транзитного потоку пакетів, що передається в ТКМ; обґрунтовано актуальність теми дослідження; позначений зв'язок роботи з науковими програмами і темами; сформульовані мета і завдання дослідження; визначено об'єкт, предмет і методи дослідження; розкрито наукову новизну і практичне значення отриманих в дисертаційній роботі результатів.

В *першому розділі* представлено аналіз актуальності теми дослідження та напрацювань інших вчених в даному напрямі. Також проаналізовані методи кібератак на процеси динамічної маршрутизації та існуючі методи захисту від них. Сформульовані вимоги щодо методів розрахунку ризику інформаційної безпеки та їх врахуванні у метриках протоколів динамічної маршрутизації. На основі ґрунтовного аналізу поставлена науково-практична задача дослідження.

В *другому розділі* представлені методи розрахунку ризику інформаційної безпеки заданого шляху передачі трафіку. Це дозволило використовувати отримані параметри при розрахунках метрик протоколів динамічної маршрутизації та впливати таким чином на вибір оптимального шляху передачі трафіку.

В *третьому розділі* представлено удосконалені моделі динамічної маршрутизації з урахуванням ризику інформаційної безпеки шляхів при розрахунках метрик протоколів динамічної маршрутизації, які досліджуються в роботі – RIP, OSPF, EIGRP.

У *четвертому розділі* представлені результати кількісного аналізу запропонованих методів та моделей, в ході якого було виявлено, що захищеність потоку пакетів зростає на 4% у разі використання метрики протоколу RIP, та у 13-14% у разі використання метрик протоколів OSPF та EIGRP.

За результатами оцінки тексту дисертаційної роботи можна зробити висновок, що твердження та результати, основні висновки, що подані в дисертаційній роботі, сумнівів не викликають.

#### **7. Мова та стиль викладення наукових положень**

Тема дисертації повністю відповідає її змісту та відображає суть розглянутих та вирішених наукових завдань. Дисертант логічно та аргументовано викладає результати досліджень і отримані ним наукові положення. Текст дисертації та автореферату написані грамотною, науково-технічною мовою з застосуванням загальновизнаної термінології. Автореферат відповідає змісту дисертації та достатньо повно і послідовно розкриває основні положення дисертаційної роботи.

#### **8. Недоліки та зауваження**

В якості основних недоліків та рекомендацій по дисертаційній роботі необхідно відмітити такі:

1. Замалий масштаб та низька якість графіку в основному тексті роботи – рис. 2.2 на стор. 63.

2. В роботі при розрахунках ризиків інформаційної безпеки немає обґрунтування механізму розрахунку ймовірності реалізації загрози, яка повинна розраховуватися на підставі моделі загроз (порушника).

3. Проблема усереднення ризику інформаційної безпеки заданого шляху, яка описана в висновках дисертаційної роботи та автореферату (с. 16 п. 2), є вагомим недоліком, що може призвести, у деяких випадках, до некоректної роботи запропонованої в роботі моделі динамічної маршрутизації.

4. Другий розділ має великий об'єм, зі структурної точки зору було б більш прийнятно розділити його на два окремі розділи.

5. В дисертації немає обґрунтування часу оновлення інформації в системі маршрутизації про реалізацію загроз кібербезпеки.

6. В дисертації для опису маршрутизатора як одноканальної системи масового обслуговування з очікуванням, прийнята модель M/M/1. На даний час існують дослідження в яких доказано, що вхідний потік в систему є

самоподібним. Доцільно розповсюдити результати дослідження на ситуації з самоподібним вхідним потоком на маршрутизатор.

Вказані недоліки та зауваження не впливають на загальний висновок про дисертаційну роботу.

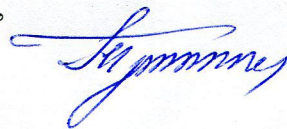
### 9. Загальний висновок щодо дисертації

1. У дисертаційній роботі Чакряна Вадима Хазаровича розв'язано актуальну наукову задачу, яка полягає в підвищенні інформаційної безпеки потоку пакетів в процесі його динамічної маршрутизації в телекомунікаційній мережі шляхом урахування ризиків порушення конфіденційності, цілісності та доступності транзитних даних як додаткових параметрів вибору оптимального шляху передачі.

2. За ступенем обґрунтованості, наукової новизни та практичної значимості отриманих у роботі результатів дисертація Чакряна Вадима Хазаровича відповідає п.п. 9,11,12,13 "Порядку присудження наукових ступенів", затвердженого постановою Кабінету Міністрів України від 24 липня 2013 р. № 567 (назва Порядку із змінами, внесеними згідно з Постановою КМ № 656 від 19.08.2015, №1159 від 30.12.2015р., та №567 від 27.07.2016р.), а її автор Чакрян Вадим Хазарович гідний присудження наукового ступеня кандидата технічних наук зі спеціальності 05.12.02 – телекомунікаційні системи та мережі

#### Офіційний опонент:

професор кафедри кібербезпеки та захисту  
інформації Київського національного  
університету імені Тараса Шевченка,  
доктор технічних наук, професор



С.В. Толупа

ПІАПИС ЗАСВІДЧУЮ  
ВЧЕНИЙ СЕКРЕТАР НАУК  
КАРАУЛЬНА Н.В.  
15.01.2016

